Universidad Mayor de San Andrés
Facultad de Ciencias Puras y Naturales
Carrera de Matemática

PROYECTO DE GRADO

Espacios cuadráticos: Teoremas fundamentales de Witt

Autor: **Univ. Juan Daniel Copacondo Mamani**
Tutor: **Lic. Ramiro Choque Canaza**

copacondodaniel@gmail.com

La Paz, febrero de 2019

Espacios cuadráticos: Teoremas fundamentales de Witt

Por: Juan Daniel Copacondo Mamani

REMITIDO EN CUMPLIMIENTO PARCIAL DE LOS
REQUISITOS PARA LA OBTENCIÓN DEL GRADO DE
LICENCIATURA EN MATEMÁTICA
DE LA
UNIVERSIDAD MAYOR DE SAN ANDRÉS

TUTOR:
LIC. RAMIRO CHOQUE CANAZA
TRIBUNAL:
LIC. RAUL BORDA VEGA
LIC. HELDER LÓPEZ ROMERO

LA PAZ - BOLIVIA
2019

Índice general

Resumen

Sean K un cuerpo de característica diferente de 2 y E un K-espacio vectorial de dimensión finita. Se define un espacio cuadrático como una pareja (E, B), donde B es una forma bilineal simétrica sobre E. Fijada una base de E, B determina una matriz simétrica $n \times n$, con $n = \dim E$, cuyos coeficientes definen simultáneamente una forma cuadrática sobre K.

Dos espacios (E, B) y (E', B') son isométricos si existe un isomorfismo de espacios vectoriales $T : E \longmapsto E'$ tal que, para cualesquiera $u, v \in E$, $B'(Tu, Tv) = B(u, v)$. Se define de forma similar la equivalencia de formas cuadráticas (def. 1.5). Entonces, existe una correspondencia biunívoca entre las clases de isometría de espacios cuadráticos y las clases de equivalencia de K-formas (prop. 1.2).

Dado (E, B), si existe $0 \neq v \in E$ tal que $B(v, v) = 0$, v es llamado isótropo, al igual que E. Si E no tiene vectores isótropos, es llamado anisótropo. Se muestra que la isotropía es una propiedad de la clase de isometría de un espacio dado.

Dados dos espacios cuadráticos E y E', se define su suma ortogonal $E \perp E'$ (def. 2.2). Se demuestra que todo espacio isótropo es o contiene una suma ortogonal de uno o más planos hiperbólicos. Luego, se caracteriza cada espacio como suma ortogonal de dos subespacios: $E \cong E_a \perp r\mathbb{H}$, donde E_a es anisótropo y $r\mathbb{H}$ es una suma de planos hiperbólicos (teorema 4.5 y corolario 4.6).

Se define el anillo de Witt $W(K)$ sobre la colección de K-formas regulares (def. 1.8) con el producto tensorial; y, la suma ortogonal módulo $\mathbb{H}$. Este anillo exhibe propiedades de K mismo; y, según su estructura, clasifica y caracteriza las clases de equivalencia de K-formas.

Introducción

Formas cuadráticas aparecen en muchas áreas de las matemáticas: teoría de números, geometría algebraica, topología y teoría de la información, por mencionar algunas. Estas surgen de manera natural en estadística, mecánica y en otros problemas de física. También utilizamos formas cuadráticas para clasificar cónicas y superficies cuádricas. Aparecen, además, al estudiar los máximos y mínimos de funciones de varias variables.

En este trabajo se hace un estudio de los fundamentos de la teoría algebraica de formas cuadráticas.

Clásicamente, se define una forma cuadrática de grado n con coeficientes en un cuerpo K, como un polinomio homogéneo f de grado 2. Uno de los problemas más importantes de la teoría es determinar cuándo f posee ceros no triviales, es decir, determinar si existen escalares en K, no todos cero, tales que el polinomio f se anula en ellos. Si f posee un cero no trivial, es denominada isótropa; y, anisótropa en caso contrario. La isotropía de f depende de su estructura misma y del cuerpo subyacente.

Se denomina "teoría algebraica" porque se establece una definición equivalente a la definición clásica de formas cuadráticas, en términos de espacios vectoriales sobre el cuerpo de coeficientes de la forma cuadrática; y, formas bilineales simétricas sobre estos. Luego, se "simplifica" su expresión mediante transformaciones lineales para determinar la isotropía de su clase de equivalencia, la que se define en términos de operadores invertibles. Se advierte que la isotropía es una propiedad de la clase de equivalencia de la forma cuadrática dada. Entonces, el estudiar las propiedades de las clases de equivalencia de formas cuadráticas es el enfoque que da la teoría algebraica de formas cuadráticas y, por tanto, su principal problema es clasificar las formas cuadráticas sobre un cuerpo dado, es decir, establecer condiciones necesarias y suficientes para determinar si dos formas cuadráticas son equivalentes o no.

Antecedentes

Existe una estrecha relación entre la teoría algebraica de formas cuadráticas y la teoría de números; de hecho, tiene sus orígenes en problemas de esta área. A este respecto cabe señalar los trabajos de Pierre Fermat como los pioneros de la teoría moderna de formas cuadráticas (1601-1655).

Por otro lado, a finales del siglo XIX se llegó a establecer que es más sencillo resolver ecuaciones con coeficientes en un cuerpo que en un dominio de integridad que no es un cuerpo y, que un sólido conocimiento del conjunto de soluciones en el cuerpo de fracciones

de un dominio de integridad permite conocer el conjunto de soluciones en el dominio mismo. Considerando esto último, una teoría general de formas cuadráticas con coeficientes racionales fue desarrollada por H. Minkowski en la década de 1880, extendida y completada por H. Hasse en su disertación de 1921.

A principios del siglo XX, con ayuda de la sintaxis dada por el álgebra abstracta y su definición de cuerpo, se pudo extender el estudio de formas cuadráticas sobre cuerpos abstractos gracias al trabajo de E. Artin y O. Schreier en la década de 1920, culminando con la solución dada por Artin del problema 17 de Hilbert: toda función racional semi-definida positiva con coeficientes reales es una suma de cuadrados de funciones racionales.

Así, es natural considerar tales desarrollos como preludio y afirmar que la teoría algebraica de formas cuadráticas inició propiamente con un artículo escrito por E. Witt en 1937, con los siguientes resultados:

1. Todo aspecto formal de la teoría Hasse-Minkowski se mantiene invariable tomando las formas cuadráticas sobre cuerpos de característica diferente de 2.

2. El teorema de cancelación de Witt, que puede ser visto como el "teorema fundamental" en esta área de las matemáticas.

3. La construcción de un anillo conmutativo $W(K)$ cuyos elementos son clases de equivalencia de ciertas formas cuadráticas sobre K.

En los años siguientes, su desarrollo ha sido vigoroso debido principalmente a los trabajos del matemático alemán A. Pfister, quien recogió las ideas fundamentales del trabajo de Witt.

Objetivos

Asumiremos que K es un cuerpo de característica diferente de 2. Son 3 los objetivos trazados en este trabajo:

(1) Definir y describir un espacio cuadrático sobre un cuerpo K en términos de formas bilineales simétricas, expresarlo en su forma diagonal y estudiar su isotropía.

(2) Demostrar el Teorema de Cancelación de Witt y el Teorema de Descomposición de Witt como corolario de este último.

(3) Construir el anillo de Witt $W(K)$ sobre un cuerpo K para estudiar las propiedades de las clases de equivalencia de formas cuadráticas anisótropas sobre el cuerpo en cuestión.

Todas las demostraciones de proposiciones, teoremas, lemas y corolarios se desarrollan equilibrando concisión y detalle.

Capítulo 1

Espacios Cuadráticos

En este capítulo y posteriores, un cuerpo K será de característica diferente de 2, salvo se haga mención de lo contrario. Imponemos esta condición para evitar el siguiente inconveniente: Supongamos que tenemos dos elementos $\alpha, \beta \in K$; entonces, $(\alpha+\beta)^2 = \alpha^2+2\alpha\beta+\beta^2$; si K fuera de característica 2, tendríamos $(\alpha+\beta)^2 = \alpha^2+\beta^2$.

El concepto de espacio cuadrático generaliza el de espacio vectorial con un producto interno, pues este último es una forma bilineal simétrica positiva. Un espacio cuadrático será definido como una pareja (E, B) compuesta por un K-espacio vectorial E de dimensión finita y una forma bilineal simétrica B.

1.1. Relación entre Formas Bilineales Simétricas, Aplicaciones Cuadráticas y Formas Cuadráticas

Empecemos por definir una forma bilineal simétrica.

Definición 1.1. *Sean E un espacio vectorial de dimensión n sobre un cuerpo K y $B : E \times E \longrightarrow K$ una función que cumpla:*

i) $B(u+v, w) = B(u, w) + B(v, w)$ *y* $B(u, v+w) = B(u, v) + B(u, w)$;

ii) $B(\alpha u, v) = \alpha B(u, v)$ *y* $B(u, \beta v) = \beta B(u, v)$;

iii) $B(u, v) = B(v, u)$;

para todos los $u, v \in E$ y $\alpha, \beta \in K$. La función B es llamada forma bilineal simétrica o simplemente fbs.

Nuestro siguiente objetivo es representar matricialmente una *fbs*. Para ello, tomemos una base [ordenada] $\mathscr{B} = (b_1, ..., b_n)$ de E y veamos sus imágenes bajo la forma B. Sea $u \in E$; este vector tiene la forma $u = u_1 b_1 + \cdots + u_n b_n$, con $u_i \in K$, $i = 1, ..., n$; así, podemos identificar E con K^n [en la base canónica] y escribir, para simplificar la notación,

$$u = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}.$$

Ahora, hallemos una matriz que represente a B con respecto a la base fijada $\mathscr{B}$. Sean $u, v \in E$, $u = u_1 b_1 + \cdots + u_n b_n$, $v = v_1 b_1 + \cdots + v_n b_n$; tenemos por la bilinealidad de B, que:

$$\begin{aligned} B(u,v) &= B\left(\sum_{i=1}^{n} u_i b_i, \sum_{j=1}^{n} v_j b_j\right) \\ &= \sum_{i=1}^{n} u_i \sum_{j=1}^{n} v_j B(b_i, b_j) \\ &= \begin{pmatrix} u_1 & \cdots & u_n \end{pmatrix} \cdot \begin{pmatrix} \sum_{j=1}^{n} v_j B(b_1, b_j) \\ \vdots \\ \sum_{j=1}^{n} v_j B(b_n, b_j) \end{pmatrix} \\ &= \begin{pmatrix} u_1 & \cdots & u_n \end{pmatrix} \cdot \begin{pmatrix} B(b_1,b_1) & \ldots & B(b_1,b_n) \\ \vdots & \ddots & \vdots \\ B(b_n,b_1) & \ldots & B(b_n,b_n) \end{pmatrix} \cdot \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}; \end{aligned}$$

es decir,

$$B(u,v) = u^T \cdot M_B \cdot v, \tag{1.1}$$

donde M_B está determinada *unívocamente* y es simétrica, pues $B(b_i, b_j) = B(b_j, b_i)$, para $i, j = 1, ..., n$. Esta observación nos permite establecer la siguiente definición.

Definición 1.2. *Sea B una fbs definida en un espacio vectorial E de dimensión finita n y sea $\mathscr{B} = (b_1, ..., b_n)$ una base de E. Definimos la matriz de B en la base $\mathscr{B}$ como*

$$M_B = [B(b_i, b_j)].^{1} \tag{1.2}$$

Consecuencia de la bilinealidad y simetría de la *fbs* B, obtenemos la identidad:

$$B(u+v, u+v) = B(u,u) + B(v,v) + 2B(u,v); \text{ y así,}$$

$$B(u,v) = \frac{1}{2}[B(u+v, u+v) - B(u,u) - B(v,v)] \tag{1.3}$$

para cualesquiera $u, v \in E$. Esta igualdad es conocida como la *identidad polar*. Vemos, gracias a ella, que la forma B está determinada completamente por los valores que ésta toma en la diagonal $E \times E$. Así, la misma *fbs* B es, en cierto sentido, "diagonal"; y efectivamente, en el siguiente capítulo veremos que ella adopta una forma diagonal.

Definición 1.3. *Sean E un K-espacio vectorial de dimensión finita. Si $q : E \longrightarrow K$ es una aplicación que verifica:*

i) $q(\alpha v) = \alpha^2 q(v)$, $\forall \alpha \in K$, $v \in E$;

[1] Para ser más precisos, podemos denotar la matriz M_B por $M_{(B,\mathscr{B})}$. Esta notación es útil cuando se tiene dos bases diferentes para definir dos diferentes matrices de una *fbs*.

ii) la correspondencia $(v,w) \longmapsto q(v+w)-q(v)-q(w)$ *es una aplicación bilineal de* $E \times E$ *a* K.

Entonces, llamamos a q *una aplicación cuadrática sobre* E.

Notemos lo siguiente: toda *fbs* $B : E \times E \longrightarrow K$ determina de forma única una aplicación cuadrática $q = q_B : E \longrightarrow K$ definida por la ecuación

$$q(v) = B(v,v). \tag{1.4}$$

Recíprocamente, toda aplicación cuadrática $q : E \longrightarrow K$ define una *fbs* $B = B_q : E \times E \longrightarrow K$ por

$$B(v,w) = \frac{1}{2}(q(v+w)-q(v)-q(w)). \tag{1.5}$$

De las ecuaciones 1.1 y 1.4 deducimos que, dada una base $\mathscr{B} = (b_1,...,b_n)$ de E, con $v = v_1 b_1 + \cdots + v_n b_n$,

$$q(v) = B(v,v) = v^T \cdot M_B \cdot v = \sum_{i,j=1}^{n} v_i v_j \beta_{ij},$$

donde $\beta_{ij} \in K$ con $i,j = 1,...,n$; es decir q o equivalentemente B, en una base $\mathscr{B}$, toma la forma de un polinomio homogéneo de grado 2 en n "indeterminadas" $v_1,...,v_n$ con $\beta_{ij} = \beta_{ji}$.

Definición 1.4. *Una forma cuadrática* f *de grado* n *sobre un cuerpo* K *es un polinomio homogéneo de grado* 2 *en* n *variables, es decir,*

$$f(X_1,...,X_n) = \sum_{i,j=1}^{n} \alpha_{ij} X_i X_j, \tag{1.6}$$

donde $\alpha_{ij} \in K$, *para* $i,j = 1,...,n$.[2]

Si f es una forma cuadrática de grado n sobre K, nos referiremos a ella también como una K-forma de grado n, o como una K-forma de dimensión n.

En la igualdad de la ecuación 1.6, no necesariamente ocurre que $\alpha_{ij} = \alpha_{ji}$ para $i,j = 1,...,n$. Sin embargo, escribiendo $\beta_{ij} = \frac{1}{2}(\alpha_{ij} + \alpha_{ji})$ tenemos:

$$f(X_1,...,X_n) = \sum_{i,j=1}^{n} \beta_{ij} X_i X_j, \tag{1.7}$$

con $\beta_{ij} = \beta_{ji}$. En notación matricial, dado

$$X = \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix},$$

[2] En adelante, denotaremos las n variables $X_1,...,X_n$ por X, es decir, $f(X) = f(X_1,...,X_n)$. Usaremos también la notación matricial $X = \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix}$.

se cumple

$$f(X) = X^T \cdot M_f \cdot X,$$

donde $M_f = [\beta_{ij}]$ es una matriz $n \times n$ simétrica con coeficientes en K.

Veamos ahora la relación de equivalencia de K-formas, con la ayuda de matrices invertibles (y claro, las transformaciones lineales inducidas por estas). Luego, mostraremos que a cada clase de equivalencia de K-formas corresponde una única clase de equivalencia de espacios cuadráticos (que definiremos un poco más adelante).

Definición 1.5. *Sean f y g K-formas de grado n. Decimos que f es equivalente a g y escribiremos $f \cong g$, si existe una matriz $A \in GL_n(K)$ tal que se cumple la igualdad:*

$$f(X) = g(AX). \tag{1.8}$$

Mostremos que $\cong$ es una relación de equivalencia en la colección de las K-formas de grado n, que denotaremos por $F(K)$:

Reflexividad. $f(X) = f(IX)$, luego $f \cong f$.

Simetría. Si $f \cong g$, entonces $f(X) = g(AX)$, con A invertible; y como consecuencia, $g(Y) = g(A(A^{-1}Y)) = f(A^{-1}Y)$, es decir, $g \cong f$.

Transitividad. Si $f \cong g$ y $g \cong h$, $f(X) = g(AX)$ y $g(Y) = h(BY)$, con $A, B \in GL_n(K)$, entonces $f(X) = g(AX) = h(B(AX)) = h((BA)X)$, es decir, $f \cong h$, pues $BA \in GL_n(K)$.

Sea ahora B una *fbs* sobre E, entonces ella define de forma única una aplicación cuadrática q_B de E en K; tomando una base $\mathscr{B} = (b_1, ..., b_n)$ de E, $q = q_B$ define unívocamente una K-forma de grado n $f = f_B$ dada por la ecuación:

$$B(x,x) = q(x) = \sum_{i,j=1}^{n} x_i x_j B(b_i, b_j) = \sum_{i,j=1}^{n} \beta_{ij} x_i x_j = f(x_1, ..., x_n) = f(x);$$

donde $x = \sum x_i b_i$ y $B(b_i, b_j) = \beta_{ij}$, con $i, j = 1, ..., n$. Veamos qué ocurre con la matriz de B cuando tomamos otra base de E y, las K- formas inducidas por ellas.

Proposición 1.1. *Sea B una fbs sobre E y sean M_B y M'_B matrices de B en las bases $\mathscr{B} = (b_1, ..., b_n)$ y $\mathscr{B}' = (b'_1, ..., b'_n)$, respectivamente. Sean:*

$$f(X) = X^T M_B X \quad y \quad g(Y) = Y^T M'_B Y.$$

Entonces $f \cong g$.

Demostración. Sea $\mathrm{p} = [p_{ij}]$ la matriz cambio de base de $\mathscr{B}$ a $\mathscr{B}'$, definida por las ecuaciones:

$$b'_j = \sum_{i=1}^{n} p_{ij} b_i = P b_j; \quad j = 1, ..., n;$$

donde $P : E \longrightarrow E$ es el operador cuya matriz es p en las bases dadas. Sea $X = X_1 b_1 + \cdots + X_n b_n$; notemos lo siguiente: $PX = P(X_1 b_1 + \cdots + X_n b_n) = X_1 P b_1 + \cdots + X_n P b_n = X_1 b'_1 +$

$\cdots + X_n b'_n$. Entonces, X tiene la misma representación *matricial* en ambas bases. Ahora, tenemos lo siguiente:

$$\begin{aligned} g(X) &= X^T M'_B X \\ &= X^T [B(b'_i, b'_j)] X \\ &= X^T \left[B\left(\sum_{k=1}^{n} p_{ki} b_k, \sum_{r=1}^{n} p_{rj} b_r \right) \right] X \\ &= X^T \left[\sum_{k=1}^{n} \sum_{r=1}^{n} p_{ki} p_{rj} B(b_k, b_r) \right] X \\ &= X^T \mathrm{p}^T [B(b_k, b_r)] \mathrm{p} X \\ &= (\mathrm{p}X)^T M_B \mathrm{p}X \\ &= f(\mathrm{p}X); \end{aligned}$$

que es por definición, $g \cong f$. □

Por tanto, dos bases diferentes de E generan dos K-formas equivalentes. Así, una *fbs* B determina una clase de equivalencia (f_B).

Ya queda evidente la relación entre formas cuadráticas, formas bilineales simétricas y aplicaciones cuadráticas: La matriz de una *fbs* sobre un espacio vectorial E de dimensión n, en una base dada, define una K-forma de dimensión n, de hecho, la clase de equivalencia de una forma cuadrática dada es correspondida de forma única con una *fbs* .

Llegados a este punto, podemos establecer la definición primaria de este capítulo.

Definición 1.6. *Definimos un n-espacio cuadrático (o espacio cuadrático) como una pareja (E, B) compuesta por un K-espacio vectorial E de dimensión n y una fbs $B : E \times E \longrightarrow K$.*

Denotaremos el espacio cuadrático E provisto de la *fbs* B también por (E, q), donde q es la aplicación cuadrática inducida por B (es decir, $q = q_B$). Si la forma B es clara en un contexto dado, denotaremos (E, B) simplemente por E.

Luego de todas estas observaciones y definiciones, queda justificado el uso indiscriminado de cualesquiera de las anteriores definiciones para determinar un espacio cuadrático: una pareja constituida por un K-espacio vectorial y una *fbs* o una aplicación cuadrática.

Más adelante estudiaremos la equivalencia de espacios cuadráticos por isometrías y veremos que las clases inducidas por esta están relacionadas directamente con las clases de equivalencia de las K-formas asociadas a estos espacios.

Veremos ahora ejemplos concretos de espacios cuadráticos.

1.1.1. Ejemplos

Ejemplo **1.1.** *El espacio euclidiano $\mathbb{R}^n$ y el producto interno usual $\langle\ ,\ \rangle$ constituyen un espacio cuadrático $(\mathbb{R}^n, \langle\ ,\ \rangle)$. Más general, un espacio vectorial V de dimensión finita provisto de un producto interno $\langle\ ,\ \rangle$, viene siendo un espacio cuadrático $(V, \langle\ ,\ \rangle)$ en el sentido de la definición 1.6.*

Sea $X=(X_1,...,X_n)\in\mathbb{R}^n$ en la base canónica, entonces, como es sabido, $\langle X,X\rangle = X_1^2+\cdots+X_n^2=f(X_1,...,X_n)$, es una $\mathbb{R}$-forma de dimensión n. Su matriz en la base canónica es $[\langle e_i,e_j\rangle]=[\delta_{ij}]=I$, es decir,

$$\langle X,X\rangle=(X_1,...,X_n)\cdot I\cdot\begin{pmatrix}X_1\\ \vdots\\ X_n\end{pmatrix}=(X_1,...,X_n)\cdot\begin{pmatrix}X_1\\ \vdots\\ X_n\end{pmatrix}=X^T\cdot X.$$

Sea $n=2$, y sea $\mathscr{B}=((1,1),(-1,2))$, la matriz cambio de base de la canónica a $\mathscr{B}$ es $P=\begin{pmatrix}1&-1\\1&2\end{pmatrix}$; definamos $g(X)=X^TP^TPX$, entonces, es claro que esta forma será equivalente a la forma $f(X)=X_1^2+X_2^2$. Veamos su ecuación:

$$\begin{aligned}g(X)=X^TP^TPX&=(X_1,X_2)\begin{pmatrix}1&1\\-1&2\end{pmatrix}\begin{pmatrix}1&-1\\1&2\end{pmatrix}\begin{pmatrix}X_1\\X_2\end{pmatrix}\\&=(X_1,X_2)\begin{pmatrix}2&1\\1&5\end{pmatrix}\begin{pmatrix}X_1\\X_2\end{pmatrix}=2X_1^2+2X_1X_2+5X_2^2,\end{aligned}$$

así, $X_1^2+X_2^2\sim 2X_1^2+2X_1X_2+5X_2^2$.[3]

Ejemplo **1.2.** *(E,B) donde $B\equiv 0$ es la fbs 0, a este espacio lo denotaremos por $(E,B)=0$ y nos referiremos a él como el espacio cero.*[4]

Ejemplo **1.3.** *Definimos la forma cuadrática h por $h(X_1,X_2)=X_1X_2$, con $X_1,X_2\in K$.*

Hallemos la matriz de h: $X_1X_2=0X_1^2+\frac{1}{2}X_1X_2+\frac{1}{2}X_2X_1+0X_2^2=X_1(0X_1+\frac{1}{2}X_2)+X_2(\frac{1}{2}X_1+X_2)$, entonces

$$h(X_1,X_2)=(X_1,X_2)\begin{pmatrix}0&1/2\\1/2&0\end{pmatrix}\begin{pmatrix}X_1\\X_2\end{pmatrix}.$$

Sea $(X_1,X_2)\longmapsto(X_1+X_2,X_1-X_2)$ un cambio de coordenadas definido por la matriz (simétrica de hecho) $A=\begin{pmatrix}1&1\\1&-1\end{pmatrix}$, entonces $h'(X_1,X_2)=h(A(X_1,X_2))=h(X_1+X_2,X_1-X_2)=(X_1+X_2)(X_1-X_2)=X_1^2-X_2^2$ es equivalente a X_1X_2. Notemos lo siguiente:

$$(X_1,X_2)\ A^T\begin{pmatrix}0&1/2\\1/2&0\end{pmatrix}A\begin{pmatrix}X_1\\X_2\end{pmatrix}=(X_1,X_2)\begin{pmatrix}1&0\\0&-1\end{pmatrix}\begin{pmatrix}X_1\\X_2\end{pmatrix}=X_1^2-X_2^2=h'(X_1,X_2),$$

es decir, $M_{h'}=A^T\cdot M_h\cdot A$.

---

[3] Note la facilidad de utilizar formas cuadráticas en vez de *fbs*, puesto que el concepto de *fbs* es más abstracto que el de forma cuadrática.

[4] Sería más preciso decir que es el n-espacio 0, y denotarlo por 0_n, pero, para cada dimensión n, este espacio tiene las mismas propiedades.

1.2. Isometrías

Hemos construido ya una estructura algebraica (E,B) dados E un K-espacio vectorial de dimensión finita y B una *fbs*. Se puede hacer un estudio categórico de estas estructuras; sin embargo, ahora solamente realizaremos un estudio de carácter introductorio de los morfismos entre estas.

Definición 1.7. *Sean (E,B), (E',B') n-espacios cuadráticos sobre un cuerpo K. Decimos que ellos son isométricos, denotando por $(E,B)\cong(E',B')$,[5] si existe una transformación lineal invertible $T:E\longrightarrow E'$ cumpliendo*

$$B'(T(v),T(w))=B(v,w),\ \forall v,w\in E. \tag{1.9}$$

T es llamada isometría.

Note que $\cong$ es una relación de equivalencia en la colección de espacios cuadráticos, la que denotaremos por $M_0(K)$. Si (E,B) es un n-espacio cuadrático, denotamos su clase de equivalencia por $\langle(E,B)\rangle$.

Proposición 1.2. *$(E,B)\cong(E',B')\Longleftrightarrow f_B\cong f_{B'}$, donde f_B y $f_{B'}$ son inducidas por B y B', en dos bases $\mathscr{B}$ y $\mathscr{B}'$ de E y E', respectivamente. En otras palabras, a cada clase de isometría de espacios cuadráticos le corresponde una única clase de equivalencia de formas cuadráticas.*

Demostración. ($\Rightarrow$) Supongamos que $(E,B)\cong(E',B')$. Entonces, dado $x\in E$ se tiene $B'(Tx,Tx)=B(x,x)$, donde $T:E\longrightarrow E'$ es una isometría. Escrito de otro modo, $f_{B'}(Tx)=f_B(x)$, es decir, $f_B\cong f_{B'}$. ($\Leftarrow$) Puesto que f_B y $f_{B'}$ son las K-formas inducidas por B y B', respectivamente, el recíproco es simplemente el anterior argumento invertido. □

Así, existe una correspondencia biyectiva entre las clases de isometría de n-espacios cuadráticos y las clases de equivalencia de las formas cuadráticas de grado n. Claro, esto era de esperarse.

Una cuestión natural es: Dado un espacio cuadrático (E,B), ¿qué propiedades tiene este, cuando M_B es invertible? Mostraremos algunas de estas en la siguiente subsección.

1.2.1. Regularidad

Sea (E,B) un n-espacio cuadrático y sea M_B una matriz asociada a B en alguna base $\mathscr{B}=(b_1,...,b_n)$ de E, que a su vez define una K-forma $f(X)=X^TM_BX$ de grado n.

Proposición 1.3. *Son equivalentes:*

(1) M_B es una matriz invertible (no singular).

(2) $v\longmapsto B(\ ,v)$ define un isomorfismo $\varphi:E\longrightarrow E^*$.

[5] Usamos el mismo símbolo "$\cong$" para denotar la equivalencia de formas cuadráticas y para la isometría de espacios cuadráticos. La proposición 1.2 justificará este abuso de notación.

(3) Dado $v \in E$, si $B(v,w)=0$ para todo $w \in E$, entonces $v=0$.

Demostración. (1) $\Rightarrow$ (2) Supongamos que M_B es invertible. Sabemos que E^* es de dimensión $1 \times n = n$, entonces, basta probar que el conjunto $A=\{B(\ ,b_1),...,B(\ ,b_n)\}$, cuyos elementos son funcionales lineales de E a K, es linealmente independiente y genera E^*. Tomemos $X^T=(\alpha_1 \ \cdots \ \alpha_n)$, con $\alpha_i \in K$, $i=1,...,n$; y sea

$$C=\alpha_1 B(\ ,b_1)+\cdots+\alpha_n B(\ ,b_n)\equiv 0$$

una combinación lineal de los elementos de A. Para todo $v \in E$, $C(v)=0$, en particular, para los elementos básicos b_i, $i=1,...,n$. Entonces,

$$\begin{aligned} 0=C(b_1)&=\alpha_1 B(b_1,b_1)+\cdots+\alpha_n B(b_1,b_n),\\ &\vdots\\ 0=C(b_i)&=\alpha_1 B(b_i,b_1)+\cdots+\alpha_n B(b_i,b_n),\\ &\vdots\\ 0=C(b_n)&=\alpha_1 B(b_n,b_1)+\cdots+\alpha_n B(b_n,b_n); \end{aligned}$$

matricialmente es $M_B X=0$, entonces es $X=0$, es decir, $\alpha_1=\cdots=\alpha_n=0$. Luego los elementos de A son linealmente independientes. Por otra parte, es claro que A genera E^*, para ello basta observar que $S(A)$, el subespacio de E^* generado por A, es de dimensión n. Entonces, $\varphi : E \longrightarrow E^*$ definida por $\varphi(v)=B(\ ,v)$, es un isomorfismo. *(2) $\Rightarrow$ (3)* Supongamos ahora que φ es un isomorfismo. Entonces, dado $v \in E$, tal que $B(w,v)=0$, para todo $w \in E$, significa que $\varphi(v)=B(\ ,v)\equiv 0$, entonces $v \in \ker\varphi$, luego $v=0$. *$\sim$ (1) $\Rightarrow$ $\sim$ (3)* Para concluir la demostración, supongamos que M_B es singular, entonces existen escalares $\alpha_1,...,\alpha_n \in E$, no todos cero, tales que $M_B X=0$, donde $X=\begin{pmatrix}\alpha_1\\ \vdots \\ \alpha_n\end{pmatrix}$. Dado $w \in E$, $w=\beta_1 b_1+\cdots+\beta_n b_n$, y su representación matricial $Y^T=(\beta_1 \ \cdots \ \beta_n)$, tenemos $Y^T M_B X = Y^T \cdot 0 = 0$. En notación vectorial, esto significa que $0 \neq v=\alpha_1 b_1+\cdots+\alpha_n b_n$ es tal que, para todo $w \in E$, $B(w,v)=0$. □

Con las equivalencias establecidas por la anterior proposición, podemos definir la regularidad de un espacio dado.

Definición 1.8. *(E,B) es llamado regular si cumple cualquiera de las equivalencias de la proposición 1.3. Decimos también que f_B es una K-forma de grado n no singular, o también regular; de manera similar para sus equivalentes B y q.*[6]

Definición 1.9. *Sea (E,B) un espacio cuadrático de dimensión n, y sea S un subespacio vectorial de E de dimensión m. Entonces, queda definido el espacio cuadrático $(S, B|_{S\times S})$ de dimensión m. Decimos que S es un subespacio cuadrático de E (o simplemente subespacio, cuando se considera en E la estructura de espacio cuadrático) y lo denotamos por $S \leq E$.*

[6] El espacio cuadrático $\mathbf{0}$ satisface solamente *(2)*; aún así, lo llamaremos regular.

Definición 1.10. *Sea (E,B) un espacio cuadrático, y sea $S \leq E$. El complemento ortogonal de S en E es definido por*

$$S^{\perp} = \{v \in E; B(v,S) = 0\},$$

donde $B(v,S) = \{B(v,w) \in K; w \in S\}$ contiene solo al vector 0.

Es fácil ver que $S^{\perp}$ es un subespacio de E. En efecto: si $u, v \in S^{\perp}$, $B(u+v,S) = B(u,S) + B(v,S) = 0$, luego $u+v \in S^{\perp}$ y, dado $\kappa \in K$, $B(\kappa u, S) = \kappa B(u,S) = 0$, entonces $\kappa u \in S^{\perp}$.

Definición 1.11. *Sea $S = E$; entonces, $E^{\perp} = \{v \in E; B(v,E) = 0\}$ es llamado el radical de (E,B) y es denotado por $\mathrm{rad}E$.*

Note que (E,B) es regular si, y solo si, $\mathrm{rad}E = \{0\}$.[7]

Ejemplo **1.4.** *Todo espacio vectorial con producto interno es regular, esto se sigue directamente de la definición de producto interno.*

Proposición 1.4. *Sean E un espacio cuadrático y S un subespacio de E. Entonces $\mathrm{rad}S = S \cap S^{\perp}$.*

Demostración. Tenemos lo siguiente: $\mathrm{rad}S = \{x \in S; B(x,S) = 0\} = S \cap S^{\perp}$. □

La siguiente proposición nos mostrará en qué sentido $S^{\perp}$ es ortogonal a $S \leq E$ cuando E *es regular.*

Proposición 1.5. *Sea (E,B) un n-espacio cuadrático regular, y sea $S \leq E$. Entonces*

(1) $\dim S + \dim S^{\perp} = E$.

(2) $(S^{\perp})^{\perp} = S$.

Demostración. (1) Por la regularidad de (E,B), existe un isomorfismo $\varphi : E \longrightarrow E^*$,

$$\begin{aligned} v \longmapsto \varphi_v : E &\longrightarrow K \\ w &\longmapsto \varphi_v(w) = B(v,w); \end{aligned}$$

este cumple $\varphi(S) \cong S^*$ (como espacios vectoriales). Definimos un nuevo morfismo $\xi : E^* \longrightarrow S^*$, como

$$\xi(\varphi_v) = \varphi_v|_S : S \longrightarrow K.$$

Sea $\varphi_v \in \ker \xi$, entonces $\varphi_v|_S \equiv 0$, es decir, para todo $w \in S$, $0 = \varphi_v(w) = B(v,w)$, es decir, $v \in S^{\perp}$ o $\varphi_v \in \varphi(S^{\perp})$. Este argumento es de ida y vuelta. Luego $\ker \xi = \varphi(S^{\perp})$. Ahora, notemos que todos los elementos de S^* son de la forma $\varphi_v|_S$, entonces ξ es suryectiva; dicho de otro modo, $\xi(E^*) = S^*$. Por el Teorema del Núcleo e Imagen, tenemos

$$\begin{aligned} \dim E = \dim E^* &= \dim \ker \xi + \dim \xi(E^*) \\ &= \dim \varphi(S^{\perp}) + \dim S^* \\ &= \dim S^{\perp} + \dim S. \end{aligned}$$

[7] Si (E,B) es regular, no necesariamente se tiene que $S \leq E$ sea regular, pues puede ocurrir, por ejemplo, que $B|_{S \times S} \equiv 0$.

(2) Aplicando la parte *(1)* dos veces, tenemos $\dim(S^\perp)^\perp = \dim E - \dim S^\perp = \dim E - (\dim E - \dim S) = \dim S$. Por otra parte, $w \in S$ si, y solo si, $B(w, S^\perp) = 0$ si, y solo si, $w \in (S^\perp)^\perp$; así, $S = (S^\perp)^\perp$. Esto concluye la demostración. □

Si (E, B) no es regular y $S \leq E$ es un subespacio de E, entonces la igualdad $\dim E = \dim S + \dim S^\perp$ no necesariamente se cumple. Veamos.

Ejemplo **1.5.** *Sea $E = K^2$ y B la fbs cuya matriz en la base canónica es $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. Sea $S = K \cdot e_2$. Entonces, dado $v = v_1 e_1 + v_2 e_2$ un vector de E y $w = k e_2 \in S$, tenemos que $B(v, w) = B(v_1 e_1 + v_2 e_2, k e_2) = k v_1 B(e_1, e_2) + k v_2 B(e_2, e_2) = k v_1 \cdot 0 + k v_2 \cdot 0 = 0$. Luego $S^\perp = E$ y*

$$\dim E < \dim E + \dim S = \dim S^\perp + \dim S,$$

pues $\dim S = 1$.

Al definir la ortogonalidad de un subespacio de un espacio cuadrático, introducimos en este una noción de geometría. Entonces, de forma natural, se puede considerar la ortogonalidad de dos vectores dados en E, vía su *fbs* B.

1.2.2. Ortogonalidad

Definición 1.12. *Sea (E, B) un espacio cuadrático y sean $v, w \in E$. Decimos que v es ortogonal a w, si $B(v, w) = 0$.*

Definición 1.13. *Sean (E, B) un n-espacio cuadrático y $\mathscr{B} = (b_1, ..., b_n)$ una base de E. Decimos que $\mathscr{B}$ es una base ortogonal si para $i, j = 1, ..., n$ e $i \neq j$, $B(b_i, b_j) = 0$.*

Proposición 1.6. *Todo espacio cuadrático (E, B) tiene una base ortogonal.*

Demostración. Sea E un K-espacio vectorial de dimensión finita, entonces podemos escribir $E = \mathrm{rad}E \oplus F$ (basta tomar una base de $\mathrm{rad}E$ y extenderla a una de E). El subespacio cuadrático (F, B'), donde $B' = B|_{F \times F}$ es la restricción de la forma B a F es regular pues, si dado $x \in F$ satisfaciendo $B'(x, F) = 0$ y, dado $y \in E$, que se escribe de forma única $y = u + v$ con $u \in \mathrm{rad}E$ y $v \in F$, se tiene $B(x, y) = B(x, u + v) = B(x, u) + B(x, v) = B(x, u) + B'(x, v) = 0$, entonces $x \in \mathrm{rad}E$, luego $x \in \mathrm{rad}E \cap F$, es decir, $x = 0$. Así, es suficiente demostrar la proposición para E regular, pues tendríamos una base para F que se puede completar a una base de $\mathrm{rad}E$, cuyos elementos ya son dos a dos ortogonales y serán [dos a dos] ortogonales a los elementos de F. Supongamos entonces que E es regular. Demostraremos la proposición por inducción sobre la dimensión de E. Si $\dim E = 1$, es trivial la conclusión. Supongamos que la proposición se cumple para todo espacio de dimensión n y sea E de dimensión $n + 1$. Por la ecuación 1.3, B está determinada por sus valores en la diagonal $E \times E$ y, por la regularidad de E, existe $0 \neq v \in E$ tal que $B(v, v) \neq 0$. Vamos a descomponer $E = K \cdot v \oplus (K \cdot v)^\perp$, donde $(K \cdot v)^\perp$ será de dimensión n; esto nos permitirá aplicar la hipótesis de inducción a $(K \cdot v)^\perp$ y la base obtenida para este subespacio será extendida a una base de E añadiéndole v que, por definición será ortogonal a todo elemento básico de

$(K\cdot v)^{\perp}$. Primero probemos que $(K\cdot v)^{\perp}$ es regular. Las siguientes igualdades se siguen de la regularidad de E y la proposición 1.4:

$$\begin{aligned}\mathrm{rad}(K\cdot v)^{\perp} &= (K\cdot v)^{\perp}\cap((K\cdot v)^{\perp})^{\perp}\\ &= (K\cdot v)^{\perp}\cap K\cdot v\\ &= \mathrm{rad}K\cdot v\\ &= 0;\end{aligned}$$

pues, $K\cdot v$ es regular (esto se sigue inmediatamente de la definición de $K\cdot v$; recuerde que $B(v,v)\neq 0$ y todo elemento de $K\cdot v$ es de la forma αv). Luego $(K\cdot v)^{\perp}$ es regular. Vemos también que $K\cdot v\cap(K\cdot v)^{\perp}=0$. Por último, si $x\in E$, es posible escribirlo de forma única como suma de dos vectores $x=u+w$, donde $u\in K\cdot v$ y $w\in(K\cdot v)^{\perp}$. Veamos: sean $u=\dfrac{B(x,v)}{B(v,v)}v\in K\cdot v$ y $w=x-\dfrac{B(x,v)}{B(v,v)}v$; afirmamos que $w\in(K\cdot v)^{\perp}$. En efecto,

$$B(w,v)=B\left(x-\frac{B(x,v)}{B(v,v)}v,v\right)=B(x,v)-B\left(\frac{B(x,v)}{B(v,v)}v,v\right)=B(x,v)-\frac{B(x,v)}{B(v,v)}B(v,v)=0.$$

Así, $E\subseteq K\cdot v\oplus(K\cdot v)^{\perp}$, de donde $E=K\cdot v\oplus(K\cdot v)^{\perp}$. □

En la anterior demostración, "proyectamos" x sobre el vector v.

Definición 1.14. *Dados $v\in E$ con $B(v,v)\neq 0$ y $x\in E$, definimos la proyección ortogonal de x sobre v por la igualdad*

$$\mathrm{proy}_{v}(x)=\frac{B(x,v)}{B(v,v)}v.$$

La proyección ortogonal sobre un vector v no necesariamente está definida cuando tenemos solamente que $v\neq 0$; necesitamos que sea $B(v,v)\neq 0$. Estudiaremos estos vectores (a los que llamaremos anisótropos) en la siguiente sección.

1.3. Isotropía

Un problema importante a ser resuelto en este trabajo es determinar las condiciones para que una K-forma f de grado n represente no trivialmente al 0, es decir, encontrar elementos $X_i\in K$ no todos cero tales que $f(X_1,...,X_n)=0$ o equivalentemente, hallar un vector $v\in E$ no cero tal que la *fbs* B dada por la clase (f), cumpla $B(v,v)=0$.

Definición 1.15. *Sea v un vector no nulo en un espacio cuadrático (E,B). Decimos que v es un vector isótropo si $B(v,v)=0$, y decimos que es anisótropo si $B(v,v)\neq 0$. Análogamente, dada una K-forma f de grado n, decimos que es isótropa si existen $X_1,...,X_n\in K$ no todos cero, tales que $f(X_1,...,X_n)=0$. El espacio cuadrático (E,B) es llamado isótropo si contiene al menos un vector isótropo, y es llamado anisótropo si todos sus vectores no nulos son anisótropos.*

Note que si (E,B) es anisótropo, entonces es regular.

Ejemplo **1.6.** (E,B), *donde* E *es cualquier* K*-espacio vectorial y* $B\equiv 0$ *es la forma cero, es llamado totalmente isótropo.*

Ejemplo **1.7.** $\mathbb{R}^n$ *con el producto interno usual, es un espacio anisótropo.*

Ejemplo **1.8.** *Sea* $f(X_1,X_2,X_3)=X_1X_2+X_3^2$, *con* $X_i\in\mathbb{R}$. *Matricialmente*

$$f(X)=(X_1,X_2,X_3)\cdot\begin{pmatrix}0 & 1/2 & 0\\ 1/2 & 0 & 0\\ 0 & 0 & 1\end{pmatrix}\cdot\begin{pmatrix}X_1\\ X_2\\ X_3\end{pmatrix},$$

notamos que f *es regular, sin embargo,* $f(1.-1,1)=1(-1)+1^2=0$, *por tanto* f *es isótropa. Luego el espacio* $(\mathbb{R}^3,B_f)$ *donde* B_f *es la fbs en la base canónica, inducida por* f, *es regular isótropo.*

Sean f y g K-formas. Es fácil demostrar que si $f\cong g$ entonces f isótropa implica g isótropa (suficiente observar que $f(X)=g(AX)$, con A no singular). Vemos entonces que la isotropía de una forma f es una propiedad de la clase (f). Propiedades de esta naturaleza son las que nos interesan en este estudio.

Capítulo 2

Diagonalización

Breves observaciones antes del desarrollo principal de este capítulo: Sea f una K-forma de grado n. Vimos en el anterior capítulo que f puede escribirse como $f(X) = \sum_{i=1}^{n} \beta_{ij} X_i X_j$, donde $M_f = [\beta_{ij}]$ es una matriz simétrica. Sea (f) la clase de K-formas de grado n equivalentes a f. Esta, como vimos, tiene una correspondiente clase de isometría de espacios cuadráticos $\langle(E,B)\rangle$; un representante es el siguiente: (K^n, B), donde $B(e_i, e_j) = \beta_{ij}$, es decir, la matriz de B en la base canónica es precisamente M_f. Si $(E,B_0) \in \langle(K^n,B)\rangle$, entonces, dada una base $\mathscr{B} = (b_1,...,b_n)$ de E, definimos la isometría $\tau : E \longrightarrow K^n$ con los valores $\tau(b_i) = e_i$, $i = 1,...,n$; así, en la base $\mathscr{B}$ de E, la matriz de B_0 será también M_f. Entonces, podemos trabajar simplemente en (K^n, B).

En este capítulo, dada f, una K-forma cuadrática de grado n y su correspondiente clase (f), hallaremos un representante que pueda expresarse de la manera más simple posible, pues esto nos facilitará estudiar las propiedades de la clase. En otras palabras, diagonalizaremos la forma f, aplicando algunas propiedades de los elementos no nulos de K. Para ello, dado un espacio (E,B) en la clase de isometrías correspondiente a (f), hallaremos una base $\mathscr{B}$ en la que la matriz de B es diagonal.

Recordemos que $\dot{K} = (K - \{0\}, \cdot)$ es el grupo multiplicativo subyacente del cuerpo K.

Definición 2.1. *Sea f una K-forma de grado n, y $\kappa \in \dot{K}$. Decimos que κ es representado por f si existen $X_1,...,X_n \in K$ tales que $f(X_1,...,X_n) = \kappa$. Escribimos $D_K(f) = D(f)$ para denotar la colección de elementos en $\dot{K}$ representados por f.*

Si (E,B) es un espacio cuadrático representante de la clase de isometría correspondiente a (f), entonces

$$D(f) = \{\kappa \in \dot{K};\ \exists v \in E,\ B(v,v) = \kappa\}.^{1}$$

Notemos que los elementos representados por f tienen como preimágenes a los vectores anisótropos de (E,B).

Proposición 2.1. *$\kappa \in D(f)$ si, y solo si, para todo $\alpha \in \dot{K}$, $\alpha^2\kappa \in D(f)$.*

Demostración. ($\Rightarrow$) Sean $\kappa \in D(f)$ y $\alpha \in \dot{K}$; entonces existe $0 \neq v \in E$ tal que $q(v) = q_B(v) = \kappa$. El vector $w = \alpha v \in E$ cumple $q(w) = q(\alpha v) = \alpha^2 q(v) = \alpha^2\kappa$ luego $\alpha^2\kappa \in D(f)$. ($\Leftarrow$) Basta tomar $\alpha = 1$. □

[1] También denotaremos a $D(f)$ por $D(E)$ cuando el contexto esté claro.

Dicho de otro modo, $D(f)$ absorbe todos los cuadrados de K y los multiplica por sus representantes, cuando f es no trivial, es decir, los elementos $\kappa \in D(f)$ determinan clases laterales módulo $\dot{K}^2 = \{\alpha^2; \alpha \in \dot{K}\}$, que es normal en $\dot{K}$. Entonces, los elementos de $D(f)$ se encuentran en relación biunívoca con un subconjunto del cociente $\dot{K}/\dot{K}^2$, al que llamaremos *grupo de clases de cuadrados*.

2.1. Suma Ortogonal

Vamos a definir la primera operación para la construcción de un anillo de Witt, la suma ortogonal de espacios cuadráticos.

Si (E_1, B_1) y (E_2, B_2) son espacios cuadráticos, podemos definir una *fbs* B sobre $E_1 \oplus E_2$ de la siguiente manera: $B((u_1,u_2),(v_1,v_2)) = B_1(u_1,v_1) + B_2(u_2,v_2)$, es, efectivamente, una *fbs*:

$$\begin{aligned} B((u_1,u_2),(v_1,v_2)+\alpha(w_1,w_2)) &= B((u_1,u_2),(v_1+\alpha w_1, v_2+\alpha w_2)) \\ &= B_1(u_1, v_1+\alpha w_1) + B_2(u_2, v_2+\alpha w_2)) \\ &= B_1(u_1,v_1) + B_1(u_1,\alpha w_1) + B_2(u_2,v_2) + B_2(u_2,\alpha w_2) \\ &= B_1(u_1,v_1) + B_2(u_2,v_2) + \alpha B_1(u_1,w_1) + \alpha B_2(u_2,w_2) \\ &= B((u_1,u_2),(v_1,v_2)) + \alpha B((u_1,u_2),(w_1,w_2)); \end{aligned}$$

análogamente en la primera coordenada. La simetría es más bien fácil de probar.

Definición 2.2. *Sean (E_1, B_1), (E_2, B_2) espacios cuadráticos de dimensiones m y n, respectivamente. Sean $E = E_1 \times E_2$ (con estructura de espacio vectorial) y $B : E \times E \longrightarrow K$ dada por*

$$B((u_1,u_2),(v_1,v_2)) = B_1(u_1,v_1) + B_2(u_2,v_2),\ \forall\, u_1, v_1 \in E_1; u_2, v_2 \in E_2.$$

Definimos la suma ortogonal de (E_1, B_1) y (E_2, B_2) como el espacio cuadrático (E, B) de dimensión $m+n$, que denotamos por $E_1 \perp E_2$.

Tenemos $B(E_1, E_2) = B(E_1 \times \{0\}, \{0\} \times E_2) = \{0\}$ (la suma se anula en los ejes), y $B|_{(E_i \times E_i)} = B_i$, $i = 1,2$. Además, notemos lo siguiente:

$$\begin{aligned} f_B(v_1,v_2) &= B((v_1,v_2),(v_1,v_2)) \\ &= B_1(v_1,v_1) + B_2(v_2,v_2) \\ &= f_{B_1}(v_1) + f_{B_2}(v_2), \end{aligned}$$

donde f_B es una K-forma asociada a B en alguna base de E. Esta igualdad nos facilita el mecanismo para operar sumas ortogonales en términos de formas cuadráticas.

Definición 2.3. *Sean f y g K-formas de grados n y m, respectivamente:*

$$f(X_1, ..., X_n) = \sum_{i,j=1}^{n} \alpha_{ij} X_i X_j \text{ y}$$

$$g(Y_1,...,Y_m)=\sum_{k,l=1}^{m}\beta_{kl}Y_kY_l.$$

Definimos la forma $f\perp g$, suma ortogonal de f y g, por la ecuación:

$$(f\perp g)(Z_1,...,Z_{n+m})=\sum_{i,j=1}^{n}\alpha_{ij}Z_iZ_j+\sum_{k,l=1}^{m}\beta_{kl}Z_{n+k}Z_{n+l}. \tag{2.1}$$

Ejemplo **2.1.** *Sean $f(X,Y)=X^2+Y^2$ y $g(X,Y,Z)=3XY-Z^2$. Entonces:*

$$f\perp g(V,W,X,Y,Z)=V^2+W^2+3XY-Z^2.$$

Sean f,g K-formas de dimensiones m y n, respectivamente. Dadas las matrices M_f y M_g, la matriz de $f\perp g$ será, evidentemente:

$$M_{f\perp g}=\begin{pmatrix}M_f & 0\\ 0 & M_g\end{pmatrix}, \tag{2.2}$$

que es una matriz $(m+n)\times(m+n)$.[2]

Las siguientes proposiciones nos muestran algunas propiedades de la suma ortogonal.

Proposición 2.2. *La suma ortogonal de espacios cuadráticos isótropos es isótropa.*

Demostración. Sean $E=E_1\oplus E_2$ y $q=q_1+q_2$. Tomemos $0\neq v_i\in E_i$, $i=1,2$ isótropos. Entonces, $q(v_1,v_2)=q_1(v_1)+q_2(v_2)=0$, luego (v_1,v_2) es un vector isótropo de $E=E_1\perp E_2$. □

Note que no necesariamente ocurre de forma análoga con dos espacios anisótropos (o sus formas inducidas).

Ejemplo **2.2.** *Sea $K=\mathbb{Z}_3$ y sean $f(X)=2X^2$, $g(X)=X^2$; es fácil ver que ambas formas son anisótropas. Sin embargo, $f\perp g(X,Y)=2X^2+Y^2$ es isótropa sobre K.*

Proposición 2.3. *Si (E_1,B_1) y (E_2,B_2) son regulares, entonces $E_1\perp E_2$ es regular.*

Demostración. Suficiente observar la matriz de la forma asociada a $E_1\perp E_2$, dada por la ecuación 2.2. □

Sea $\kappa\in K$ y consideremos la K-forma de dimensión 1, κX^2. Denotaremos la clase de isometría correspondiente a (κX^2) por $\langle\kappa\rangle$.[3] El inmediato representante de esta clase es el espacio cuadrático $\langle(K,\kappa X^2)\rangle$. Escribimos indistintamente $\langle\kappa\rangle$ para denotar tanto un espacio representante como la misma clase de isometría. Note que $\langle\kappa\rangle$ es regular si, y solo si, $\kappa\neq 0$ o (lo que es lo mismo) $\kappa\in\dot{K}$.

La siguiente proposición es el resultado principal de este capítulo, de ella se deduce el Teorema de diagonalización.

---

[2] El 0 de la parte superior derecha de la matriz 2.2 representa la matriz $n\times m$ cuyos coeficientes son todos 0; similarmente el 0 de la parte inferior izquierda, pero de orden $m\times n$.

[3] Escribiremos también, haciendo abuso de notación, $\langle\kappa\rangle$ para significar la forma κX^2 y también la clase de equivalencia (κX^2).

Proposición 2.4. Criterio de representación. *Sea (E,B) un espacio cuadrático y sea $\kappa \in \dot{K}$. Entonces $\kappa \in D(E)$ si, y solo si, existen un espacio cuadrático (E',B') y una isometría $E \cong \langle \kappa \rangle \perp E'$.*

Demostración. ($\Rightarrow$) Si $\kappa \in D(E)$ entonces existe $v \in E$ tal que $q(v) = \kappa$. Como en la demostración de la proposición 1.6, asumiremos que E mismo es regular pues si, $E = \mathrm{rad}E \oplus W = \mathrm{rad}E \perp W$ donde W es regular, entonces $D(E) = D(W)$ que es inmediato. Sea entonces E regular. El subespacio $K \cdot v$ de E es claramente isométrico a $\langle \kappa \rangle$, y $K \cdot v \cap (K \cdot v)^{\perp} = 0$. Por la regularidad de E, tenemos:

$$\dim(K \cdot v) + \dim(K \cdot v)^{\perp} = \dim E,$$

entonces $E = K \cdot v \oplus (K \cdot v)^{\perp} \cong \langle \kappa \rangle \perp (K \cdot v)^{\perp}$. Tomamos $E' = (K \cdot v)^{\perp}$. ($\Leftarrow$) Si tenemos $E \cong \langle \kappa \rangle \perp E'$ entonces κ es obviamente representado por $\langle \kappa \rangle \perp E'$, es decir, $\kappa \in D(\langle \kappa \rangle \perp E') = D(E)$. □

En teoría, estamos listos para diagonalizar una forma cuadrática.

Corolario 2.5. Teorema de diagonalización. *Si (E,B) es cualquier n-espacio cuadrático sobre un cuerpo K, entonces existen $\kappa_1, ..., \kappa_n \in K$ tales que $E \cong \langle \kappa_1 \rangle \perp \cdots \perp \langle \kappa_n \rangle$. Equivalentemente, toda K-forma de grado n $f(X_1, ..., X_n)$ es equivalente a una forma diagonal $\kappa_1 X_1^2 + \cdot + \kappa_n X_n^2$.*

Demostración. Si $D(E) = \emptyset$, entonces $B \equiv 0$ y $E \cong \langle 0 \rangle \perp \cdots \perp \langle 0 \rangle$. Si $B \neq 0$, demostraremos la proposición por inducción sobre n. El caso $n = 1$ es inmediato. Suponga que la proposición se cumple para $n-1$ y sea $\kappa \in D(E)$, esto implica que $E \cong \langle \kappa \rangle \perp E'$, donde $\dim E' = n-1$. Entonces $E' \cong \langle \kappa_1 \rangle \perp \cdots \perp \langle \kappa_{n-1} \rangle$, así:

$$E \cong \langle \kappa \rangle \perp E' \cong \langle \kappa \rangle \perp \langle \kappa_1 \rangle \perp \cdots \perp \langle \kappa_{n-1} \rangle.$$

□

Consecuentemente, denotaremos la forma diagonal $\langle \kappa_1 \rangle \perp \cdots \perp \langle \kappa_n \rangle$ por $\langle \kappa_1, ..., \kappa_n \rangle$. La K-forma de grado n $\langle \kappa, ..., \kappa \rangle$ será denotada por $n\langle \kappa \rangle$. Además, tomando $\mathscr{B} = (b_1, ..., b_n)$, la base obtenida por la diagonalización (es decir, $q(b_i) = \kappa_i$, $i = 1, ..., n$), es inmediato que $\mathscr{B}$ es una base ortogonal (porque E es isométrico a una suma ortogonal de subespacios de dimensión 1, cada uno de ellos generado por los elementos básicos); en consecuencia, la matriz de B en la base $\mathscr{B}$ es:

$$M_B = \begin{pmatrix} \kappa_1 & 0 & \cdots & 0 \\ 0 & \kappa_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \kappa_n \end{pmatrix},$$

es decir, M_B es diagonal.

Corolario 2.6. *Si (E,B) es un n-espacio cuadrático (no necesariamente regular) y $S \leq E$ es regular, entonces:*

(1) $E = S \perp S^{\perp}$;

(2) si $T \leq E$ *es tal que* $E = S \perp T$, *entonces* $T = S^{\perp}$.

Demostración. Vamos a empezar por probar *(1)*, luego probaremos que *(1)* $\Rightarrow$*(2)*. Puesto que $S \cap S^{\perp} = \mathrm{rad} S = 0$, solo queda probar que $S \oplus S^{\perp} = E$. Por la proposición 1.6, S tiene una base ortogonal $(v_1, ..., v_k)$, y, puesto que S es regular, tenemos $B(v_i, v_i) \neq 0$ para $i = 1, ..., k$. Tomemos $z \in E$; "proyectaremos" este vector en S. Sea:

$$w = z - \sum_{i=1}^{k} \frac{B(z, v_i)}{B(v_i, v_i)} v_i.$$

Afirmamos que $w \in S^{\perp}$. Así es:

$$\begin{aligned} B(w, v_j) &= B(z, v_j) - \sum_{i=1}^{k} \frac{B(z, v_i)}{B(v_i, v_i)} B(v_i, v_j) \\ &= B(z, v_j) - \frac{B(z, v_j)}{B(v_j, v_j)} B(v_j, v_j) = 0, \end{aligned}$$

esto es para $j = 1, ..., k$, luego w es ortogonal a todo elemento básico de S, luego a todo vector en S. Así, $w \in S^{\perp}$, es decir $z = v + w$, donde $v = \sum_{i=1}^{k} \frac{B(z, v_i)}{B(v_i, v_i)} v_i \in S$. Por tanto, $E = S \oplus S^{\perp} = S \perp S^{\perp}$. Así, queda probado *(1)*. Para *(2)* supongamos ahora que $E = S \perp S^{\perp}$ y sea $E = S \perp T$. Si $x \in T$ entonces, por definición, $B(x, S) = 0$ o $x \in S^{\perp}$. Por otro lado, $\dim T = \dim E - \dim S = \dim S^{\perp}$. Por tanto, $T = S^{\perp}$. □

Esta prueba nos conduce a la siguiente definición.

Definición 2.4. *Sea* (E, B) *un espacio cuadrático y sea* $S \leq E$ *un subespacio regular. Sea* $\mathscr{B} = (b_1, ..., b_k)$ *una base ortogonal de* S. *Dado* $v \in E$, *definimos la proyección de* v *sobre el subespacio* S *como:*

$$\mathrm{proy}_S(v) = w = v - \sum_{i=1}^{k} \frac{B(v, b_i)}{B(b_i, b_i)} b_i.$$

Corolario 2.7. *Sea* (E, B) *regular. Entonces* $S \leq E$ *es regular si, y solo si, existe* $T \subseteq E$ *tal que* $E = S \perp T$.

Demostración. ($\Rightarrow$) Es inmediato. ($\Leftarrow$) Si $E = S \perp T$, $B(S, T) = 0$ y, dado $v \in \mathrm{rad} S$, $B(v, S) = 0$, luego $B(v, E) = B(v, S \perp T) = B(v, S) + B(v, T) = 0$, entonces $v \in \mathrm{rad} E = \{0\}$, luego $v = 0$, es decir, S es regular. □

En teoría, toda K-forma admite una diagonalización. Sin embargo, en la demostración no se da ningún mecanismo para hallar los vectores básicos en los que la matriz de la K-forma es diagonal.

2.2. Un método de diagonalización

Dado un n-espacio cuadrático (E,B) y una base $\mathscr{B}=(b_1,...,b_n)$ de E, de modo que la matriz de B en la base $\mathscr{B}$ es M_B; y queremos diagonalizar esta matriz por medio de operaciones elementales. No olvidemos que M_B es simétrica. Sea:

$$M_B=\begin{pmatrix}\alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n}\\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2n}\\ \vdots & \vdots & \ddots & \vdots\\ \alpha_{n1} & \alpha_{n2} & \cdot & \alpha_{nn}\end{pmatrix}=\begin{pmatrix}\alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n}\\ \alpha_{12} & & & \\ \vdots & & M & \\ \alpha_{1n} & & & \end{pmatrix}$$

donde $\alpha_{ij}=\alpha_{ji}$, $i,j=1,...,n$ y M es simétrica.

1. Si $\alpha_{11}\neq 0$:

$$\begin{pmatrix}1 & 0 & \cdots & 0\\ -\frac{\alpha_{12}}{\alpha_{11}} & 1 & & \vdots\\ \vdots & & \ddots & 0\\ -\frac{\alpha_{1n}}{\alpha_{11}} & 0 & \cdots & 1\end{pmatrix}\begin{pmatrix}\alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n}\\ \alpha_{12} & & & \\ \vdots & & M & \\ \alpha_{1n} & & & \end{pmatrix}\begin{pmatrix}1 & -\frac{\alpha_{12}}{\alpha_{11}} & \cdots & -\frac{\alpha_{1n}}{\alpha_{11}}\\ 0 & 1 & & 0\\ \vdots & & \ddots & \vdots\\ 0 & \cdots & 0 & 1\end{pmatrix}=$$

$$=\begin{pmatrix}\alpha_{11} & 0 & \cdots & 0\\ 0 & & & \\ \vdots & & M' & \\ 0 & & & \end{pmatrix}\qquad \text{con } M' \text{ simétrica.}$$

   Ahora se sigue diagonalizando M'.

2. Si $\alpha_{1i}=0$ para todo $i=1,...,n$ entonces $M_B=\begin{pmatrix}0 & \cdots & 0\\ \vdots & M & \\ 0 & & \end{pmatrix}$ y basta diagonalizar M.

3. Si $\alpha_{11}=0$ y existe i con $2\leq i\leq n$ tal que $\alpha_{1i}\neq 0$ puede ocurrir dos cosas:

   i) Si $\alpha_{ii}\neq 0$, se multiplica a izquierda y derecha por la matriz elemental P^{1i} y se obtiene la matriz simétrica $P^{1i}\cdot M_B\cdot P^{1i}$ tal que $[P^{1i}\cdot M_B\cdot P^{1i}]_{11}=\alpha_{ii}$, con lo que volvemos al primer caso.[4]

   ii) Si $\alpha_{ii}=0$, sea $C^{(i)}$ la matriz definida por

$$[C^{(i)}]_{kj}=\begin{cases}1, & \text{si } k=j\text{; o } k=i \text{ cuando } j=1\\ 0, & \text{en otro caso.}\end{cases}$$

   Entonces $[(C^{(i)})^T\cdot M_B\cdot C^{(i)}]_{11}=2\alpha_{1i}$ y la matriz es simétrica, con lo que también estamos en el primer caso.

[4] P^{1i} se obtiene intercambiando la primera fila por la i-ésima fila de la matriz identidad.

Ejemplo **2.3.** *Sea* $B:\mathbb{R}^3\times\mathbb{R}^3\longrightarrow\mathbb{R}$ *la fbs tal que su matriz en la base canónica es*

$$M_B=\begin{pmatrix}0&1&1\\1&1&0\\1&0&1\end{pmatrix}.$$

Hallemos una base $\mathscr{B}$ *de* $\mathbb{R}^3$ *tal que la matriz de* B *sea diagonal.*

Siguiendo el algoritmo anterior, estamos en el caso en que $\alpha_{11}=0$ y $\alpha_{22}\neq 0$. Multiplicando a izquierda y derecha por la matriz P^{12} obtenemos:

$$P^{12}M_BP^{12}=\begin{pmatrix}0&1&0\\1&0&0\\0&0&1\end{pmatrix}\begin{pmatrix}0&1&1\\1&1&0\\1&0&1\end{pmatrix}\begin{pmatrix}0&1&0\\1&0&0\\0&0&1\end{pmatrix}=\begin{pmatrix}1&1&0\\1&0&1\\0&1&1\end{pmatrix}.$$

Estamos en condiciones de aplicar el primer paso del algoritmo, ya que tenemos $[P^{12}M_BP^{12}]_{11}=1\neq 0$. Luego:

$$\begin{pmatrix}1&0&0\\-1&1&0\\0&0&1\end{pmatrix}\begin{pmatrix}1&1&0\\1&0&1\\0&1&1\end{pmatrix}\begin{pmatrix}1&-1&0\\0&1&0\\0&0&1\end{pmatrix}=\begin{pmatrix}1&0&0\\0&-1&1\\0&1&1\end{pmatrix}.$$

Ahora, nos basta diagonalizar el bloque $\begin{pmatrix}-1&1\\1&1\end{pmatrix}$, que nuevamente satisface las condiciones del paso 1, así que:

$$\begin{pmatrix}1&0\\1&1\end{pmatrix}\begin{pmatrix}-1&1\\1&1\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix}=\begin{pmatrix}-1&0\\0&2\end{pmatrix}.$$

Podemos resumir las operaciones efectuadas de la siguiente forma:

$$\begin{pmatrix}1&0&0\\0&1&0\\0&1&1\end{pmatrix}\cdot\begin{pmatrix}1&0&0\\-1&1&0\\0&0&1\end{pmatrix}\cdot P^{12}\cdot M_B\cdot P^{12}\cdot\begin{pmatrix}1&-1&0\\0&1&0\\0&0&1\end{pmatrix}\cdot\begin{pmatrix}1&0&0\\0&1&1\\0&0&1\end{pmatrix}=$$

$$=\begin{pmatrix}1&0&0\\0&-1&0\\0&0&2\end{pmatrix}.$$

Por tanto, la base $\mathscr{B}$ de $\mathbb{R}^3$ que estamos buscando debe tener la matriz cambio de base igual a:

$$P=P^{12}\cdot\begin{pmatrix}1&-1&0\\0&1&0\\0&0&1\end{pmatrix}\cdot\begin{pmatrix}1&0&0\\0&1&1\\0&0&1\end{pmatrix}=\begin{pmatrix}0&1&1\\1&-1&-1\\0&0&1\end{pmatrix}$$

y así, la base es la colección de los vectores columna de P:

$$\mathscr{B}=\{(0,1,0),(1,-1,0),(1,-1,1)\}.$$

Ejemplo **2.4.** *Sea* $B_1 : \mathbb{R}^3 \times \mathbb{R}^3 \longrightarrow \mathbb{R}$ *la fbs tal que su matriz en la base canónica es*

$$M_{B_1} = \begin{pmatrix} 0 & 1 & 3 \\ 1 & 0 & 0 \\ 3 & 0 & 0 \end{pmatrix}.$$

Hallemos una base $\mathscr{B}_1$ *de* $\mathbb{R}^3$ *tal que la matriz de* B_1 *sea diagonal.*

En este caso, $\alpha_{11} = 0$ y $\alpha_{22} = 0$. Como estamos en *ii)* del caso 2 del algoritmo anterior, multiplicamos por las matrices $(C^{(2)})^T$ y $C^{(2)}$ por izquierda y derecha, respectivamente y obtenemos:

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot M_{B_1} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 3 \\ 1 & 0 & 0 \\ 3 & 0 & 0 \end{pmatrix}.$$

Luego, como estamos en el primer caso del algoritmo:

$$\begin{pmatrix} 1 & 0 & 0 \\ -1/2 & 1 & 0 \\ -3/2 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 & 1 & 3 \\ 1 & 0 & 0 \\ 3 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1/2 & -3/2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 0 & 0 \\ 0 & -1/2 & -3/2 \\ 0 & -3/2 & -9/2 \end{pmatrix}.$$

Diagonalizando ahora el bloque de 2×2 nos queda:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 & 0 & 0 \\ 0 & -1/2 & -3/2 \\ 0 & -3/2 & -9/2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -3 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 0 & 0 \\ 0 & -1/2 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Como en el anterior ejemplo, si $\mathscr{B}_1$ es la base buscada, la matriz cambio de base P_1 resulta

$$P_1 = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1/2 & -3/2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -3 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -1/2 & 0 \\ 1 & 1/2 & -3 \\ 1 & -1/2 & 1 \end{pmatrix},$$

así que $\mathscr{B}_1 = \{(1,1,1), (-1/2, 1/2, -1/2), (0, -3, 1)\}$.

Capítulo 3

Espacios Hiperbólicos

En este capítulo definiremos un importante elemento en la colección de los espacios cuadráticos: el plano hiperbólico. Recordemos que, dado un n-espacio cuadrático (E,B) sobre un cuerpo K y un vector $v \in E$ no nulo, v es isótropo si $B(v,v)=0$, luego el mismo espacio E es llamado isótropo. El vector v es anisótropo en el caso opuesto y E lo es si todo vector no nulo $w \in E$ es tal que $B(w,w) \neq 0$ (note que puede ocurrir $B(v,w)=0$, $0 \neq v,w \in E$, $v \neq w$ aún siendo E anisótropo, por ejemplo, suficiente tomar dos vectores ortogonales). Convenimos que (E,B) con $B \equiv 0$, es anisótropo.

Antes, discutiremos una definición que nos será útil para estudiar espacios cuadráticos en general, particularmente para el estudio de espacios hiperbólicos: el determinante de una forma cuadrática.

Definición 3.1. *Sea f una K-forma de grado n no singular. Definimos el determinante de f por la ecuación:*

$$d(f) = \det(M_f) \cdot \dot{K}^2.$$

Notamos que $d(f)$ es un elemento del grupo de clases de cuadrados $\dot{K}/\dot{K}^2$, (tanto este determinante como $\dot{K}/\dot{K}^2$ jugarán roles importantes en la caracterización de los anillos de Witt). Si (E,B) es un espacio cuadrático regular correspondiente a la clase se equivalencia de f, escribiremos $d(E)$ para significar $d(f)$, es decir, $d(E)=d(f)$.[1]

Proposición 3.1. *Sean f,g K-formas. Entonces:*

(1) Si $f \cong g$ entonces $d(f)=d(g)$;

(2) $d(f \perp g)=d(f)d(g)$.

Demostración. (1) Sea $f \cong g$, entonces $M_f = C^T \cdot M_g \cdot C$, con C invertible, y

$$d(f) = \det(M_f)\cdot \dot{K}^2 = \det(C^T M_g C)\cdot \dot{K}^2 = \det(C)^2 \det(M_g)\cdot \dot{K}^2 = \det(M_g)\cdot \dot{K}^2 = d(g).$$

(2) Recordemos que

$$M_{f\perp g} = \begin{pmatrix} M_f & 0 \\ 0 & M_g \end{pmatrix};$$

entonces, $d(f \perp g) = \det(M_{f\perp g})\cdot \dot{K}^2 = \det(M_f)\det(M_g)\cdot \dot{K}^2 = d(f)d(g)$. □

[1] ¡No confundir $d(f)$ con $D(f)$!

Así, d es un invariante de la clase de equivalencia de una K-forma f y transforma la suma ortogonal de formas en producto de clases laterales de $\dot{K}/\dot{K}^2$. Una observación más: Si $(E,B)\cong\langle d_1,...,d_n\rangle$, entonces $d(E)=d(f_B)=d_1d_2...d_n\cdot\dot{K}^2$. Esto se sigue directamente del corolario 2.5.

3.1. Caracterización del plano hiperbólico

Veamos preliminarmente una propiedad de la forma $X_1^2-X_2^2$.

Proposición 3.2. $D(\langle 1,-1\rangle)=\dot{K}$.

Demostración. En efecto, dado $\alpha\in\dot{K}$, se tiene:

$$\alpha=\left(\frac{\alpha+1}{2}\right)^2-\left(\frac{\alpha-1}{2}\right)^2.$$

□

Definición 3.2. *Un espacio cuadrático (E,B) es llamado universal si $D(f_B)=D(E)=\dot{K}$, es decir f_B representa todos los elementos de K.*

A continuación caracterizaremos al plano hiperbólico, pero para ello necesitamos el siguiente lema, el que establece la equivalencia de formas diagonales regulares de dimensión 2 y será utilizado en la demostración del siguiente teorema.

Lema 3.3. *Sean $f=\langle\alpha,\beta\rangle$, $g=\langle\gamma,\delta\rangle$ K-formas regulares. Entonces $f\cong g$ si, y solo si, $d(f)=d(g)$, y, tanto f como g representan un elemento común $\epsilon\in\dot{K}$.*

Demostración. ($\Rightarrow$) Se sigue inmediatamente de la definición de "$\cong$". ($\Leftarrow$) Si $d(f)=d(g)\in\dot{K}/\dot{K}^2$ y existe $\epsilon\in D(f)\cap D(g)$, entonces, por el Criterio de Representación (2.4), tenemos $f\cong\langle\epsilon,\epsilon'\rangle$ para algún $\epsilon'\in\dot{K}$. Tomando los determinantes, obtenemos $\alpha\beta\cdot\dot{K}^2=\epsilon\epsilon'\cdot\dot{K}^2$, luego $\alpha\beta\epsilon\cdot\dot{K}^2=\epsilon'\cdot\dot{K}^2$ es decir, $\alpha\beta\epsilon=\epsilon'\lambda^2$, para algún $\lambda\in\dot{K}$. Luego:

$$\begin{pmatrix}1&0\\0&\lambda\end{pmatrix}\begin{pmatrix}\epsilon&0\\0&\epsilon'\end{pmatrix}\begin{pmatrix}1&0\\0&\lambda\end{pmatrix}=\begin{pmatrix}\epsilon&0\\0&\epsilon'\lambda^2\end{pmatrix}=\begin{pmatrix}\epsilon&0\\0&\alpha\beta\epsilon\end{pmatrix},$$

es decir, $f\cong\langle\epsilon,\alpha\beta\epsilon\rangle$. De manera similar, $g\cong\langle\epsilon,\gamma\delta\epsilon\rangle$. Pero, por hipótesis, $\alpha\beta\cdot\dot{K}^2=\gamma\delta\cdot\dot{K}^2$, entonces $\alpha\beta=\gamma\delta\kappa^2$, con $\kappa\in\dot{K}$. Finalmente,

$$\begin{pmatrix}1&0\\0&\kappa\end{pmatrix}\begin{pmatrix}\epsilon&0\\0&\gamma\delta\epsilon\end{pmatrix}\begin{pmatrix}1&0\\0&\kappa\end{pmatrix}=\begin{pmatrix}\epsilon&0\\0&\gamma\delta\epsilon\kappa^2\end{pmatrix}=\begin{pmatrix}\epsilon&0\\0&\alpha\beta\epsilon\end{pmatrix},$$

así, $f\cong g$. □

Tenemos ahora, los elementos para definir el plano hiperbólico $\mathbb{H}$. Veamos ahora cuatro condiciones equivalentes que caracterizan a este.

Teorema 3.4. *Sea (E,q) un 2-espacio cuadrático. Son equivalentes:*

(1) E *es regular e isótropo;*

(2) E *es regular, con* $d(E) = -1 \cdot \dot{K}^2$*;*

(3) E *es isométrico a* $\langle 1, -1 \rangle$*;*

(4) E *corresponde a la clase de* K*-formas de grado* 2 *de la forma cuadrática* $X_1 X_2$*.*

Demostración. Para empezar, vimos ya en el capítulo 1, ejemplo 1.3, que *(3)*$\Leftrightarrow$*(4)*. Así, probaremos solamente *(1)*$\Rightarrow$*(2)*$\Rightarrow$*(3)*$\Rightarrow$*(1)*.
(1)$\Rightarrow$*(2)* Sea $v \in E$ un vector isótropo. Por hipótesis, tenemos una isometría $E \cong \langle \kappa_1, \kappa_2 \rangle$ donde, tanto κ_1 como κ_2, son elementos de $\dot{K}$. Sea (v_1, v_2) una base correspondiente a la forma diagonal de E, es decir, $q(v_1) = \kappa_1$ y $q(v_2) = \kappa_2$. Luego podemos escribir v como combinación lineal de v_1 y v_2, $v = \alpha v_1 + \beta v_2$ con

$$0 = q(v) = \kappa_1 \alpha^2 + \kappa_2 \beta^2$$

donde, por la isotropía de v, $\alpha \neq 0$ y $\beta \neq 0$. Vemos también que $\kappa_1 = -(\beta \alpha^{-1})^2 \kappa_2$. Por definición, $d(E) = \kappa_1 \kappa_2 \cdot \dot{K}^2 = -(\beta \alpha^{-1})^2 \kappa_2 \kappa_2 \cdot \dot{K}^2 = (\beta \alpha^{-1} \kappa_2)^2 (-1) \cdot \dot{K}^2 = -1 \cdot \dot{K}^2$.
(2)$\Rightarrow$*(3)* Tenemos por hipótesis que $d(E) = -\dot{K}^2 = d(\langle 1, -1 \rangle)$ y $D(E) \cap D(\langle 1, -1 \rangle) = D(E)$; luego, por el anterior lema, E es un elemento de la clase de isometría correspondiente a $\langle 1, -1 \rangle$.
(3)$\Rightarrow$*(1)*. Suponiendo $E \cong \langle 1, -1 \rangle$, es claro que E es regular. Probemos que es isótropo. De hecho, todo vector $v \in E$ de la forma $v = \alpha v_1 + \alpha v_2$, donde (v_1, v_2) es la base ortogonal correspondiente a la forma diagonal de E, cumple $q(v) = \alpha^2 - \alpha^2 = 0$. □

Definición 3.3. *Definimos el plano hiperbólico* $\mathbb{H}_K$ *sobre un cuerpo* K*, por la ecuación*

$$\mathbb{H}_K = \langle 1, -1 \rangle.$$

Un espacio E *es llamado espacio hiperbólico si existe una isometría*

$$E \cong \mathbb{H}_K \perp \cdots \perp \mathbb{H}_K,$$

es decir, E *es una suma ortogonal de planos hiperbólicos.*[2]

Notemos que si E es un espacio hiperbólico, entonces tendrá dimensión par; y, la forma asociada a E será $(X_1^2 - X_2^2) + \cdots + (X_{2n-1}^2 - X_{2n}^2)$ o la forma equivalente $X_1 X_2 + \cdots + X_{2n-1} X_{2n}$.

Teorema 3.5. *Sea* (E, B) *regular. Entonces:*

(1) Todo subespacio totalmente isótropo $S \leq E$ *de dimensión* r *está contenido en un subespacio hiperbólico* $S \leq T \leq E$ *de dimensión* $2r$*.*

(2) E *es isótropo si, y solo si,* E *contiene un plano hiperbólico.*

(3) E *isótropo* $\Rightarrow$ E *universal.*

[2] Escribiremos simplemente $\mathbb{H}$ cuando K esté fijo.

Demostración. (1) Probaremos por inducción sobre r. Sea $S \leq E$ de dimensión 1 totalmente isótropo. Entonces $S = K \cdot v$ con $v \neq 0$ y $B(v,v) = 0$. Sea $(b_1, ..., b_n)$ una base ortogonal de E y por su regularidad, $B(b_i, b_i) \neq 0$, para $i = 1, ..., n$. Además, $v = \alpha_1 b_1 + \cdots + \alpha_n b_n$ donde digamos, $\alpha_k \neq 0$. Entonces, $B(v, b_k) = \sum_i \alpha_i B(b_i, b_k) = \alpha_k B(b_k, b_k) \neq 0$. Podemos entonces proyectar v sobre b_k. Sea $x = v - \text{proy}_{b_k}(v) = v - \alpha_k b_k$; tenemos que:

$$\begin{aligned} B(x,x) &= B(v,v) - 2B(v, \alpha_k b_k) + B(\alpha_k b_k, \alpha_k b_k) \\ &= 0 - 2\alpha_k^2 B(b_k, b_k) + \alpha_k^2 B(b_k, b_k) \\ &= -\alpha_k^2 B(b_k, b_k) \neq 0 \text{ y} \end{aligned}$$

$$B(b_k, x) = B(b_k, v) - B(b_k, \alpha_k b_k) = \alpha_k B(b_k, b_k) - \alpha_k B(b_k, b_k) = 0;$$

luego, b_k y x son ortogonales y $v = x + \alpha_k b_k$, es decir, v está en el subespacio T generado por x y b_k. Además,

$$\det T = \begin{vmatrix} B(x,x) & B(x,b_k) \\ B(b_k,x) & B(b_k,b_k) \end{vmatrix} \dot{K}^2 = -\alpha_k^2 B(b_k, b_k)^2 \dot{K}^2 = -\dot{K}^2,$$

es decir, $T \cong \mathbb{H}$.

Sea ahora $S \leq E$ totalmente isótropo. Sea $X = (x_1, ..., x_r)$ una base de S y sea $U = \text{span}(X \backslash \{x_1\})$. Es claro que $S^\perp \subseteq U^\perp$. Por la regularidad de E, tenemos:

$$\dim U^\perp = \dim E - \dim U > \dim E - \dim S = \dim S^\perp.$$

Esto significa que existe un vector y_1 que es ortogonal a $x_2, ..., x_r$ pero no a x_1, o sea, $B(x_1, y_1) \neq 0$. Notemos también que x_1 y y_1 son linealmente independientes, de lo contrario tendríamos que $y = \alpha x_1$, $\alpha \in \dot{K}$ y $B(x_1, y_1) = B(x_1, x_1) = \alpha B(x_1, x_1) = 0$; y así, $y_1 \in S^\perp$, absurdo. El subespacio $H_1 = \text{span}(\{x_1, y_1\})$ tiene como determinante:

$$d(H_1) = \begin{vmatrix} 0 & B(x_1,y_1) \\ B(x_1,y_1) & B(y_1,y_1) \end{vmatrix} \cdot \dot{K}^2 = -1 \cdot \dot{K}^2;$$

por tanto, $H_1 \cong \mathbb{H}$. Tenemos entonces una isometría $E = H_1 \perp E'$, donde $E' = H_1^\perp$. Por la regularidad de H_1, E' es regular y contiene a U totalmente isótropo de dimensión $r-1$; entonces, por la hipótesis de inducción, este está contenido en un espacio hiperbólico H_2 de dimensión $2(r-1)$, es decir, $E \cong H_1 \perp H_2 \perp E''$. *(1) ⇒ (2)* Si $v \in E$ es isótropo, entonces $K \cdot v$ es totalmente isótropo de dimensión 1, luego está contenido en un espacio hiperbólico T de dimensión 2, es decir un plano hiperbólico $T \cong \mathbb{H}$. *(2) ⇒ (3)* Como E es isótropo, contiene un plano hiperbólico $\mathbb{H}$, el que es universal. □

Corolario 3.6. Primer Teorema de Representación. *Sea (E, B) regular, y sea $\kappa \in \dot{K}$. Entonces, $\kappa \in D(E)$ si, y solo si, $E \perp \langle -\kappa \rangle$ es isótropo.*

Demostración. (⇒) Sea $f(X) = f_B(X) = a_1 X_1^2 + \cdots + a_n X_n^2$ en su forma diagonal, para alguna base ortogonal de E. Si $\kappa \in D(E)$, entonces existen $x_1, ..., x_n \in \dot{K}$ tales que

$$\kappa = a_1 x_1^2 + \cdots + a_n x_n^2,$$

o, lo que es lo mismo,

$$a_1x_1^2+\cdots+a_nx_n^2+(-\kappa)\cdot 1^2=0,$$

así que la forma $E\perp\langle-\kappa\rangle$ es isótropa.
($\Leftarrow$) Sea $(x_1,...,x_n,x_{n+1})$ un vector isótropo de $E\perp\langle-\kappa\rangle$, entonces $a_1x_1^2+\cdots+a_nx_n^2-\kappa x_{n+1}^2=0$. Si $x_{n+1}\neq 0$, entonces

$$\kappa=a_1\left(\frac{x_1}{x_{n+1}}\right)^2+\cdots+a_n\left(\frac{x_n}{x_{n+1}}\right)^2\in D(E).$$

Si por el contrario, $x_{n+1}=0$, entonces $(x_1,...,x_n)\neq 0$ es un vector isótropo para E mismo. Por la parte (3) del teorema anterior, E es universal, o $D(E)=\dot{K}$, así, por supuesto, $\kappa\in D(E)$. □

Una demostración más corta de ($\Rightarrow$): si $\kappa\in D(E)$, entonces: $E\cong\langle\kappa\rangle\perp E'$, luego

$$\begin{aligned}E\perp\langle-\kappa\rangle&\cong\langle-\kappa\rangle\perp\langle\kappa\rangle\perp E'\\&=\langle\kappa,-\kappa\rangle\perp E'\\&\cong\mathbb{H}\perp E',\end{aligned}$$

que es isótropo. En el siguiente capítulo veremos que, de manera similar, a cualquier espacio cuadrático se le puede "separar" de forma única su parte hiperbólica.

Capítulo 4

Cancelación y Descomposición de Witt

El principal objetivo de este capítulo es demostrar el llamado "Teorema de Cancelación de Witt", que es uno de los resultados más importantes de la teoría de formas cuadráticas sobre cuerpos. Un punto que resaltamos es que no supondremos la regularidad del espacio en cuestión en la demostración de este teorema. Previamente, haremos un breve estudio del grupo de reflexiones sobre un hiperplano en un espacio cuadrático dado. Posterior a ello, daremos una caracterización de cualquier espacio cuadrático, su descomposición en forma única como suma ortogonal, que comprende sus partes hiperbólica y anisótropa, es decir, dado E un n-espacio cuadrático, este será isométrico a $r\mathbb{H} \perp E_a$, para algún $r \in \mathbb{N}$ y E_a anisótropo.

4.1. Reflexiones sobre hiperplanos

Definición 4.1. *Sea (E,B) un n-espacio cuadrático. Escribiremos $O_B(E) = O(E)$ para denotar la colección de isometrías de (E,B), donde $T \in O(E)$ si $T : E \longrightarrow E$ es un automorfismo que cumple*

$$B(T(x),T(y)) = B(x,y),\ \forall x,y \in E.$$

Proposición 4.1. *$(O(E),\cdot)$ es un grupo, donde "$\cdot$" es el producto de transformaciones lineales.*

Demostración. Sean $T_1, T_2 \in O(E)$; entonces, $T_1 \cdot T_2 : E \longrightarrow E$ es un automorfismo que cumple:

$$B(T_1 \cdot T_2(x), T_1 \cdot T_2(y)) = B(T_1(T_2(x)), T_1(T_2(y))) = B(T_2(x), T_2(y)) = B(x,y);$$

luego $T_1 \cdot T_2 \in O(E)$. Por otro lado, es inmediato que $I \in O(E)$ actúa como neutro. Sabemos también que el producto de transformaciones lineales es asociativo. Por último, si $T \in O(E)$, existe T^{-1} [que es también un automorfismo] tal que $T \cdot T^{-1} = I$. Probemos que T^{-1} está en $O(E)$:

$$B(x,y) = B(T(T^{-1}(x)), T(T^{-1}(y))) = B(T^{-1}(x), T^{-1}(y));$$

luego $T^{-1} \in O(E)$. □

A continuación, haremos una importante construcción en $O(E)$.

Definición 4.2. *Sea $y \in E$ un vector anisótropo, es decir, $B(y,y) \neq 0$. A este vector asociamos un operador $\tau_y : E \longrightarrow E$, definido por la ecuación:*

$$\tau_y(v) = v - 2\text{proy}_y(v), \ \forall v \in E. \tag{4.1}$$

Llamamos a τ_y reflexión sobre el hiperplano $(K \cdot y)^\perp$ o simplemente reflexión.

Recordemos que $\text{proy}_y(v) = \dfrac{B(v,y)}{B(y,y)}y$; luego τ_y se escribe de la forma:

$$\tau_y(v) = v - 2\frac{B(v,y)}{B(y,y)}y.$$

Proposición 4.2. *Sea τ_y una reflexión. Entonces:*

(1) τ_y es lineal;

(2) $\tau_y|_{(K\cdot y)^\perp} = I$ y $\tau_y|_{K\cdot y} = -I$;

(3) $\tau_y^2 = I$;

(4) $\det \tau_y = -1$;

(5) $\tau_y \in O(E)$.

Demostración. *(1)* Si $v, w \in E$ y $\alpha \in K$, entonces:

$$\begin{aligned}
\tau_y(v+w) &= v + w - 2\frac{B(v+w,y)}{B(y,y)}y \\
&= v + w - 2\frac{B(v,y)+B(w,y)}{B(y,y)}y \\
&= v - 2\frac{B(v,y)}{B(y,y)}y + w - 2\frac{B(w,y)}{B(y,y)}y \\
&= \tau_y(v) + \tau_y(w), \text{ y}
\end{aligned}$$

$$\begin{aligned}
\tau_y(\alpha v) &= \alpha v - 2\frac{B(\alpha v,y)}{B(y,y)}y = \alpha v - 2\alpha\frac{B(v,y)}{B(y,y)}y \\
&= \alpha\left(v - 2\frac{B(v,y)}{B(y,y)}y\right) = \alpha\tau_y(v).
\end{aligned}$$

(2) Sea $x \in (K\cdot y)^\perp$, entonces $B(x,y) = 0$ y:

$$\tau_y(x) = x - 2\frac{B(x,y)}{B(y,y)}y = x.$$

En cambio, si $w \in K \cdot y$, entonces $w = \alpha y$ y:

$$\begin{aligned}\tau_y(w) = \tau_y(\alpha y) &= \alpha y - 2\frac{B(\alpha y, y)}{B(y,y)} y \\ &= \alpha y - 2\alpha \frac{B(y,y)}{B(y,y)} y \\ &= \alpha y - 2\alpha y = -\alpha y = -w.\end{aligned}$$

(3) Consecuencia directa de *(2)*.

(4) Como $(\det \tau_y)^2 = 1$, y τ_y no es la identidad, debe ser $\det \tau_y = -1$.

(5)

$$\begin{aligned}B(\tau_y(v), \tau_y(w)) &= B\left(v - 2\frac{B(v,y)}{B(y,y)} y, w - 2\frac{B(w,y)}{B(y,y)} y\right) \\ &= B(v,w) - 2\frac{B(w,y)}{B(y,y)} B(v,y) - 2\frac{B(v,y)}{B(y,y)} B(y,w) + 4\frac{B(v,y)B(w,y)}{B(y,y)^2} B(y,y) \\ &= B(v,w) - 4\frac{B(v,y)B(w,y)}{B(y,y)} + 4\frac{B(v,y)B(w,y)}{B(y,y)} \\ &= B(v,w);\end{aligned}$$

así, $\tau_y \in O(E)$.

□

Consideremos ahora el conjunto de reflexiones sobre hiperplanos $\tau = \{\tau_y ; B(y,y) \neq 0\}$.

Proposición 4.3. *τ es un subgrupo normal del grupo ortogonal $O(E)$ ($\tau \lhd O(E)$).*

Demostración. Sean $\omega \in O(E)$ y $x \in E$. Entonces:

$$\begin{aligned}(\omega \tau_y \omega^{-1})(x) &= \omega(\tau_y(\omega^{-1}(x))) \\ &= \omega\left(\omega^{-1}(x) - 2\frac{B(\omega^{-1}(x), y)}{B(y,y)} y\right) \\ &= x - 2\frac{B(\omega^{-1}(x), y)}{B(y,y)} \omega(y) \\ &= x - 2\frac{B(x, \omega(y))}{B(\omega(y), \omega(y))} \omega(y) \\ &= \tau_{\omega(y)}(x),\end{aligned}$$

es decir, $\omega \tau \omega^{-1} \subseteq \tau$, para todo $\omega \in O(E)$. □

4.2. El Teorema de Cancelación

Primero demostraremos un lema que será utilizado en la demostración del teorema principal de este trabajo.

Lema 4.4. *Sea $(E,B)=(E,q)$ un n-espacio cuadrático. Sean $\kappa \in D(E)$ y $x,y \in E$ tales que $q(x)=q(y)=\kappa$. Entonces existe una isometría $T:E \longrightarrow E$ que cumple $T(x)=y$.*

Demostración. Primero vemos que $q(x+y)+q(x-y)=B(x+y,x+y)+B(x-y,x-y)=2(B(x,x)+B(y,y))=2(q(x)+q(y))=4q(x)\neq 0$, entonces, $q(x+y)$ y $q(x-y)$ no pueden ser ambos cero. Supongamos que $B(x-y,x-y)=q(x-y)\neq 0$. Afirmamos que $T=\tau_{x-y}$ es la isometría que lleva x a y. En efecto:

$$\begin{aligned}
\tau_{x-y}(x) &= x-2\frac{B(x,x-y)}{B(x-y,x-y)}(x-y)\\
&= x-\frac{2B(x,x-y)}{B(x,x)+B(y,y)-2B(x,y)}(x-y)\\
&= x-\frac{2B(x,x-y)}{2B(x,x)-2B(x,y)}(x-y)\\
&= x-\frac{2B(x,x-y)}{2B(x,x-y)}(x-y)\\
&= x-(x-y)=y.
\end{aligned}$$

Si tuviéramos $q(x-y)=0$, entonces $q(x+y)\neq 0$ y la isometría $T'=-I\circ\tau_{x+y}$ cumple:

$$\begin{aligned}
T'(x) &= -I(\tau_{x+y}(x))\\
&= -(\tau_{x+y}(x))\\
&= -\left(x-\frac{2B(x,x+y)}{B(x+y,x+y)}(x+y)\right)\\
&= -x+\frac{2B(x,x+y)}{B(x,x)+B(y,y)+2B(x,y)}(x+y)\\
&= -x+\frac{2B(x,x+y)}{2B(x,x+y)}(x+y)\\
&= -x+(x+y)=y.
\end{aligned}$$

□

Teorema 4.5. Teorema de Cancelación de Witt. *Sean f,f_1 y f_2 K-formas. Si existe una equivalencia $f\perp f_1\cong f\perp f_2$, entonces $f_1\cong f_2$.*

Demostración. Supongamos que existe una equivalencia $f\perp f_1\cong f\perp f_2$.
Caso 1. Supongamos que f es totalmente isótropa y f_1 regular. Sean M_1 y M_2 las matrices asociadas a las formas f_1 y f_2, respectivamente. Las matrices de $f\perp f_1$ y $f\perp f_2$ son por

hipótesis $\begin{pmatrix}0&0\\0&M_1\end{pmatrix}$ y $\begin{pmatrix}0&0\\0&M_2\end{pmatrix}$ respectivamente, además congruentes, es decir, existe una matriz invertible $E=\begin{pmatrix}A&B\\C&D\end{pmatrix}$ tal que:

$$\begin{aligned}\begin{pmatrix}0&0\\0&M_1\end{pmatrix}&=E^T\begin{pmatrix}0&0\\0&M_2\end{pmatrix}E\\&=\begin{pmatrix}A^T&C^T\\B^T&D^T\end{pmatrix}\begin{pmatrix}0&0\\0&M_2\end{pmatrix}\begin{pmatrix}A&B\\C&D\end{pmatrix}\\&=\begin{pmatrix}A^T&C^T\\B^T&D^T\end{pmatrix}\begin{pmatrix}0&0\\M_2C&M_2D\end{pmatrix}\\&=\begin{pmatrix}C^TM_2C&C^TM_2D\\D^TM_2C&D^TM_2D\end{pmatrix}.\end{aligned}$$

Vemos que $M_1=D^TM_2D$. Como f_1 es regular, M_1 es invertible y por tanto M_2 también lo es, y además son congruentes. Entonces $f_1\cong f_2$.

Caso 2. Sea f totalmente isótropa. Supongamos que f_1 tiene exactamente r ceros en su diagonalización, mientras que f_2 tiene r ceros o más. Reescribiendo la hipótesis, tenemos:

$$f\perp r\langle 0\rangle\perp f_1'\cong f\perp r\langle 0\rangle\perp f_2',$$

donde f_1' es regular. Por el caso 1, $f_1'\cong f_2'$.

Caso 3. Sea $\langle\alpha_1,...,\alpha_n\rangle$ una diagonalización de f. Probaremos por inducción sobre n. Sea entonces $f=\langle\alpha\rangle$. Si $\alpha=0$ entonces estamos nuevamente en el caso 2. Supongamos que $\alpha\neq 0$. Tenemos $\langle\alpha\rangle\perp f_1\cong\langle\alpha\rangle\perp f_2$. Sea (E,B) un representante de la clase de isometrías de espacios cuadráticos correspondiente a la clase de equivalencias de $\langle\alpha\rangle\perp f_1$. Entonces, dadas dos bases $\mathscr{B}_1=(x,x_1,...,x_m)$ y $\mathscr{B}_2=(y,y_1,...,y_m)$ de E, las matrices de $\langle\alpha\rangle\perp f_1$ y $\langle\alpha\rangle\perp f_2$ son, respectivamente:

$$M_1=\begin{pmatrix}\alpha&0&\cdots&0\\0&&&\\\vdots&&M_1'&\\0&&&\end{pmatrix}\text{ y }M_2=\begin{pmatrix}\alpha&0&\cdots&0\\0&&&\\\vdots&&M_2'&\\0&&&\end{pmatrix},$$

donde $q(x)=B(x,x)=\alpha=B(y,y)=q(y)$. Entonces podemos aplicar el lema 4.4. Así, existe una isometría $T:E\longrightarrow E$ tal que $T(x)=y$. Revisemos las estructuras de M_1 y M_2. Notemos que $B(x,x_i)=0=B(y,y_i)$, para $i=1,...,n$; y los subespacios $K\cdot x$, $K\cdot y$ son regulares; entonces, por el corolario 2.6, $E\cong K\cdot x\perp(K\cdot x)^\perp\cong K\cdot y\perp(K\cdot y)^\perp$ y, bajo la isometría T restringida a $(K\cdot x)^\perp$, $(K\cdot x)^\perp\cong(K\cdot y)^\perp$. Notemos también que las matrices de f_1 y f_2 son, respectivamente, M_1' y M_2' y cada una de ellas corresponde a $(K\cdot x)^\perp$ y $(K\cdot y)^\perp$, respectivamente. Dicho de otro modo, $f_1\cong f_2$. Esto prueba el caso $n=1$. Supongamos ahora que la hipótesis se cumple para $n-1$. Si $f=\langle\alpha_1,...,\alpha_n\rangle$, entonces tenemos:

$$\begin{aligned}\langle\alpha_1,...,\alpha_{n-1}\rangle\perp f_1'&=\langle\alpha_1,...,\alpha_{n-1}\rangle\perp\langle\alpha_n\rangle\perp f_1\\&\cong\langle\alpha_1,...,\alpha_{n-1}\rangle\perp\langle\alpha_n\rangle\perp f_2\\&=\langle\alpha_1,...,\alpha_{n-1}\rangle\perp f_2'.\end{aligned}$$

Por tanto, $f_1' \cong f_2'$, o $\langle \alpha_n \rangle \perp f_1 \cong \langle \alpha_n \rangle \perp f_2$, de donde $f_1 \cong f_2$. Esto concluye la demostración. □

Corolario 4.6. Teorema de Descomposición de Witt. *Sea (E, B) un espacio cuadrático. E se descompone en suma ortogonal $E \cong r\mathbb{H} \perp E_a$, donde E_a es anisótropo y $r \in \mathbb{N}$. E_a está unívocamente determinado (salvo isometría) y se denomina la parte anisótropa de E y, r es llamado el índice de Witt de E.*

Demostración. Si E es anisótropo, tomamos $E_a = E$ y $r = 0$. De lo contrario, si E es isótropo, por el teorema 3.5, E puede escribirse $E = \mathbb{H} \perp E_1$; si E_1 es anisótropo, el teorema está demostrado. En caso contrario, podemos escribir $E_1 = \mathbb{H} \perp E_2$ y $E \cong 2\mathbb{H} \perp E_2$. Luego de un número finito de pasos llegamos a la descomposición deseada $E \cong r\mathbb{H} \perp E_a$. Supongamos ahora que existe otra descomposición de E, $E \cong E_b \perp r'\mathbb{H}$, con $r \leq r'$ y E_b anisótropo. Entonces $E_a \perp r\mathbb{H} \cong E_b \perp r'\mathbb{H}$. Por el teorema 4.5, $E_a \cong E_b \perp (r'-r)\mathbb{H}$. Por ser E_a anisótropo, $r' - r = 0$. Por tanto $E_a \cong E_b$. □

Capítulo 5

Anillos de Witt

En este capítulo aplicaremos el Teorema de Cancelación de Witt para la construcción de un anillo que tendrá dos operaciones bien definidas: la suma ortogonal y el producto de Kronecker (producto tensorial) de formas cuadráticas regulares ($\perp$ y $\otimes$).[1] Veremos algunas propiedades del grupo de clases de cuadrados $\dot{K}/\dot{K}^2$ y la estrecha relación de este con el anillo de Witt sobre un cuerpo K. De aquí en adelante, cuando digamos K-forma, nos referiremos a una K-forma regular. Algo más: si el contexto es claro, escribiremos "$=$" para significar "$\cong$".

5.1. Definiciones preliminares

Definición 5.1. *Sea K un cuerpo. Definimos $M(K)$ como la colección de todas las clases de equivalencia de K-formas de grado n, con $n \in \mathbb{N}$.*

5.1.1. Producto de Kronecker de espacios cuadráticos

En esta subsección definiremos el producto tensorial de dos espacios cuadráticos, llamado también producto de Kronecker.

Definición 5.2. *Sean (E_1, B_1) y (E_2, B_2) espacios cuadráticos sobre K, de dimensiones m y n, respectivamente. Definimos un nuevo espacio vectorial $E = E_1 \otimes E_2$ ($\otimes = \otimes_K$), y sea $B : E \times E \longrightarrow K$ la única forma bilineal simétrica que satisface*

$$B(v_1 \otimes v_2, v_1' \otimes v_2') = B_1(v_1, v_1')B_2(v_2, v_2'), \qquad (v_i, v_i' \in E_i,\ i = 1, 2).$$

El par (E, B) es un nuevo espacio cuadrático sobre K de dimensión mn, al que llamaremos el producto tensorial de (E_1, B_1) y (E_2, B_2).

[1] En realidad, de clases de isometría de espacios cuadráticos, o equivalentemente, de clases de equivalencia de K-formas.

La aplicación cuadrática asociada $q = q_B$ satisface

$$\begin{aligned} q(v_1 \otimes v_2) &= B(v_1 \otimes v_2, v_1 \otimes v_2) \\ &= B_1(v_1, v_1)B_2(v_2, v_2) \\ &= q_1(v_1)q_2(v_2) \quad (v_i \in E_i,\ i = 1,2). \end{aligned}$$

Denotaremos q por $q_1 \otimes q_2$.[2]

Fijemos bases ordenadas $(b_1, ..., b_m)$ y $(c_1, ..., c_n)$ de E_1 y E_2, respectivamente. Sean $\alpha_{ij} = B_1(b_i, b_j)$, $\beta_{kl} = B_2(c_k, c_l)$. Entonces $M = (\alpha_{ij})$ y $N = (\beta_{kl})$ son las matrices simétricas asociadas a q_1 y q_2, respectivamente en las bases dadas. Ahora consideremos la base ordenada de $E = E_1 \otimes E_2$ dada por

$$\{b_1 \otimes c_1, b_1 \otimes c_2, ..., b_1 \otimes c_n, ..., b_m \otimes c_1, ..., b_m \otimes c_n\}.$$

La matriz [simétrica] de q con respecto a esta base será

$$M' = \begin{pmatrix} \alpha_{11}\beta_{11} & \alpha_{11}\beta_{12} & \cdots & \alpha_{12}\beta_{11} & \alpha_{12}\beta_{12} & \cdots & \cdots \\ \alpha_{11}\beta_{21} & \alpha_{11}\beta_{22} & \cdots & \alpha_{12}\beta_{21} & \alpha_{12}\beta 22 & \cdots & \cdots \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \ddots \\ \alpha_{21}\beta_{11} & \alpha_{21}\beta_{12} & \cdots & & \cdots & & \cdots \\ \vdots & \vdots & \ddots & & \cdots & & \cdots \end{pmatrix} = \begin{pmatrix} \alpha_{11}N & \alpha_{12}N & \cdots & \alpha_{1m}N \\ \alpha_{21}N & \alpha_{22}N & \cdots & \alpha_{2m}N \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{m1}N & \alpha_{m2}N & \cdots & \alpha_{mm}N \end{pmatrix}$$

que es precisamente el ordinario producto de Kronecker de dos matrices M y N. [3]

Ejemplo **5.1.** *Es inmediato que* $\langle\alpha\rangle \otimes \langle\beta\rangle \cong \langle\alpha\beta\rangle$ *para todos los* $\alpha, \beta \in K$.

Ejemplo **5.2.** *Sean* $f = \langle\alpha_1, ..., \alpha_m\rangle$ *y* $g = \langle\beta_1, ..., \beta_n\rangle$ K*-formas diagonales. Entonces, por definición,*

$$f \otimes g = \langle\alpha_1\beta_1, ..., \alpha_1\beta_n, \alpha_2\beta_1, ..., \alpha_m\beta_n\rangle.$$

Ejemplo **5.3.** *Sean* f, g K*-formas definidas por las matrices* $M_f = \begin{pmatrix} 1 & 3 \\ 3 & 1 \end{pmatrix}$ *y* $M_g = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 2 \\ 0 & 2 & 1 \end{pmatrix}$, *respectivamente. Entonces:*

$$M_{f\otimes g} = \begin{pmatrix} M_g & 3M_g \\ 3M_g & M_g \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 3 & 0 & 0 \\ 0 & 2 & 2 & 0 & 6 & 6 \\ 0 & 2 & 1 & 0 & 6 & 3 \\ 3 & 0 & 0 & 1 & 0 & 0 \\ 0 & 6 & 6 & 0 & 2 & 2 \\ 0 & 6 & 3 & 0 & 2 & 1 \end{pmatrix};\ y,$$

[2] También por $q_1 q_2$.

[3] Si f y g son las K-formas asociadas a las matrices M y N, respectivamente, definimos la forma $f \otimes g$, el producto tensorial de f y g, dada por la matriz M'.

$$M_{g\otimes f}=\begin{pmatrix} M_f & 0 & 0 \\ 0 & 2M_f & 2M_f \\ 0 & 2M_f & M_f \end{pmatrix}=\begin{pmatrix} 1 & 3 & 0 & 0 & 0 & 0 \\ 3 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 6 & 2 & 6 \\ 0 & 0 & 6 & 2 & 6 & 2 \\ 0 & 0 & 2 & 6 & 1 & 3 \\ 0 & 0 & 6 & 2 & 3 & 1 \end{pmatrix}.$$

Esto ocurre porque al realizar ambos productos, se toman diferentes bases [ordenadas]; sin embargo, es sencillo mostrar que ambas matrices, $M_{f\otimes g}$ y $M_{g\otimes f}$, son equivalentes.

Notemos que el producto tensorial de formas cuadráticas es conmutativo, asociativo y distributivo con respecto a la suma ortogonal. Veamos.

Proposición 5.1. *Sean q_1, q_2 y q_3 aplicaciones cuadráticas. Entonces*

(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) $q_1\otimes(q_2\perp q_3)\cong(q_1\otimes q_2)\perp(q_1\otimes q_3)$.

Demostración. (1) Sean (E_1,q_1) y (E_2,q_2) espacios cuadráticos sobre K. Es inmediato que la transformación $T:E_1\otimes E_2\longrightarrow E_2\otimes E_1$, definida por $v_1\otimes v_2\longmapsto v_2\otimes v_1$, es un isomorfismo lineal. Así, $E_1\otimes E_2\cong E_2\otimes E_1$.
(2) se prueba de manera similar.
Probemos *(3)*:

$$\begin{aligned}(q_1\otimes(q_2\perp q_3))(v_1,v_2,v_3)&=q_1(v_1)[(q_2\perp q_3)(v_2,v_3)]\\&=q_1(v_1)[q_2(v_2)+q_3(v_3)]\\&=q_1(v_1)q_2(v_2)+q_1(v_1)q_3(v_3)\\&=(q_1\otimes q_2)(v_1,v_2)\perp(q_1\otimes q_3)(v_1,v_3),\end{aligned}$$

para cualesquiera $v_i\in E_i$, $i=1,2,3$. □

Corolario 5.2. *Si q es cualquier aplicación cuadrática regular, entonces $q\otimes\mathbb{H}\cong(\dim q)\cdot\mathbb{H}$.*

Demostración. Por inducción sobre $\dim q$, queda reducida la demostración al caso $q=\langle a\rangle$, $a\neq 0$. Entonces, $\langle a\rangle\otimes\mathbb{H}=\langle a\rangle\otimes\langle 1,-1\rangle\cong\langle a,-a\rangle\cong\mathbb{H}$. □

Notación. Si n es un número entero no negativo y f es una K-forma, denotaremos

$$n\cdot f=f\perp f\perp\cdots\perp f,\quad (n \text{ veces}),$$

la suma ortogonal de n copias de f.[4]

[4] Hemos de ser precavidos con esta notación. En la literatura de formas cuadráticas, para $\alpha\in K$, muchos autores escriben $\alpha\cdot f$ denotando el producto tensorial $\langle\alpha\rangle\otimes f$. Esto genera ambigüedad. Por ejemplo, $3\cdot f$ significa $f\perp f\perp f$ pero también significaría $\langle 3\rangle\otimes f$. Nosotros, para evitar este inconveniente, escribimos $n\cdot f$ solo cuando n es un entero no negativo, para significar $f\perp\cdots\perp f$ (n veces) , y $n\cdot f$ en ninguna circunstancia significará $\langle n\rangle\otimes f$.

5.1.2. Grupo de Grothendieck

Sea $(M,+)$,[5] $M \neq \emptyset$, un monoide conmutativo y de cancelación, es decir cumple, para todos los $a,b,c \in M$:

i) $+ : M \times M \longrightarrow M$ es una ley de composición interna;

ii) $(a+b)+c = a+(b+c)$;

iii) $\exists e \in M,\ a+e=a$;

iv) $a+b=b+a$; y,

v) si $a+c=b+c$, entonces $a=b$.

Definición 5.3. *Definimos en $M \times M$ la relación $\sim$ dada por*

$$(a,b) \sim (c,d) \Longleftrightarrow a+d=c+b.$$

Proposición 5.3. *$\sim$ es una equivalencia en $M \times M$.*

Demostración. La reflexividad y simetría se deducen directamente de la definición de $\sim$. Probemos la transitividad. Sean $a,b,c,d,e,f \in M$. Si $(a,b) \sim (c,d)$ y $(c,d) \sim (e,f)$, entonces $a+d=c+b$ y $c+f=e+d$. Entonces

$$\begin{aligned} a+f+d &= a+d+f \\ &= c+b+f \\ &= c+f+b \\ &= e+d+b \\ &= e+b+d, \end{aligned}$$

entonces, por (v), $a+f=e+b$ o $(a,b) \sim (e,f)$. □

Definición 5.4. *Definimos en $M \times M$ la operación $\oplus$ como:*

$$(a,b) \oplus (c,d) = (a+c, b+d),$$

para $a,b,c,d \in M$.

Definición 5.5. *Definimos el Grupo de Grothendieck $\mathrm{Groth}(M)$ de M, como*

$$\mathrm{Groth}(M) = ((M \times M)/\sim, +)$$

cuya operación suma $+$ es definida como, dadas dos clases $[x],[y] \in (M \times M)/\sim$, $x=(a,b)$ y $y=(c,d)$,

$$[x]+[y]=[x \oplus y].$$

[5] Escribiremos algunas veces M para denotar $(M,+)$, para simplificar la notación.

En $\mathrm{Groth}(M)$, el elemento neutro es $[(e,e)]$ y, dado $[(a,b)] \in \mathrm{Groth}(M)$, su inverso es $-[(a,b)] = [(b,a)]$. La asociatividad y conmutatividad son heredadas de la estructura de $(M,+)$.

Ejemplo **5.4.** $\mathbb{N}$ *es un monoide conmutativo de cancelación. El grupo de Grothendieck* $\mathrm{Groth}(\mathbb{N})$ *es* $((\mathbb{N}\times\mathbb{N})/\sim,+) = (\mathbb{Z},+)$.

Definamos la aplicación $i : M \longrightarrow \mathrm{Groth}(M)$ como $i(x) = [(x,0)]$, llamada *inclusión*, que puede verse como una "inmersión" $M \subseteq \mathrm{Groth}(M)$. Notemos lo siguiente:

$$\begin{aligned} i(x) - i(y) &= [(x,0)] - [(y,0)] \\ &= [(x,0)] + [(0,y)] \\ &= [(x,0) \oplus (0,y)] \\ &= [(x,y)], \end{aligned}$$

entonces denotaremos $[(x,y)] = i(x) - i(y) = x - y$, siempre que no haya confusión. Sea ahora $f : M \longrightarrow G$ un morfismo, donde G es un grupo abeliano. Entonces f puede extenderse a un morfismo $[f] : \mathrm{Groth}(M) \longrightarrow G$ definido por $[f](x-y) = f(x) - f(y) \in G$. Esta es llamada la "propiedad universal" de $\mathrm{Groth}(M)$. Por último, supongamos que M tiene una multiplicación $\cdot : M \times M \longrightarrow M$ asociativa, conmutativa y distributiva respecto de la suma; junto con la suma, M es un semianillo y entonces la multiplicación induce una en $\mathrm{Groth}(M)$ dada por

$$[(x,y)] \cdot [(x',y')] = [(xx' + yy', yx' + xy')].$$

Luego $(\mathrm{Groth}(M), +, \cdot)$ es un anillo conmutativo.

5.2. $\widehat{W}(K)$ y $W(K)$

Definición 5.6. *Definimos el anillo Grothendieck de Witt de* K*-formas como*

$$\widehat{W}(K) = \mathrm{Groth}(M(K)).$$

Vemos que todo elemento de $\widehat{W}(K)$ se expresa como $f_1 - f_2$, donde f_1, f_2 son K-formas regulares. Consideremos el morfismo $\dim : M(K) \longrightarrow \mathbb{Z}$ dado por $f \longmapsto \dim f$. Este puede extenderse naturalmente a un morfismo $\dim = [\dim] : \widehat{W}(K) \longrightarrow \mathbb{Z}$ definido por

$$[\dim](f_1 - f_2) = \dim f_1 - \dim f_2.$$

El núcleo de este homomorfismo, denotado por $\widehat{I}K$, es llamado el *ideal fundamental* de $\widehat{W}(K)$. Puesto que $\mathrm{Im}(\dim) = \mathbb{Z}$, por el Teorema de isomorfismo, $\widehat{W}(K)/\widehat{I}K \cong \mathbb{Z}$.

Definición 5.7. $\mathbb{Z}\cdot\mathbb{H} = \{r\mathbb{H}; r \in \mathbb{Z}\}$ *es la colección de las formas (espacios) hiperbólicas (hiperbólicos).*

Corolario 5.4. $\mathbb{Z}\cdot\mathbb{H} = \{r\mathbb{H}; r \in \mathbb{Z}\}$ *es un ideal de* $\widehat{W}(K)$.

Demostración. Se deduce directamente del corolario 5.2. □

Definición 5.8. *Definimos el anillo de Witt $W(K)$ de un cuerpo K como:*

$$W(K) = \frac{\widehat{W}(K)}{\mathbb{Z}\cdot\mathbb{H}} \tag{5.1}$$

con las operaciones inducidas por $\perp$ y $\otimes$.

Proposición 5.5.

(1) Los elementos de $W(K)$ están en correspondencia unívoca con las clases de equivalencia de formas anisótropas.

(2) Dos K-formas f, f' representan el mismo elemento en $W(K)$ si, y solo si, $f_a \cong f'_a$.[6]

(3) Si $\dim f = \dim f'$, entonces f y f' representan el mismo elemento en $W(K)$ si, y solo si, $f \cong f'$.

Demostración. Hemos de probar solamente *(1)*. *(2)* y *(3)* se deducen directamente de *(1)*. Puesto que la forma $\mathbb{H}$ representa al 0 en $W(K)$, es decir, $0 = \langle 1,-1\rangle = \langle \alpha,-\alpha\rangle = \langle\alpha\rangle \perp \langle -\alpha\rangle = \langle\alpha\rangle + \langle -\alpha\rangle$ tenemos $-\langle\alpha\rangle = \langle -\alpha\rangle \in W(K)$ para todo $\alpha \in \dot{K}$. En particular, todo elemento de $W(K)$ es representado por *alguna* K-forma f. Esta se escribe de forma única, salvo isometría (equivalencia), como $f = r\mathbb{H} \perp f_a$, entonces f y f_a representan el mismo elemento en $W(K)$ (porque $r\mathbb{H} = 0 \in W(K)$, $\mathbb{Z}\cdot\mathbb{H}$ absorbe la parte hiperbólica de f). Así, cada elemento de $W(K)$ es representado por una K-forma anisótropa apropiada. Entonces, para la prueba de *(1)*, solo queda mostrar que si f y f' son K-formas anisótropas, entonces $f = f' \in W(K) \Rightarrow f \cong f'$. Si $f = f' \in W(K)$, entonces $f = f' + m\mathbb{H} \in \widehat{W}(K)$ para algún $m \in \mathbb{Z}$. Si $m \geq 0$, entonces tenemos una isometría $f \cong f' \perp m\mathbb{H}$, que implica $m = 0$ pues f es anisótropa y así $f \cong f'$. Si $m \leq 0$ entonces basta tomar $f' = f + (-m)\mathbb{H}$ y nuevamente tenemos $f' \cong f$. □

5.2.1. El ideal fundamental IK

Analicemos con más detalle el morfismo $\dim : \widehat{W}(K) \longrightarrow \mathbb{Z}$, con $\ker(\dim) = \widehat{I}K$. Veremos ahora que $\widehat{I}K$ es generado por expresiones "sencillas".

Proposición 5.6. *$\widehat{I}K$ es generado aditivamente por K-formas $\langle\alpha\rangle - \langle 1\rangle$, con $\alpha \in \dot{K}$.*

Demostración. Sea $f \in \widehat{I}K$, entonces tiene la forma $f = f_1 - f_2$, con $\dim f_1 = \dim f_2$. Expresando en sus formas diagonales, tenemos que $f_1 = \langle \alpha_1, ..., \alpha_n\rangle$ y $f_2 = \langle \beta_1, ..., \beta_n\rangle$ para algún $n \in \mathbb{N}$. Entonces:

$$f = \sum_{i=1}^{n} (\langle\alpha_i\rangle - \langle\beta_i\rangle) = \sum_{i=1}^{n} (\langle\alpha_i\rangle - \langle 1\rangle) - \sum_{i=1}^{n} (\langle\beta_i\rangle - \langle 1\rangle).$$

□

[6] En este caso, f y f' son llamados "similares según Witt".

Esta proposición nos indica que los elementos de $\widehat{I}K$ son K-formas de grado par. Analicemos ahora qué estructura tiene su imagen bajo la proyección natural $\pi : \widehat{W}(K) \longrightarrow W(K)$. Denotemos por IK a la imagen de $\widehat{I}K$ bajo el morfismo π. Como se tiene $\dim \mathbb{H} = 2$ y $\dim(\widehat{I}K) = 0$, claramente se cumple que $\mathbb{Z}\cdot\mathbb{H} \cap \widehat{I}K = \{0\}$; por tanto, dado $f \in \widehat{I}K$, la proyección natural $f \longmapsto f + \mathbb{Z}\cdot\mathbb{H}$ define un isomorfismo $\widehat{I}K \cong IK$.

Proposición 5.7. *Una forma f representa un elemento en $IK \leq W(K)$ si, y solo si, $\dim f$ es par.*

Demostración. ($\Rightarrow$) Si f representa un elemento en IK, entonces existe algún $m \in \mathbb{Z}$ tal que $f = f_1 - f_2 + m\mathbb{H} \in \widehat{W}(K)$, con $\dim f_1 = \dim f_2$. Entonces,

$$\dim f = \dim f_1 - \dim f_2 + \dim m\mathbb{H} = \dim m\mathbb{H} = 2m.$$

($\Leftarrow$) Supongamos ahora que f es de dimensión par, digamos $f = \langle \alpha, \beta \rangle$. Entonces f es claramente la imagen de $\langle \alpha \rangle - \langle -\beta \rangle \in \widehat{I}K$ bajo π, es decir, $f \in IK$. □

Vemos así que, IK particiona $W(K)$ en formas representantes de grado par o impar. Considerando nuevamente el morfismo $\dim : \widehat{W}(K) \longrightarrow \mathbb{Z}$, éste induce un epimorfismo $\dim_0 : W(K) \longrightarrow \mathbb{Z}_2$ (formas de dimensión par o impar); y, por la anterior proposición, el núcleo de este es IK. Entonces podemos concluir el siguiente resultado.

Corolario 5.8. $\dfrac{W(K)}{IK} \cong \mathbb{Z}_2$ *vía el morfismo* $\dim_0$.

Tenemos ahora las herramientas necesarias para estudiar la estructura de algunos anillos de Witt, dadas ciertas propiedades del cuerpo K subyacente.

5.3. Grupo de clases de cuadrados

En esta sección, estudiaremos las relaciones entre $W(K)$ y $\dot{K}/\dot{K}^2$, el grupo de clases de cuadrados de K.

Definimos, en el capítulo 3, el determinante de una forma f como un elemento $d(f)$ del grupo de clases de cuadrados $\dot{K}/\dot{K}^2$; y, por la proposición 3.1, $d : M(K) \longrightarrow \dot{K}/\dot{K}^2$ define un morfismo de semigrupos. Por la propiedad universal, este se extiende a un morfismo $d : \widehat{W}(K) \longrightarrow \dot{K}/\dot{K}^2$. Sin embargo, tenemos que $d(\mathbb{H}) = -1\dot{K}^2$, que no necesariamente es el neutro de $\dot{K}/\dot{K}^2$, es decir, podría representar una clase no nula de este. Entonces no tendría sentido siquiera considerar un morfismo entre $W(K)$ y $\dot{K}/\dot{K}^2$, vía d.

Definición 5.9. *Dada una forma $f \in M(K)$, definimos su determinante con signo $d_\pm$ mediante la ecuación*

$$d_\pm(f) = (-1)^{n(n-1)/2} d(f),$$

donde $n = \dim f$.

Con esta definición solucionamos el anterior inconveniente:

$$d_\pm(\mathbb{H}) = (-1)^{2(2-1)/2} d(\mathbb{H}) = (-1)(-1)\dot{K}^2 = 1 \cdot \dot{K}^2.$$

Sin embargo, esta aplicación presenta un nuevo problema. Veamos un ejemplo:

$$\begin{aligned} d_\pm(\langle \alpha_1, ..., \alpha_6 \rangle) &= (-1)^{6(6-1)/2} \alpha_1 \cdots \alpha_6 \dot{K}^2 \\ &= -\alpha_1 \cdots \alpha_6 \dot{K}^2; \text{ pero} \\ d_\pm(\langle \alpha_1 \rangle) \cdot d_\pm(\langle \alpha_2, ..., \alpha_6 \rangle) &= (-1)^{1(1-1)/2} \alpha_1 \dot{K}^2 \cdot (-1)^{5(5-1)/2} \alpha_2 \cdots \alpha_6 \dot{K}^2 \\ &= \alpha_1 \cdots \alpha_6 \dot{K}^2; \end{aligned}$$

entonces, no necesariamente se cumple que $d_\pm(f \perp g) = d_\pm(f) d_\pm(g)$. Así, $d_\pm$ no puede definir un morfismo de $W(K)$ en $\dot{K}/\dot{K}^2$. Solucionamos este problema extendiendo $\dot{K}/\dot{K}^2$ y combinando los morfismos $\dim_0$ y $\dim_\pm$.

Definición 5.10. *Sea $Q(K)$ el conjunto $\mathbb{Z}_2 \times \dot{K}/\dot{K}^2$. En él definimos la operación:*

$$(m, \alpha) \bullet (n, \beta) = (m, \alpha)(n, \beta) = (m + n, (-1)^{mn} \alpha\beta).$$

Es inmediato que $\bullet$ es asociativo y conmutativo. Por otra parte, $(m, \alpha)(0, 1) = (m, (-1)^{m \cdot 0} \alpha) = (m, \alpha)$, luego $(0, 1)$ actúa como neutro en $Q(K)$. Además, dado $(n, \alpha) \in Q(K)$,

$$(n, \alpha) \bullet (n, (-1)^n \alpha) = (n + n, (-1)^{n \cdot n} \alpha (-1)^n \alpha = (0, (-1)^{n(n+1)} \alpha^2) = (0, 1);$$

entonces, el inverso de (n, α) en $Q(K)$ es $(n, (-1)^n \alpha)$, y así, $(Q(K), \bullet)$ es un grupo [abeliano].

Consideremos ahora la sucesión exacta corta:

$$1 \longrightarrow \frac{\dot{K}}{\dot{K}^2} \xrightarrow{i} Q(K) \xrightarrow{\pi} \mathbb{Z}_2 \longrightarrow 0,$$ [7]

donde $i(\alpha) = (0, \alpha)$ y $\pi(n, \alpha) = n$ (la inclusión y la proyección natural). Evaluando al cuadrado los elementos de la imagen de i tenemos que $(0, \alpha)(0, \alpha) = (0, \alpha^2) = (0, 1)$, para todo $\alpha \in \dot{K}$; y, $(1, \alpha)(1, \alpha) = (1+1, (-1)^{1 \cdot 1} \alpha^2) = (0, -1 \cdot \alpha^2) = (0, -1)$, en particular, $(1, 1)^2 = (0, -1)$. Consideremos ahora el morfismo $f : \mathbb{Z}_2 \longrightarrow Q(K)$ dado por $f(0) = (0, 1)$ y $f(1) = (1, 1)$. Si -1 *es un cuadrado* en K, entonces $Q(K)$ es una extensión partible.[8]

Proposición 5.9. *La aplicación $(\dim_0, d_\pm) : M(K) \longrightarrow Q(K)$ determina un epimorfismo de monoides. Esta se extiende a un epimorfismo de grupos $(\dim_0, d_\pm) : \widehat{W}(K) \longrightarrow Q(K)$, el que se factoriza a través de $W(K)$ (es decir, se anula en $\mathbb{Z} \cdot \mathbb{H}$, luego induce un epimorfismo $W(K) \longrightarrow Q(K)$). Este último induce un isomorfismo de grupos $W(K)/I^2K \cong Q(K)$.*

Demostración. La aplicación definida en la anterior proposición lleva una forma f a

$$(\dim_0(f)), d_\pm(f)) \in Q(K).$$

[7] 1 y 0 representan al grupo trivial.

[8] Dada una sucesión exacta corta $0 \longrightarrow H \longrightarrow G \longrightarrow F \longrightarrow 0$, decimos que G es una extensión partible de H si existe un morfismo $f : F \longrightarrow G$ tal que $\pi \circ f = \mathrm{id}_F$, donde $\pi : G \longrightarrow F$.

Veamos que es efectivamente un homomorfismo de monoides. Dadas las formas f y f' de dimensiones n y n', respectivamente, tenemos que:

$$\begin{aligned}(\dim_0, d_\pm)(f)\cdot(\dim_0, d_\pm)(f') &= (n(\mathrm{mod}\ 2), (-1)^{n(n-1)/2}d(f))(n'(\mathrm{mod}\ 2), (-1)^{n'(n'-1)/2}d(f')) \\ &= (n+n'(\mathrm{mod}\ 2), (-1)^{nn'}(-1)^{[n(n-1)+n'(n'-1)]/2}d(f)d(f')) \\ &= (n+n'(\mathrm{mod}\ 2), (-1)^{[2nn'+n^2-n+n'^2-n']/2}d(f\perp f')) \\ &= (n+n'(\mathrm{mod}\ 2), (-1)^{(n+n')(n+n'-1)/2}d(f\perp f')) \\ &= (\dim_0, d_\pm)(f\perp f') \in Q(K).\end{aligned}$$

Más aún, $(\dim_0, d_\pm)$ es un epimorfismo. Lo verificamos como sigue:

$$(\dim_0, d_\pm)(\langle\alpha\rangle) = (1, \alpha\cdot\dot{K}^2) \text{ y } (\dim_0, d_\pm)(\langle 1,-\alpha\rangle) = (0, \alpha\cdot\dot{K}^2), \tag{5.2}$$

para todo $\alpha\in\dot{K}$. Nuevamente, por la propiedad universal de $\widehat{W}(K)$, $(\dim_0, d_\pm)$ se extiende de forma única a un *epimorfismo* de $\widehat{W}(K)$ a $Q(K)$, que se anula en $\mathbb{Z}\cdot\mathbb{H}$. Veamos:

$$(\dim_0, d_\pm)(\mathbb{H}) = (0, (-1)d(\mathbb{H})) = (0,1),$$

la identidad en $Q(K)$. Así $(\dim_0, d_\pm)$ induce un epimorfismo $\overline{(\dim_0, d_\pm)} : W(K)\longrightarrow Q(K)$. Ahora mostraremos que este se anula en I^2K. Por la proposición 5.7, IK es generado aditivamente por formas de grado par $\langle 1,\alpha\rangle$; así, I^2K es generado aditivamente por formas de dimensión 4, $\langle 1,\alpha\rangle\otimes\langle 1,\beta\rangle = \langle 1,\alpha,\beta,\alpha\beta\rangle$. Calculemos su imagen bajo $\overline{(\dim_0, d_\pm)}$:

$$\overline{(\dim_0, d_\pm)}(\langle 1,\alpha,\beta,\alpha\beta\rangle) = (0, (-1)^{4(4-1)/2}\alpha\cdot\beta\cdot\alpha\beta\cdot\dot{K}^2) = (0,1),$$

por tanto se anula en I^2K y así, obtenemos un epimorfismo $\varphi : W(K)/I^2K\longrightarrow Q(K)$. Construyendo una inversa de φ, mostraremos que este último es un isomorfismo. Definimos $\psi : Q(K)\longrightarrow W(K)/I^2K$ considerando las igualdades de la ecuación 5.2 como:

$$\psi(0,\alpha) = \langle 1,-\alpha\rangle(\mathrm{mod}\ I^2K), \quad \psi(1,\alpha) = \langle\alpha\rangle(\mathrm{mod}\ I^2K).$$

Realicemos ahora los cálculos necesarios, teniendo en cuenta que estamos operando en $W(K)$ módulo I^2K:

$$\begin{aligned}\psi[(0,\alpha)(0,\beta)] &= \psi(0,\alpha\beta) = \langle 1,-\alpha\beta\rangle = \langle 1,-\alpha\beta\rangle + \langle 1,-\alpha\rangle\otimes\langle 1,-\beta\rangle \\ &= \langle 1,-\alpha\beta\rangle + \langle 1,-\alpha,-\beta,\alpha\beta\rangle = \langle 1,-\alpha,1,-\beta\rangle \\ &= \psi(0,\alpha)+\psi(0,\beta)\ (\mathrm{mod}\ I^2K); \\ \psi[(1,\alpha)(1,\beta)] &= \psi(0,-\alpha\beta) = \langle 1,\alpha\beta\rangle = \langle 1,\alpha\beta\rangle + \langle 1,-\alpha\rangle\otimes\langle\beta,-1\rangle \\ &= \langle 1,\alpha\beta\rangle + \langle\beta,-1,-\alpha\beta,\alpha\rangle = \langle\alpha,\beta\rangle \\ &= \psi(1,\alpha)+\psi(1,\beta)\ (\mathrm{mod}\ I^2K); \\ \psi[(0,\alpha)(1,\beta)] &= \psi(1,\alpha\beta) = \langle\alpha\beta\rangle = \langle\alpha\beta\rangle + \langle 1,-\alpha\rangle\otimes\langle 1,\beta\rangle \\ &= \langle\alpha\beta\rangle + \langle 1,\beta,-\alpha,-\alpha\beta\rangle = \langle 1,-\alpha,\beta\rangle \\ &= \psi(0,\alpha)+\psi(1,\beta)\ (\mathrm{mod}\ I^2K).\end{aligned}$$

Así, ψ es un morfismo de grupos, que es suryectivo, pues, $\psi(1,\alpha)=\langle\alpha\rangle(\mathrm{mod}\ I^2K)$. Finalmente,

$$\begin{aligned}\varphi\circ\psi(0,\alpha)&=\varphi(\langle 1,-\alpha\rangle\ (\mathrm{mod}\ I^2K))\\&=\overline{(\dim_0,d_\pm)}(\langle 1,-\alpha\rangle(\mathrm{mod}\ I^2K))\\&=(0,(-1)(-\alpha))=(0,\alpha);\\\varphi\circ\psi(1,\alpha)&=\varphi(\langle\alpha\rangle(\mathrm{mod}\ I^2K))\\&=\overline{(\dim_0,d_\pm)}(\langle\alpha\rangle(\mathrm{mod}\ I^2K))\\&=(1,\alpha).\end{aligned}$$

Así, concluimos que ψ es inyectiva (pues tiene a φ como inversa a izquierda) y por tanto un isomorfismo con $\psi^{-1}=\varphi$. Dicho de otro modo, $W(K)/I^2K\cong Q(K)$. □

Hemos mostrado que $W(K)/I^2K$ y $Q(K)$ son isomorfos *como grupos*. Pero $W(K)/I^2K$ tiene estructura de anillo [conmutativo]. Esto sugiere que $Q(K)$ debe tener también estructura de *anillo*, vía φ. Dados $\alpha,\beta\in\dot{K}/\dot{K}^2$,definimos la multiplicación "$*$" como sigue:

$$\begin{aligned}(0,\alpha)*(0,\beta)&=(0,1);\\(0,\alpha)*(1,\beta)&=(0,\alpha);\\(1,\alpha)*(1,\beta)&=(1,\alpha\beta).\end{aligned}$$

Note que esta multiplicación depende solamente del grupo $\dot{K}/\dot{K}^2$.

Corolario 5.10. *Tenemos los siguientes resultados:*

(1) (Pfister) I^2K está constituido por clases de formas de dimensión par f para las cuales $d(f)=(-1)^{n(n-1)/2}$, con $n=\dim f$.

(2) (Pfister) La restricción de φ induce un isomorfismo entre IK/I^2K y $\dot{K}/\dot{K}^2$.

Demostración. (1) Es claro que si $f\in I^2K$, $\dim f$ es par y $d(f)=(-1)^{n(n-1)/2}$. Ahora, si f cumple ambas condiciones, $\overline{(\dim_0,d_\pm)}(f)=(0,(-1)^{n(n-1)/2}d(f))=(0,1)$, luego $f\in I^2K$.
(2) Si restringimos φ a IK, cuyos elementos son de la forma $\langle 1,\alpha\rangle$, sus imágenes serán de la forma $(0,\alpha)$, que como vimos, constituyen $\dot{K}/\dot{K}^2$. □

Corolario 5.11. *Las siguientes afirmaciones son equivalentes:*

(1) $\widehat{W}(K)$ es un anillo noetheriano.

(2) $W(K)$ es un anillo noetheriano.

(3) $\dot{K}/\dot{K}^2$ es un grupo finito.

Demostración. (1)⇒(2) es inmediato (el anillo cociente de un anillo noetheriano resulta noetheriano).
(2)⇒(3) Suponiendo $W(K)$ noetheriano, IK es un $W(K)$-módulo finitamente generado, luego IK/I^2K es un $W(K)/IK$-módulo finitamente generado. Recordemos que $W(K)/IK\cong$

$\mathbb{Z}_2$, por tanto $IK/I^2K \cong \dot{K}/\dot{K}^2$ debe ser finito.
(3)⇒(1) Por el Teorema de diagonalización 2.5, $\widehat{W}(K)$ es generado aditivamente por las formas $\langle\alpha\rangle$, $\alpha \in \dot{K}/\dot{K}^2$. Como $\dot{K}/\dot{K}^2$ es finito, tenemos que $\widehat{W}(K)$ es un grupo abeliano generado finitamente. Esto significa que, como anillo, $\widehat{W}(K)$ es noetheriano. □

En la siguiente sección estudiaremos algunos anillos de Witt sobre cuerpos concretos o con ciertas propiedades. Este estudio nos ayudará a ilustrar la teoría general.

5.4. Cálculos elementales

Empecemos estudiando los cuerpos K cuadráticamente cerrados, es decir, dado $\alpha \in K$, existe $\beta \in K$ tal que $\beta^2 = \alpha$.[9]

Proposición 5.12. *Son equivalentes:*

(1) K *es cuadráticamente cerrado.*

(2) $\dim : \widehat{W}(K) \longrightarrow \mathbb{Z}$ *es un isomorfismo de anillos.*

(3) $\dim_0 : W(K) \longrightarrow \mathbb{Z}_2$ *es un isomorfismo de anillos.*

Demostración. (1)⇒(2) Si K es cuadráticamente cerrado, entonces $\langle\alpha\rangle \cong \langle 1\rangle$ para cualquier $\alpha \in K$. Entonces, si f es de dimensión n, esta es equivalente a $n\langle 1\rangle$, así queda claro que $\dim$ es un isomorfismo de anillos (por la propiedad universal de $\widehat{W}(K)$).
(2)⇒(3) Es inmediato.
(3)⇒(1) Sea $\alpha \in \dot{K}$. Vía $\dim_0$, $W(K)$ tiene solo dos elementos preimágenes de $\mathbb{Z}_2$: $\langle 0\rangle$ y $\langle 1\rangle$ módulo $\mathbb{Z}\cdot\mathbb{H}$. Como α es no nulo, debe ser $\langle\alpha\rangle = \langle 1\rangle (\mathrm{mod}\, \mathbb{Z}\cdot\mathbb{H})$, es decir, $\langle\alpha\rangle = \langle 1\rangle + m\mathbb{H}$, con $m \in \mathbb{Z}$; entonces debe ser $m = 0$ y así $\langle\alpha\rangle = \langle 1\rangle$, es decir, α es un cuadrado en $\dot{K}$. □

Así, quedan caracterizados los anillos de Witt sobre cuerpos cuadráticamente cerrados.

Proposición 5.13. *Sea* $K = \mathbb{R}$. *Tenemos que:*

(1) Existen exactamente dos formas anisótropas (salvo isometría) para cada dimensión. Para $n > 0$, *estas son* $n\langle 1\rangle$ *y* $n\langle -1\rangle$;

(2) $W(\mathbb{R}) \cong \mathbb{Z}$;

(3) $\widehat{W}(\mathbb{R}) \cong \mathbb{Z} \oplus \mathbb{Z}$.

Demostración. (1) Puesto que $\dot{\mathbb{R}}/\dot{\mathbb{R}}^2 = \{1, -1\}$, toda forma f admite una diagonalización $f = \langle \alpha_1, ..., \alpha_n\rangle$, con $\alpha_i = 1$ o -1, $i = 1, ..., n$. Si f es anisótropa, queda claro que los signos no pueden alternarse en su diagonalización (de lo contrario contendría planos hiperbólicos y dejaría de ser anisótropa). Luego será $f = n\langle 1\rangle$ o $f = n\langle -1\rangle$.

[9] Note que todo cuerpo algebraicamente cerrado es automáticamente cuadráticamente cerrado, así que estos últimos ofrecen más ejemplos, los que no se tratarán en este trabajo.

(2) Por la proposición 5.5, $W(\mathbb{R})$ está en correspondencia biunívoca con las formas anisótropas; así, por *(1)*, $W(\mathbb{R})\cong\mathbb{Z}$.
(3) Para esta parte, mostraremos que $\widehat{W}(\mathbb{R})$ es un $\mathbb{Z}$-módulo libre de dimensión 2 Así, basta probar que $\{\langle 1\rangle,\langle -1\rangle\}$ es una base. Por *(1)*, es claro que $\langle 1\rangle$ y $\langle -1\rangle$ generan $\widehat{W}(\mathbb{R})$. Sean, entonces, $m,n\in\mathbb{Z}$ tales que $m\langle 1\rangle+n\langle -1\rangle=0$ (en $\widehat{W}(\mathbb{R})$). Llevando a $W(\mathbb{R})$ (es decir, módulo $\mathbb{Z}\cdot\mathbb{H}$), debemos tener $m=n$. Volviendo a $\widehat{W}(\mathbb{R})$, debe ser $m=n=0$, por tanto $\langle 1\rangle$ y $\langle -1\rangle$ son linealmente independientes. □

Nota. $\widehat{I}\mathbb{R}$ es generado por $\langle 1\rangle-\langle -1\rangle$.

En *(1)* de la anterior demostración, vimos que una forma f admite una diagonalización $f=\langle\alpha_1,...,\alpha_n\rangle$, con $\alpha_i=1$ o -1; reordenando tenemos que $f=\langle\beta_1,...,\beta_n\rangle$, con $\beta_1=...=\beta_r=1$ y $\beta_{r+1}=...=\beta_n=-1$. Note lo siguiente

$$0<r<n \;\Rightarrow\; f \text{ isótropa; y,}$$
$$r=0 \text{ o } r=n \;\Rightarrow\; f \text{ anisótropa.}$$

Definición 5.11. *Sea $s=n-r$. Definimos para la $\mathbb{R}$-forma f su signatura* $\operatorname{sig}(f)$ *como* $\operatorname{sig}(f)=r-s=$*(número de términos iguales a* 1*)*$-$*(número de términos iguales a* -1*).*

Proposición 5.14. *(Ley de inercia de Sylvester) Dos formas regulares sobre $\mathbb{R}$ son equivalentes si, y solo si, tienen la misma dimensión y la misma signatura.*

En otras palabras, que la signatura es independiente de la diagonalización de la forma en cuestión.

Demostración. Sean $r\langle 1\rangle\perp s\langle -1\rangle$ y $r'\langle 1\rangle\perp s'\langle -1\rangle$ dos diagonalizaciones de f, con $r'\geq r$. Entonces, llevando esta equivalencia al anillo de Witt, tenemos:

$$r\langle 1\rangle-s\langle 1\rangle=r'\langle 1\rangle-s'\langle 1\rangle;$$

teniendo en cuenta que $s=n-r$ y $s'=n-r'$, con $n=\dim f$; esto implica que $2r\langle 1\rangle=2r'\langle 1\rangle\in W(\mathbb{R})$. Por ser $W(\mathbb{R})\cong\mathbb{Z}$, debe ser $r=r'$. □

Así, podemos escribir $n_+=r$ (número de términos positivos) y $n_-=s$ (número de términos negativos). Luego,

$$\operatorname{sig}(f)=n_+-n_-=n_+-(n-n_+)=2n_+-n.$$

Estudiemos ahora los anillos de Witt sobre cuerpos finitos de característica >2. Sea $K=F_q$ el cuerpo finito de $q=p^m$ elementos (p primo mayor que 2). Sea $\alpha\in\dot{F}_q$ un generador de este. Dado que $\dot{K}$ es cíclico y de orden par $|\dot{K}|=q-1$, es claro que α^n con $0\leq n<q$, es un cuadrado si, y solo si, n es par. Así, $\dot{K}/\dot{K}^2$ tiene dos clases laterales. Denotaremos estas por 1 y ξ. Como $\alpha^{(q-1)/2}$ no es 1 y, elevado al cuadrado da 1, resulta $\alpha^{(q-1)/2}=-1$. Por tanto, -1 es un cuadrado si, y solo si, $(q-1)/2$ es par, es decir, $q\equiv 1(\mathrm{mod}\,4)$. En el otro caso, cuando $q\equiv 3(\mathrm{mod}\,4)$, podemos tomar $\xi=-1$.

Proposición 5.15. *En $K=F_q$ tenemos que toda forma regular binaria es universal.*

Demostración. Sea $\dot{K}/\dot{K}^2 = \{1, \xi\}$. Primero mostraremos que ξ puede tomarse como suma de dos cuadrados (como 1 y ξ son las únicas clases de cuadrados, esto equivale a decir que la forma $\langle 1,1\rangle$ es universal). Si -1 es un cuadrado en K (si $q \equiv 1 (\mathrm{mod}\, 4)$), entonces $\langle 1,1\rangle \cong \langle 1,-1\rangle = \mathbb{H}$ es universal. Cuando -1 no es cuadrado en K (es decir, $q \equiv 3 (\mathrm{mod}\, 4)$), tomamos $\xi = -1$. Consideremos los conjuntos $\dot{K}$ y $1+\dot{K}$ de K. Es claro que ambos son de orden $(q-1)/2$ y son distintos, pues, $1 \in \dot{K}^2 - (1+\dot{K}^2)$. Así, existe un elemento de la forma $1+\alpha^2$ que no está en $\dot{K}^2$. Tenemos que $1+\alpha^2 \neq 0$, pues de lo contrario, sería $\alpha^2 = -1$, contradiciendo la hipótesis. Entonces, $1+\alpha^2$ pertenece a la clase $\xi \cdot \dot{K}^2$, es decir, existe $\beta \in \dot{K}$ tal que $1+\alpha^2 = \xi\beta^2$, luego $\xi = (\beta^{-1})^2 + (\alpha\beta^{-1})^2$, es decir, la forma $\langle 1,1\rangle$ es universal. Ahora, dado que 1 y ξ son las únicas clases de cuadrados, hay como máximo tres formas diferentes (no equivalentes): $\langle 1,1\rangle$, $\langle 1,\xi\rangle$ y $\langle \xi,\xi\rangle$. Solo resta probar que las dos últimas son universales. $\langle 1,\xi\rangle$ obviamente representa a 1 y ξ, luego es universal. Por último, dado $\alpha \in \dot{K}$, existen $\beta_1, \beta_2 \in K$ tales que $\xi^{-1}\alpha = \beta_1^2 + \beta_2^2$ (recordemos que $\langle 1,1\rangle$ es universal). Entonces $\xi\beta_1^2 + \xi\beta_2^2 = \xi(\beta_1^2+\beta_2^2) = \xi\xi^{-1}\alpha = \alpha$. □

Lema 5.16. *En un cuerpo finito, toda forma ternaria es isótropa.*

Demostración. Sea $\langle \alpha,\beta,\gamma\rangle$ sobre F_q, entonces $\langle \beta,\gamma\rangle$ representa a $-\alpha$. Por el Criterio de representación, $\langle \beta,\gamma\rangle = \langle -\alpha,\xi\rangle$ para algún $\xi \in F_q$. Luego $\langle \alpha,\beta,\gamma\rangle = \langle \alpha,-\alpha,\xi\rangle = \mathbb{H} \perp \langle \xi\rangle$ es isótropa. □

Corolario 5.17. *Sea $K = F_q$ ($q = p^m$, $2 \neq p$ primo).*

(1) Si $q \equiv 1 (\mathrm{mod}\, 4)$, entonces existe un isomorfismo de anillos $W(K) \cong \mathbb{Z}_2[\dot{K}/\dot{K}^2]$.

(2) Si $q \equiv 3 (\mathrm{mod}\, 4)$, existe un isomorfismo de anillos $W(K) \cong \mathbb{Z}_4$.

Demostración. Ambas partes del corolario se deducen analizando la estructura de $Q(K)$, que esta es una extensión partible de $\dot{K}/\dot{K}^2$ cuando -1 es un cuadrado en K, y así, *(1)* se sigue directamente. Cuando -1 no es cuadrado en K, $Q(K)$ no es una extensión partible de $\dot{K}/\dot{K}^2$, de ese hecho se deduce *(2)* (en ambos casos $Q(K)$ es de orden 4). Sin embargo, podemos probar esto directamente sin recurrir a $Q(K)$. Para *(1)*, sea ξ el representante de la clase no trivial. Entonces, las formas anisótropas son $\langle 0\rangle$, $\langle 1\rangle$, $\langle \xi\rangle$ y $\langle 1,\xi\rangle$. Además, recordando que $\langle 1,1\rangle = \langle 1,-1\rangle = 0 \ (\mathrm{mod}\, \mathbb{Z}\cdot\mathbb{H})$, $W(K)$ es claramente isomorfo al anillo de grupo $\mathbb{Z}_2[\dot{K}/\dot{K}^2]$, identificando $\dot{K}/\dot{K}^2$ con $\{1,\xi\}$. Para *(2)*, con $\xi = -1$, las formas anisótropas son $\langle 0\rangle$, $\langle 1\rangle$, $\langle 1,1\rangle$ y $\langle -1\rangle = \langle 1,1,1\rangle (\mathrm{mod}\, \mathbb{Z}\cdot\mathbb{H})$, así queda claro que $W(K)$ es isomorfo a $\mathbb{Z}_4$. □

Nota. De acuerdo al anterior resultado, en el caso de cuerpos finitos, tratamos separadamente los casos $q \equiv 1 (\mathrm{mod}\, 4)$ y $q \equiv 3 (\mathrm{mod}\, 4)$, estudiando *sus anillos de Witt*. Sin embargo, ambos tienen el mismo anillo Grothendieck $\widehat{W}(K)$. Esto muestra la ventaja que $W(K)$ tiene sobre $\widehat{W}(K)$, que el primero muestra más propiedades de K que el segundo.

Conclusión

Definimos y establecimos una correspondencia uno-uno entre clases de isometría de espacios cuadráticos y clases de equivalencia de formas cuadráticas sobre un cuerpo K. Probamos el Teorema de diagonalización de la mano del Criterio de representación. Caracterizamos el plano hiperbólico y su directa relación con la isotropía del espacio considerado. Luego de definir la suma ortogonal de espacios, probamos los teoremas de Cancelación y Descomposición de Witt, que establecen que todo espacio E es isométrico a $E_a \perp r\mathbb{H}$, donde E_a y $r\mathbb{H}$ son sus partes anisótropa e hiperbólica, respectivamente y son únicos, salvo isometría. Definimos el producto tensorial de K-formas y construimos $\widehat{W}(K)$, el anillo Grothendieck de Witt; mostramos que $\mathbb{Z}\cdot\mathbb{H}$ es un ideal de $\widehat{W}(K)$; y, definimos el anillo de Witt $W(K)$ como $\dfrac{\widehat{W}(K)}{\mathbb{Z}\cdot\mathbb{H}}$. Luego estudiamos la estructura de $W(K)$ considerando el morfismo $\mathbf{dim}$ y el grupo de clases de cuadrados $\dot{K}/\dot{K}^2$. Finalmente, clasificamos las formas cuadráticas sobre cuerpos cuadráticamente cerrados, la colección de números reales y cuerpos finitos. Resumiendo, realizamos un estudio introductorio de los fundamentos de la teoría algebraica de formas cuadráticas.

Bibliografía

[1] T. Y. Lam. *Introduction to Quadratic Forms over Fields*. American Mathematical Society, Rhode Island, 2005.

[2] Francisco M. Piscoya H. *Estructuras algebraicas IV (Formas cuadráticas)*. Secretaría General de la Organización de los Estados Americanos, Washington, D.C., 1981.

[3] Jorge Alberto Guccione. *"Introducción a la teoría algebraica de formas cuadráticas"*.

[4] Satya Mandal. *Foundations of Quadratic Forms*. University of Kansas, 2013.

[5] Pete L. Clarck *Quadratic Forms Chapter I: Witt's Theory*.

[6] Huah-Chieh Li. *Quadratic Forms over $\mathbb{Q}_p$ and over $\mathbb{Q}$*.