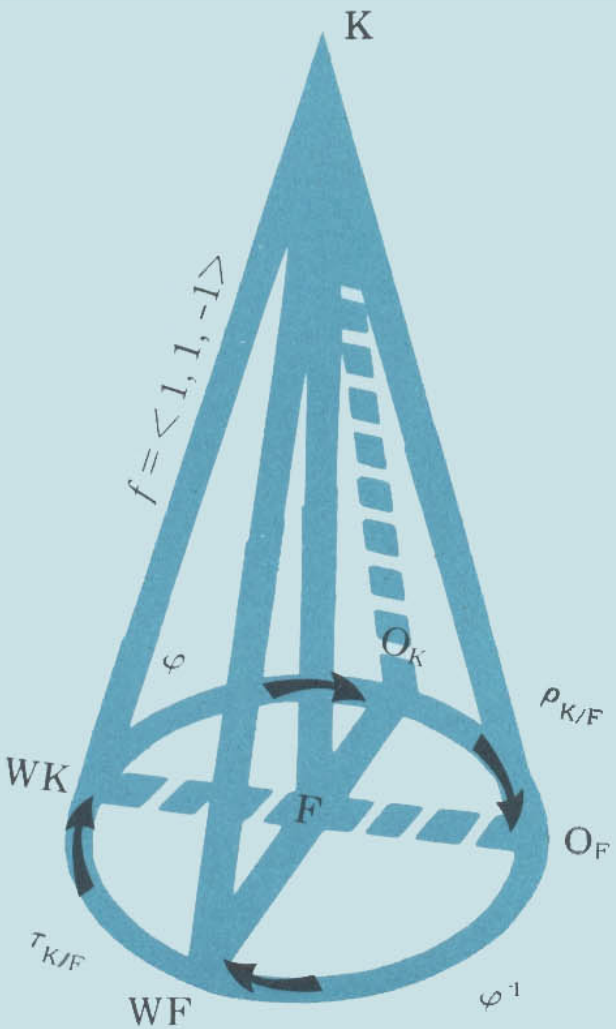
serie de matenática

monografía no. 23

ESTRUCTURAS ALGEBRAICAS VI (FORMAS CUADRATICAS)

Secretaría General de la
Organización de los Estados Americanos
Programa Regional de Desarrollo Científico y Tecnológico



ESTRUCTURAS ALGEBRAICAS VI (FORMAS CUADRATICAS)

por

Francisco M. Piscoya H.
Departamento de Matemática
Universidad Nacional Mayor de San Marcos
Lima, PERU

Secretaría General de la
Organización de los Estados Americanos
Programa Regional de Desarrollo Científico y Tecnológico
Washington, D.C. - 1981

Esta monografía ha sido preparada para su publicación en el Departamento de Asuntos Científicos y Tecnológicos de la Secretaría General de la Organización de los Estados Americanos

Editora: Eva V. Chesneau

Asesor Técnico: Dr. Héctor A. Merklen
Instituto de Matemática e Estatística
Cidade Universitária "Armando de Salles Oliveira"
São Paulo, Brasil

A los lectores

El programa de monografías científicas es una faceta de la vasta labor de la Organización de los Estados Americanos, a cargo del Departamento de Asuntos Científicos de la Secretaría General de dicha Organización, a cuyo financiamiento contribuye en forma importante el Programa Regional de Desarrollo Científico y Tecnológico.

Concebido por los Jefes de Estado Americanos en su Reunión celebrada en Punta del Este, Uruguay, en 1967, y cristalizado en las deliberaciones y mandatos de la Quinta Reunión del Consejo Interamericano Cultural, llevado a cabo en Maracay, Venezuela, en 1968, el Programa Regional de Desarrollo Científico y Tecnológico es la expresión de las aspiraciones preconizadas por los Jefes de Estado Americanos en el sentido de poner la ciencia y la tecnología al servicio de los pueblos latinoamericanos.

Demostrando gran visión, dichos dignatarios reconocieron que la ciencia y la tecnología están transformando la estructura económica y social de muchas naciones y que, en esta hora, por ser instrumento indispensable de progreso en América Latina, necesitan un impulso sin precedentes.

El Programa Regional de Desarrollo Científico y Tecnológico es un complemento de los esfuerzos nacionales de los países latinoamericanos y se orienta hacia la adopción de medidas que permitan el fomento de la investigación, la enseñanza y la difusión de la ciencia y la tecnología; la formación y perfeccionamiento de personal científico; el intercambio de informaciones, y la transferencia y adaptación a los países latinoamericanos del conocimiento y las tecnologías generadas en otras regiones.

En el cumplimiento de estas premisas fundamentales, el programa de monografías representa una contribución directa a la enseñanza de las ciencias en niveles educativos que abarcan importantísimos sectores de la población y, al mismo tiempo, propugna la difusión del saber científico.

La colección de monografías científicas consta de cuatro series, en español y portugués, sobre temas de física, química, biología y matemática. Desde sus comienzos, estas obras se destinaron a profesores y alumnos de ciencias de los primeros años de la universidad; de estos se tiene ya testimonio de su buena acogida.

Esta introducción brinda al Programa Regional de Desarrollo Científico y Tecnológico de la Secretaría General de la Organización de los Estados Americanos la ocasión de agradecer al doctor Francisco M. Piscoya, autor de esta monografía, y a quienes tengan el interés y buena voluntad de contribuir a su divulgación.

julio de 1981

ÍNDICE

	Página
A los Lectores	iii
Prólogo	1
CAPÍTULO 1. FORMAS CUADRÁTICAS Y ESPACIOS CUADRÁTICOS	5
1.1 Generalidades sobre Formas Cuadráticas y Espacios Cuadráticos	5
1.2 Suma Ortogonal de Espacios Cuadráticos	14
1.3 Teorema de Cancelación de Witt	16
1.4 Anillo de Witt	17
1.5 Formas de Pfister	20
Ejercicios	26
CAPÍTULO 2. FORMAS CUADRÁTICAS SOBRE EXTENSIONES ALGEBRAICAS DE CUERPOS	31
2.1 La Aplicación $r: WF \to WK$	31
2.2 La "Transferencia" de Scharlau	32
2.3 Extensiones de Grado Impar	33
2.4 Extensiones de Grado Par	34
2.5 Formas Cuadráticas sobre Extensiones de Galois	36
Ejercicios	39
CAPÍTULO 3. FORMAS CUADRÁTICAS SOBRE CUERPOS FORMALMENTE REALES Y PITAGÓRICOS	43
3.1 Conos Positivos y Cuerpos Ordenados	43
3.2 Extensión de Órdenes y Cuerpos Ordenados Maximales	46
3.3 Espacio de Órdenes	53
Ejercicios	61
CAPÍTULO 4. FORMAS CUADRÁTICAS SOBRE EXTENSIONES TRASCENDENTES Y CUERPOS DE FUNCIONES DE UNA FORMA CUADRÁTICA	67
4.1 Teorema de Cassels-Pfister	67
4.2 Cuerpo de Funciones de una Forma Cuadrática	71
Ejercicios	74

Página

APÉNDICE COMPLEMENTARIO AL CAPÍTULO 1. FORMAS CUADRÁTICAS SOBRE CUERPOS p-ÁDICOS 75

A. 1 Valuaciones y Valores Absolutos 75
A. 2 Topología Definida por una Valuación 76
A. 3 Cuerpo Residual de un Cuerpo p-ádico 77
A. 4 Clases Módulo Cuadrados de un Cuerpo Local 78
A. 5 Teorema de Springer para Cuerpos Locales 79
A. 6 El Teorema de Hasse-Minkowski para Q 82

APÉNDICE A. La Aplicación Traza 85

APÉNDICE B. Teorema Chino del Resto 87

BIBLIOGRAFÍA 89

ÍNDICE DE NOTACIONES 91

ÍNDICE DE TÉRMINOS 93

PRÓLOGO

La presente monografía es una introducción a la teoría algebraica de formas cuadráticas sobre cuerpos de característica distinta de 2. En la selección de los temas se ha supuesto que el lector conoce los principales temas tratados en las monografías de la subserie de álgebra de esta colección, así como tiene algunas nociones topológicas expuestas en la monografía no. 9 de la misma colección (serie de matemática).

Clásicamente se denomina forma cuadrática, de grado n, con coeficientes en un cuerpo F, a todo polinomio homogéneo, f, de grado 2 sobre F. Así, f se escribe $f = \sum a_{ij} X_i X_j$, $i, j = 1, \ldots, n$. Un problema importante de la teoría de formas cuadráticas es determinar cuando f posee ceros no triviales sobre F, es decir, determinar si existe $x = (x_1, \ldots, x_n) \in F^n$, $x \neq 0$ tal que $f(x) = f(x_1, \ldots, x_n) = \sum a_{ij} x_i x_j = 0$. Si f posee un cero no trivial sobre F, se dice que f es isótropa sobre F, en caso contrario que es anisótropa sobre F. La isotropía de una forma f depende de la estructura de la forma y del cuerpo en el cual tiene sus coeficientes (que supondremos siempre de característica distinta de 2). Así, por ejemplo, $f_1(X_1, X_2) = X_1^2 - X_2^2$ es isótropa sobre cualquier cuerpo F y $f_2(X_1, X_2) = X_1^2 - 2X_2^2$ es anisótropa sobre Q, cuerpo de los números racionales, pero isótropa sobre $Q(\sqrt{2})$. Se observa que la determinación de la isotropía de una forma f es en general un problema difícil. El punto de vista algebraico es "simplificar" f mediante transformaciones lineales de las "variables" que reduzcan f a una forma g más simple sobre la cual se pueda determinar la isotropía de f. Para ello se define la equivalencia de formas cuadráticas como sigue:

Dos formas cuadráticas f y g, de grado n, sobre F se dice que son equivalentes si existe una matriz inversible P de orden $n \times n$ sobre F, tal que $f(X) = g(P.X)$ (donde X denota el "vector" columna de filas $X_1, \ldots, X_n$). Esta relación es de equivalencia y expresa que g ha sido obtenida de f por una transformación lineal no singular de las indeterminadas $X_1, \ldots, X_n$. Si g tiene un cero no trivial sobre F, $c = (c_1, \ldots, c_n)$, entonces $P^{-1} \cdot c$ es un cero no trivial de f sobre F, pues $f(P^{-1} \cdot c) = g(P \cdot (P^{-1} \cdot c)) = g(c) = 0$, y por lo tanto se puede establecer que f es isótropa si, y sólo si, g es isótropa. Ahora bien, lo importante de la relación de equivalencia definida es que para una forma f se puede encontrar una forma g "diagonal", esto es, de la forma $g(X_1, \ldots, X_n) = a_1 X_1^2 + \ldots + a_n X_n^2$, tal que f es equivalente a g. Se observa que g es más fácil de "manejar" que f.

Ligado al problema de la determinación de la isotropía de una forma cuadrática f está el problema de determinar cuándo f representa un elemento dado d de F, es decir, dado d, determinar si existe $x = (x_1, \ldots, x_n) \in F^n$, $x \neq 0$, tal que $f(x) = d$. Si $d = 0$ es determinar la isotropía de f, si $d \neq 0$, la forma cuadrática de grado $n + 1$, $f(X_1, \ldots, X_n) - dX_{n+1}^2$ es isótropa. Además, si g equivale a f, f representa a $d \in F$,

implica que g también representa a d. O sea, representar un elemento sobre F (en particular la isotropía) es una propiedad de la clase de equivalencia de f. Es éste el enfoque de la teoría algebraica de formas cuadráticas: estudiar las propiedades de las clases de equivalencia de formas cuadráticas y por ello su problema central es clasificar las formas cuadráticas sobre un cuerpo dado, es decir determinar las condiciones necesarias y suficientes para decidir cuándo dos formas cuadráticas son equivalentes o no.

La riqueza de la estructura aritmética de los cuerpos considerados determina un amplio campo de investigación sobre el comportamiento de las clases de equivalencia de formas cuadráticas sobre ellos. En la actualidad, dicha investigación está orientada sobre todo al estudio de las clases de equivalencia sobre cuerpos ordenados y sobre extensiones trascendentes de un cuerpo dado. La teoría algebraica de formas cuadráticas tiene una larga y rica trayectoria histórica, ligada estrechamente a la teoría de los números, y a este respecto cabe señalar los trabajos de Pierre Fermat como los pioneros de la teoría moderna de formas cuadráticas (1601-1665). En los últimos años su desarrollo ha sido vigoroso debido principalmente a los trabajos del matemático alemán A. Pfister, quien recogió las ideas fundamentales de una célebre memoria de Witt (E. Witt: Theorie der quadratischen Formen in beliebigen Körpern, *J. Reine Angew. Math.*, **176**, 31-34, 1937). Witt demostró dos teoremas capitales, el teorema de cancelación (Teor. 1.3.2) y el teorema de descomposición (Corol. 1.3.3) que permitieron introducir la noción de anillo de Witt de formas cuadráticas sobre un cuerpo y obtener así una nueva caracterización de la equivalencia de formas cuadráticas, tal cual es "$f = g$ en el anillo de Witt y $\dim(f) = \dim(g)$ si, y sólo si, f es equivalente a g". A mediados de la década del 60, Pfister introdujo la teoría de formas multiplicativas, conocidas hoy como formas de Pfister, en el estudio del anillo de Witt, y en colaboración con Arason demostró uno de los resultados más importantes de la teoría conocido como el "hauptsatz" de Arason-Pfister (1971) (Teor. 4.2.2). La aplicación de la teoría de álgebras conmutativas posibilitada por la estructura de anillo permitió progresos considerables en el estudio de los cuerpos formalmente reales, teoría que tuvo su origen en los trabajos de Artin y Schreier (Algebraische Konstruktion reeller Körper, *Abh. Math. Sem. Univ. Hamburg*, **5**, 85-89, 1926) vinculados al famoso problema 17 de Hilbert. En los últimos años, Cassels, Pfister, Knebush y Arason han desarrollado fuertemente la teoría de formas cuadráticas sobre extensiones trascendentes, siendo de especial significación los trabajos de Knebush sobre cuerpos genéricos de ceros de una forma cuadrática (véase la cita 8 de la bibliografía).

Teniendo presente los diversos aspectos del desarrollo histórico de la teoría de formas cuadráticas, la presente exposición parte del concepto clásico de forma cuadrática y a lo largo de los diferentes capítulos trata de la construcción del anillo de Witt, del estudio de las formas cuadráticas sobre cuerpos reales, cuerpos p-ádicos, extensiones algebraicas, extensiones trascendentes y, finalmente, en forma breve del cuerpo de funciones de una forma cuadrática.

Al final de cada capítulo se dan ejercicios, algunos de aplicación inmediata a los temas expuestos, otros complementarios de aspectos

importantes de la teoría que no se han podido desarrollar debido a las limitaciones de esta monografía. Para ampliar el panorama y profundizar algunos de los temas aquí tratados se recomienda al lector consultar las obras citadas en (9), (10) y (14) de la bibliografía.

1

FORMAS CUADRÁTICAS Y ESPACIOS CUADRÁTICOS

1.1. GENERALIDADES SOBRE FORMAS CUADRÁTICAS Y ESPACIOS CUADRÁTICOS

Definición 1. Por forma cuadrática de grado n sobre un cuerpo F se entiende un polinomio homogéneo de grado 2 en n indeterminadas.

Si f es una forma cuadrática de grado n sobre F, nos referiremos también a f como una F-forma de grado n, o como una F-forma de dimensión n. Así, si f es F-forma de dimensión n, se escribe:

$$f(X_1, \ldots, X_n) = \sum_{1 \leq i, j \leq n} a_{ij} X_i X_j \qquad [1]$$

donde los $a_{ij} \in F$. Escribiendo $b_{ij} = 1/2(a_{ij} + a_{ji})$ se tiene:

$$f(X_1, \ldots, X_n) = \sum_{1 \leq i, j \leq n} b_{ij} X_i X_j \qquad [2]$$

donde $b_{ij} = b_{ji}$. Esta representación es la usual si se trata de una F-forma de grado n, y resulta claro que se puede asociar a f una matriz simétrica con sus coeficientes en F, la que se denotará por m_f: $m_f = (b_{ij})$. Recíprocamente, si (b_{ij}) es una $n \times n$ matriz simétrica con coeficientes en F, entonces (b_{ij}) define, mediante la fórmula [2], una F-forma de grado n.

Consideremos el vector columna

$$X = \begin{pmatrix} X_1 \\ \cdot \\ \cdot \\ \cdot \\ X_n \end{pmatrix}$$

en notación matricial la expresión [2] para f será:

$$f(X) = X^t m_f X \qquad [3]$$

donde X^t es el transpuesto del vector columna X.

Definición 2. Sean f y g F-formas de grado n. Se dice que "f es equivalente a g", y se escribe $f \simeq g$, si existe una matriz inversible A de tipo $n \times n$, con coeficientes en F, tal que $g(AX) = f(X)$, esto es, f se obtiene de g por una transformación lineal no singular de las indeterminadas $X_1, \ldots, X_n$.

Es fácil ver que la relación definida es de equivalencia. Además de [3] se obtiene que si $f \simeq g$:

$$g(AX) = (AX)^t m_g(AX) = X^t A^t m_g AX = X^t(A^t m_g A)X = f(X);$$

luego $f \simeq g$ si, y sólo si, $m_f = A^t m_g A$.

Ejemplo 1.

a) Considérese $g(X_1, X_2) = X_1X_2$, luego:

$$g(X_1, X_2) = 1/2\,X_1X_2 + 1/2\,X_2X_1 = (X_1, X_2)\begin{pmatrix} 0 & 1/2 \\ 1/2 & 0 \end{pmatrix}\begin{pmatrix} X_1 \\ X_2 \end{pmatrix}.$$

Si $f(X_1, X_2) = X_1^2 - X_2^2$ y $A = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, se observa que:

$$g(AX) = (X_1, X_2)\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1/2 \\ 1/2 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} X_1 \\ X_2 \end{pmatrix} = X_1^2 - X_2^2,$$

esto es, $f \simeq g$.

b) Sea $f(X) = X_1^2 + X_3^2 - 2X_1X_2 - 2X_1X_3 + 10X_2X_3$, y
$g(X) = X_1^2 - X_2^2 + 8X_2X_3$,

el cálculo directo muestra que $f \simeq g$ a partir de la matriz

$$A = \begin{bmatrix} 1 & -1 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad \text{y se observa que } m_g = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 4 \\ 0 & 4 & 0 \end{bmatrix}.$$

Definición 3. Sea V un espacio vectorial de dimensión finita sobre F; una forma bilineal simétrica sobre V es una aplicación $B: V \times V \to F$, lineal en ambos argumentos y que verifica $B(x, y) = B(y, x)$, $\forall\, x, y \in V$.

De la bilinealidad y simetría se deduce fácilmente la siguiente relación:

$$B(x + y,\ x + y) = B(x, x) + B(y, y) + 2B(x, y).$$

Si la característica de F es distinta de 2, se obtiene:

$$B(x, y) = 1/2\,(B(x + y,\ x + y) - B(x, x) - B(y, y))$$

$\forall\, x, y \in V$. Esta igualdad se conoce como la *identidad polar* y establece que una forma bilineal simétrica está determinada totalmente cuando se conoce la forma bilineal sobre la "diagonal" de $V \times V$.

Si B es una forma bilineal simétrica sobre un espacio vectorial V, se define $q_B: V \to F$ por $q_B(x) = B(x, x)$. Se obtiene de inmediato que q_B verifica las siguientes propiedades:

a) $q_B(ax) = a^2 q_B(x)$, $\forall\, a \in F,\ x \in V$.

b) $2B(x, y) = q_B(x + y) - q_B(x) - q_B(y)$, $\forall\, x, y \in V$.

Luego la aplicación $(x, y) \to q_B(x + y) - q_B(x) - q_B(y)$ es una aplicación bilineal de $V \times V$ en F.

Definición 4. Sean V un espacio vectorial de dimensión finita sobre F y $q: V \to F$ una aplicación que verifica:

1) $q(\alpha x) = \alpha^2 q(x)$, $\forall\, \alpha \in F$, $x \in V$.

2) $(x,y) \to q(x+y) - q(x) - q(y)$ es una aplicación bilineal de $V \times V$ en F.
Entonces se denomina a q una aplicación cuadrática sobre V.

Previamente a la definición se observó que toda aplicación bilineal simétrica $B: V \times V \to F$ define una aplicación cuadrática q_B tal que $q_B(x) = B(x,x)$. Recíprocamente, si se supone que la característica de F no es 2, entonces toda aplicación cuadrática $q: V \to F$ define una forma bilineal simétrica $B: V \times V \to F$ por $B(x,y) = 1/2\,(q(x+y) - q(x) - q(y))$. Es inmediato verificar que B es bilineal simétrica. Además se tiene que $B(x,x) = q(x)$, pues de la definición de B resulta que $B(x,x) = 1/2(q(2x) - 2q(x)) = 1/2\,(4q(x) - 2q(x)) = q(x)$.

De lo expuesto se deduce que, para un cuerpo F de característica distinta de 2, toda forma bilineal simétrica B sobre un espacio vectorial V (de dimensión finita) sobre F, define en forma única una aplicación cuadrática $q: V \to F$ y, recíprocamente, toda aplicación cuadrática define una forma bilineal simétrica de manera única. En esta monografía se supone que F tiene característica distinta de 2, salvo aclaración expresa de lo contrario, por lo tanto las aplicaciones cuadráticas se identificarán con las formas bilineales simétricas respectivas.

Definición 5. Se define un espacio cuadrático como un espacio vectorial V de dimensión finita sobre F, cuerpo de característica distinta de 2, provisto de una aplicación cuadrática $q: V \to F$.

Se denota el espacio cuadrático V provisto de la aplicación cuadrática q por (V,q) o también por (V,B), donde B es la forma bilineal correspondiente a q.

Nota. Supongamos que (V,B) es un F-espacio cuadrático, $v_1, \ldots, v_n$ una base de V. La matriz de B relativa a la base considerada es (b_{ij}) de orden n, donde $b_{ij} = B(v_i, v_j) \in F$. Si $x \in V$, $x = \sum_{i=1}^{n} x_i v_i$, $x_i \in F$, entonces:

$$q(x) = B(x,x) = B\Big(\sum_{i=1}^{n} x_i v_i,\ \sum_{j=1}^{n} x_j v_j\Big) = \sum_{i,j} b_{ij} x_i x_j.$$

Por otra parte, se sabe que la matriz (b_{ij}) define una forma cuadrática $f(X_1, \ldots, X_n) = \sum_{i,j} b_{ij} X_i X_j$. En consecuencia, especializando las indeterminadas X_i por $x_i \in F$ se obtiene que $f(x_1, \ldots, x_n) = q(x)$, esto es, fijada la base de V, la aplicación cuadrática q es la especialización de una forma cuadrática f en las coordenadas de todo $x \in V$. Por esta relación es frecuente también definir una forma cuadrática como una aplicación cuadrática.

Ejemplo 2. Sea f una F-forma de dimensión n. (F^n, B_f), donde F^n es el F-espacio vectorial de las n-uplas ordenadas de elementos de F y

$B_f : F^n \times F^n \to F$ se define por $B_f(e_i, e_j) = b_{ij}$, donde $m_f = (b_{ij})$ y $e_1, \ldots, e_n$ es la base canónica de F^n. Se observa que si $x \in F^n$, se tiene la relación:

$$f(x) = f(x_1, \ldots, x_n) = x^t \cdot m_f \cdot x = B_f(x, x) = q_f(x). \qquad [4]$$

Se tiene también de [3] y de la identidad polar

$$B_f(x, y) = x^t \cdot m_f \cdot y, \ \forall\, x, y \in F^n. \qquad [5]$$

Sea (V, B) un F-espacio cuadrático, elegida una base $v_1, \ldots, v_n$ de V, la matriz de B define una forma cuadrática $f_B = \sum_{i,j} b_{ij} X_i X_j$, donde $b_{ij} = B(v_i, v_j)$. Supóngase que $w_1, \ldots, w_n$ es otra base de V y f'_B es la forma cuadrática definida por B en relación con esta nueva base. Se afirma que las F-formas f_B y f'_B son equivalentes. Para ver esto, considérese $w_j = \sum_{i=1}^{n} c_{ij} v_i$, entonces:

$$(m_{f'_B})_{ij} = B(w_i, w_j) = B\Big(\sum_{k=1}^{n} c_{ki} v_k, \sum_{s=1}^{n} c_{sj} v_s\Big) = \sum_{k,s} c_{ki} B(v_k, v_s) c_{sj}$$

$$= (C^t \cdot m_{f_B} \cdot C)_{ij}, \text{ donde } C = (c_{ij}).$$

Se tiene entonces que $m_{f'_B} = C^t \cdot m_{f_B} \cdot C$.

Definición 6. Se dice que dos espacios cuadráticos sobre F, (V_1, B_1) y (V_2, B_2), son isométricos y se denotan por $V_1 \simeq V_2$, si existe un F-isomorfismo lineal $t : V_1 \to V_2$, que satisface la relación $B_2(t(x), t(y)) = B_1(x, y)$ para todo x, y en V.

Adviértase que la isometría es una relación de equivalencia.

Ejemplo 3. Sean f y g F-formas equivalentes de dimensión n. Los espacios cuadráticos (F^n, B_f) y (F^n, B_g), definidos en el ejemplo 2, son isométricos. Existe una matriz inversible C tal que $g(C \cdot X) = f(X)$, y se define $t : F^n \to F^n$ por $t(x) = C \cdot x$. Luego, $B_g(t(x), t(y)) = B_g(C \cdot x, C \cdot y) = (C \cdot y)^t \cdot m_g \cdot (C \cdot x)$ de [5]; esto es $B_g(t(x), t(y)) = y^t \cdot (C^t \cdot m_g \cdot C) \cdot x = y^t \cdot m_f \cdot x = B_f(x, y)$.

Ejemplo 4. Sean (V, B) un F-espacio cuadrático y $v_1, \ldots v_n$ una base de V; definamos la F-forma f_B y consideremos el F-espacio cuadrático (F^n, B_{f_B}) tal como en el ejemplo 2. Sea $t : V \to F^n$ tal que $t(v_i) = e_i$, $i = 1, \ldots, n$, donde $e_1, \ldots, e_n$ denota la base canónica de F^n. Así, t es un isomorfismo de V sobre F^n. Además:

$$B_{f_B}(t(v_i), t(v_j)) = B_{f_B}(e_i, e_j) = \text{coef. } (i, j) \text{ de } f_B = B(v_i, v_j).$$

Con lo que se ha demostrado que t es una isometría entre (V, B) y (F^n, B_{f_B}).

Proposición 1.1.1. Existe correspondencia biyectiva entre las clases de equivalencia de formas cuadráticas de grado n sobre F y las clases de isometría de espacios cuadráticos sobre F de dimensión n.

Demostración. Denotemos por (f) la clase de equivalencia representada por f y asignemos a (f) la clase de isometría correspondiente al espacio cuadrático (F^n, B_f) (Ejemplo 2). Esta correspondencia es bien definida, pues si $g \simeq f$, entonces $(F^n, B_g) \simeq (F^n, B_f)$ según el ejemplo 3. Por otra parte, a la clase de isometría de un F-espacio (V, B) asociamos la clase (f_β): si $(V', B') \simeq (V, B)$, entonces $f_{\beta'} \simeq f_\beta$ (si $v_1, \ldots, v_n$ es la base de V fijada para definir f_β, consideramos $t(v_1), \ldots, t(v_n)$ la base de V' para definir $f_{\beta'}$, donde $t: V \to V'$ es la isometría entre V y V'). Es fácil verificar que esta correspondencia es una biyección.

Como consecuencia de esta proposición se procede a identificar las clases de isometría de espacios cuadráticos con las correspondientes clases de equivalencia de F-formas, identificación que constituye la "linealización" del problema de estudiar las propiedades de las clases de equivalencia de formas cuadráticas sobre cuerpos. Por lo mencionado, en lo sucesivo nos referiremos indistintamente a las formas cuadráticas o a los espacios cuadráticos.

Un problema importante en la teoría de formas cuadráticas es determinar las condiciones para que una F-forma f de dimensión n represente no trivialmente al cero, esto es encontrar condiciones, ya sea sobre el cuerpo de coeficientes o sobre la forma f, para que existan $x_1, \ldots, x_n \in F$ no todos nulos tales que $f(x_1, \ldots, x_n) = 0$. Si f representa no trivialmente al cero, se dice que f es *isótropa* sobre F y todo $x = (x_1, \ldots, x_n)$, $x \neq 0$ tal que $f(x) = 0$ se llama *vector isótropo* para f. Se observa que:

a) Si f y g son F-formas y $f \simeq g$, entonces f isótropa implica g isótropa.

b) Sea (V, B) un F-espacio cuadrático correspondiente a (f), donde f es isótropa; se dice entonces que (V, B) es un espacio isótropo. En este caso, existe un vector $v \neq 0$ tal que $B(v, v) = 0$ (basta considerar $t: F^n \to V$ la isometría de (F^n, B_f) con (V, B) y tomar $v = t(x)$, donde x es vector isótropo de f).

Si f es F-forma no isótropa, se dice que f es *anisótropa*.

Lo observado en a) significa que la propiedad de ser isótropa de una forma f es una propiedad de la clase de f. Propiedades de esta naturaleza son las que nos interesa en el estudio que vamos a realizar y en vista de ello uno de los pasos iniciales más importantes es encontrar en (f) un elemento que tenga expresión lo más simple posible a fin de estudiar en él las propiedades de la clase. En este sentido demostraremos que toda forma f es equivalente a una forma diagonal, es decir a una forma cuya matriz asociada es una matriz diagonal. Previamente haremos algunas consideraciones.

Sea (V, B) un F-espacio cuadrático y $x, y \in V$, se dice que x es ortogonal a y si $B(x, y) = 0$. Si U es un F-subespacio de V, se define:

$$U^\perp = \{y \in V / B(x, y) = 0 \ \forall \ x \in U\},$$

$U^\perp$ se llama el complemento ortogonal de U y es fácil verificar que $U^\perp$ es un subespacio de V. $V^\perp$ se llama el *radical* de V y se denota por $r(V)$.

Se dice que (V,B) es regular cuando $r(V) = 0$, esto es, el único vector en V ortogonal a todo el espacio es el vector cero. Se observa que:

a) La regularidad es propiedad de la clase de isometría.

b) Si (V,B) tiene una base ortogonal (es decir, los vectores de la base son ortogonales dos a dos), que contiene un vector isótropo, entonces V no es regular.

c) El espacio trivial reducido a 0 es regular ($r(0) = 0$).

Ejemplo 5. Sea (F^2,B), donde $B((x_1,x_2),(y_1,y_2)) = x_2y_2$. B es forma bilineal simétrica cuya matriz asociada en la base canónica es $\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$ y $f_B(X_1,X_2) = X_2^2$. Además, $r(F^2) = \{(x,0)/x \in F\}$, luego (F^2,B) no es regular, pero $U = \{(0,x)/x \in F\}$ es un subespacio regular. En consecuencia, espacios cuadráticos no regulares pueden tener subespacios regulares. También espacios regulares pueden tener subespacios no regulares; por ejemplo, (F^2,B), donde B se define por $B'((x_1,x_2),(y_1,y_2)) = x_1y_2 + x_2y_1$. En este caso $r(F^2) = 0$, pero $U = \{(x,0)/x \in F\}$ es no regular (obsérvese que $U = U^\perp$).

Teorema 1.1.2. Todo espacio cuadrático (V,B) admite una base ortogonal.

Demostración. Escribamos $V = r(V) \oplus W$. El subespacio cuadrático (W,B'), donde B' es la restricción de B a W es regular, pues si $x \in W$ es tal que $B'(x,W) = 0$, entonces como todo $y \in V$ se escribe $y = u + v$ con $u \in r(V)$ y $v \in W$, se tiene:

$$B(x,y) = B(x,u) + B(x,v) = B'(x,v) + B(x,u) = 0;$$

entonces $x \in r(V) \cap W = 0$. Por tanto, basta demostrar el teorema para el caso en que V es regular, pues ello daría una base ortogonal para W, la misma que se puede completar con una base de $r(V)$. Reducidos al caso regular se procede por inducción sobre la dimensión del espacio. Si $\dim(V) = 0$, la conclusión es trivial. Supóngase que el teorema es válido para todo espacio regular de dimensión n y sea V de dimensión $n + 1$. Sea $v \in V$ tal que $B(v,v) \neq 0$ (tal vector existe por la regularidad y la identidad polar); veamos que $V = Fv \oplus (F \cdot v)^\perp$, lo que nos permitirá aplicar la hipótesis inductiva a $(F \cdot v)^\perp$ y la base obtenida para este subespacio, completada con v, nos proporcionará la base ortogonal para V. Si $w \in (F \cdot v)^\perp$ y $B(w,(F \cdot v)^\perp) = 0$, entonces $B(w,V) = 0$, y en consecuencia $w = 0$. Por tanto, $(F \cdot v)^\perp$ es regular. $Fv \cap (Fv)^\perp = 0$ es inmediato y por último si $x \in V$ podemos observar que $B(x - \frac{B(x,v)}{B(v,v)}v, v) = 0$, lo que demuestra que $Fv + (Fv)^\perp$ es igual a V.

Observación. Dado un F-espacio cuadrático (V,B), de la demostración del teorema se deduce que dado un vector v no isótropo se puede construir una base ortogonal que incluya al vector v.

Sea f una F-forma de dimensión n; decimos que un elemento $d \in F - \{0\} = \dot{F}$ *es representado por* f si existen $x_1,\ldots,x_n$ tales que $f(x_1,\ldots,x_n) = d, x_i \in F$. El conjunto de los elementos $\dot{F}$ representados por f se de-

nota por $D_F(f)$. Si f y g son F-formas isométricas, entonces $D_F(f) = D_F(g)$; lo recíproco no es verdadero. Sea (V, B) un F-espacio correspondiente a (f), entonces si $a \in D_F(f)$, existe un vector $v \in V$ tal que $q_B(v) = a$ y recíprocamente; por lo tanto, $D_F(f) = \{a \in \dot{F}$ existe $v \in V$ con $q_B(v) = a\}$. Por la observación realizada utilizamos también la notación $D_F(V)$ para referirnos a $D_F(f)$.

Consideremos f una F-forma de dimensión n. Sea $a_1 \in \dot{F}$ un elemento representado por f, entonces para cualquier F-espacio cuadrático correspondiente a (f) existe un vector v tal que $B(v, v) = a_1$, donde (V, B) es el F-espacio cuadrático elegido. Por la observación al teorema, existe una base ortogonal $v_1 = v, v_2, \ldots, v_n$ de V que incluye a v, mediante la cual se define la forma cuadrática f_B cuya matriz es $(B(v_i, v_j))$. Se tiene que $f_B \simeq f$. En consecuencia f es equivalente a una forma cuadrática cuya matriz es diagonal y contiene como primer término el elemento a_1 y llamando $a_2 = B(v_2, v_2), \ldots, a_n = B(v_n, v_n)$ se obtiene que:

$$m_f = \begin{bmatrix} a_1 & & \\ & \ddots & \\ & & a_n \end{bmatrix} \qquad [6]$$

lo que usualmente se denota $f \simeq \langle a_1, \ldots, a_n \rangle$ y se conoce como la representación diagonal de la F-forma f.

En términos de polinomios [6] significa que f, bajo isometría, es el polinomio $a_1 X_1^2 + \ldots + a_n X_n^2$, y en consecuencia del ejemplo 1 tenemos que $X_1 X_2 \simeq \langle 1, -1 \rangle$.

Si $f \simeq \langle a_1, \ldots, a_n \rangle$ es F-forma, cabe observar que si existe un $a_i = 0$, entonces f no es regular (entendiéndose la clase de espacios cuadráticos asociada a (f) no es regular), ya que una base ortogonal contendría un vector isótropo para f. Recíprocamente, si existe una representación diagonal para f con todos los términos no nulos, entonces es posible obtener una base ortogonal $v_1, \ldots, v_n$ en un (V, B) correspondiente, tal que $B(v_i, v_i) = a_i \neq 0$, $i = 1, \ldots, n$. Sea $v \in V$ tal que $B(v, V) = 0$; expresando $v = a_1 v_1 + \ldots + a_n v_n$ resulta $B(v, v_j) = a_j a_j = 0$, luego $v = 0$, esto es (V, B) es regular. En consecuencia f es regular si, y sólo si, existe una diagonalización de f con todos sus términos diferentes de cero.

Sea f una forma cuadrática sobre F, definimos el determinante de f, que se denota por $d(f)$, de la siguiente manera: 1) Si determinante de $m_f = 0$, entonces $d(f) = 0$. 2) Si determinante de $m_f \neq 0$, entonces $d(f) = \det(m_f)$ mód. $\dot{F}^2$. Es inmediato observar que el determinante así definido es un invariante para la clase de equivalencia de f, o lo que es lo mismo $f \simeq g$ implica $d(f) = d(g)$. Además, si $f \simeq \langle a_1, \ldots, a_n \rangle$, entonces $d(f) = a_1, \ldots, a_n$ mód$(\dot{F}^2)$, lo que significa que f es regular si, y sólo si, $d(f) \neq 0$. Por ejemplo, la forma unidimensional $\langle d \rangle$ es regular si, y sólo si, $d \in \dot{F}$.

Si (V, B) es un espacio cuadrático regular, se sabe por lo anterior que esto equivale a que la matriz de la forma bilineal B es no singular.

Estos conceptos se complementan con el siguiente resultado:

Proposición 1.1.3. Supongamos que (V, B) es regular y $h: V \to V^*$ es la aplicación definida por $h(v) = h_v \in \mathrm{Hom}(V, F)$ tal que $h_v(u) = B(u, v)$. Entonces h es un F-isomorfismo lineal entre V y su dual $V^* = \mathrm{Hom}(V, F)$.

Demostración. Sean $v_1, \ldots, v_n$ una F-base de V y $(B(v_i, v_j))$ la matriz de B asociada a esta base. Demostraremos que la matriz de h relativa a la base $v_1, \ldots v_n$ y su base dual, $w_1, \ldots, w_n$ (definida como $w_i(v_j) = 1$, si $i = j$, $w_i(v_j) = 0$, si $i \neq j$) es coincidente con la matriz de B que, por hipótesis, es no singular. Como dim V = dim V^* resultará que h es un isomorfismo de V sobre V^*. Sea $h(v_j) = \sum_{i=1}^{n} c_{ij} w_i$, luego $h_{v_j}(v_k) = B(v_k, v_j) = \sum_{i=1}^{n} c_{ij} w_i(v_k) = c_{kj}$.

Aplicación. Un Método Práctico de Diagonalización (Algoritmo de Lagrange).

Sea $f = \sum_{i,j}^{n} a_{ij} X_i X_j$, $a_{ij} \in F$ una forma cuadrática sobre F. Se trata de encontrar una forma cuadrática $g = \sum_{i=1}^{n} b_i Y_i^2$ que sea equivalente a f. Así, g debe obtenerse de f por una transformación lineal inversible de las indeterminadas $X_1, \ldots, X_n$ en las indeterminadas $Y_1, \ldots, Y_n$. En la práctica tal "cambio de coordenadas" se obtiene por sucesivos cambios de coordenadas, es decir si $P_1, \ldots, P_r$ son las matrices correspondientes a cada uno de estos cambios parciales, la matriz del cambio de f en g será la matriz $P_r \cdot P_{r-1} \ldots P_1 = P$.

Consideremos dos casos:

a) $a_{11} = a_{22} = \ldots = a_{nn} = 0$.

b) Existe algún $a_{ii} \neq 0$.

Si se trata del caso a), cabe suponer, por ejemplo, que $a_{12} \neq 0$, y escribir:

$$f(X) = 2X_1(a_{12}X_2 + \ldots + a_{1n}X_n) + g(X_2, \ldots, X_n),$$

donde $g(X_2, \ldots, X_n)$ es independiente de X_1. Definimos $Y_2 = a_{12}X_2 + \ldots + a_{1n}X_n - X_1$, $Y_i = X_i$, $i \neq 2$. Se tiene: $f_1(Y) = 2Y_1(Y_1 + Y_2) + g(Y) = 2Y_1^2 + 2Y_1Y_2 + g(Y)$.

Obsérvese que el cambio de coordenadas definido transforma f en una nueva forma equivalente a f (pues es fácil calcular que el determinante de la matriz que define el cambio es $\pm a_{12} \neq 0$) y en consecuencia el caso a) se reduce al caso b).

Veamos el caso b). Podemos suponer que $a_{11} \neq 0$ y escribir

$$f(X) = a_{11}X_1^2 + 2a_{12}X_1X_2 + \ldots + 2a_{1n}X_1X_n + \sum_{i,j>1} a_{ij}X_iX_j.$$

de donde:

$$f(X) = a_{11}^{-1}(a_{11}X_1 + a_{12}X_2 + \ldots + a_{1n}X_n)^2 - a_{11}^{-1}(a_{12}^2X_2^2 + 2a_{12}a_{13}X_2X_3 +$$

$$+ \ldots + a_{1n}^2X_n + \sum_{i,j>1} a_{ij}X_iX_j$$

$$= a_{11}^{-1}(a_{11}X_1 + a_{12}X_2 + \ldots + a_{1n}X_n)^2 + g(X_2, \ldots, X_n)$$

en que $g(X_2, \ldots, X_n)$ es una forma cuadrática en $X_2, \ldots, X_n$.

Definimos

$$Y_1 = a_{11}X_1 + \ldots + a_{1n}X_n$$

$$Y_i = X_i,\ i = 2, \ldots, n,$$

por consiguiente $f_1(Y) = a_{11}^{-1}Y_1^2 + g(Y_2, \ldots, Y_n)$ es una forma cuadrática equivalente a f (el determinante de la matriz del cambio es $a_{11} \neq 0$). Se puede ahora aplicar el mismo método a $g(Y_2, \ldots, Y_n)$.

Veamos dos ejemplos:

i) Diagonalizar la forma $f(X) = X_1^2 - X_2^2 + 3X_3^2 + X_1X_3$ sobre $F = R$.

Aplicamos directamente el caso b).

$$f(X) = X_1^2 + X_1X_3 - X_2^2 + 3X_3^2 = X_1^2 + 2(\tfrac{1}{2}X_1X_3) - X_2^2 + 3X_3^2$$

$$= (X_1 + \tfrac{1}{2}X_3)^2 - X_2^2 + \tfrac{11}{4}X_3^2.$$

Definiendo

$$Y_1 = X_1 + \tfrac{1}{2}X_3$$

$$Y_2 = X_2$$

$$Y_3 = \frac{\sqrt{11}}{2}X_3$$

Obtenemos $g(Y) = Y_1^2 - Y_2^2 + Y_3^2$. Si P es la matriz del cambio de coordenadas tenemos:

$$P = \begin{bmatrix} 1 & 0 & \frac{1}{2} \\ 0 & 1 & 0 \\ 0 & 1 & \frac{\sqrt{11}}{2} \end{bmatrix}$$

$g(Y) = g(P \cdot X) = X^t \cdot (P^t \cdot m_g \cdot P) \cdot X$, y como

$$P^t \cdot m_g \cdot P = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \frac{1}{2} & 0 & \frac{\sqrt{11}}{2} \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & \frac{1}{2} \\ 0 & 1 & 0 \\ 0 & 0 & \frac{\sqrt{11}}{2} \end{bmatrix} =$$

$$\begin{bmatrix} 1 & 0 & \frac{1}{2} \\ 0 & -1 & 0 \\ \frac{1}{2} & 0 & 3 \end{bmatrix} = m_f$$

se observa la relación $f(X) = g(P \cdot X)$.

ii) Diagonalizar sobre F, tal que caract$(F) \neq 2$, la forma $f(X) = X_1X_2$.

Aplicamos el caso a): $f(X) = X_1(X_2)$ y definimos $Z_1 = X_1$, $Z_2 = X_2 - X_1$, con lo que obtenemos $f_1(Z) = Z_1(Z_1 + Z_2) = Z_1^2 + Z_1Z_2$. Se observa que el proceso ha quedado reducido al caso b) mediante $P_1 = \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}$, $f(Z) =$

$= (Z_1^2 + Z_1Z_2 + \frac{1}{4}Z_2^2) - \frac{1}{4}Z_2^2 = (Z_1 + \frac{1}{2}Z_2)^2 - \frac{1}{4}Z_2^2$.

Definimos $\quad Y_1 = Z_1 + \frac{1}{2}Z_2 \qquad P_2 = \begin{bmatrix} 1 & \frac{1}{2} \\ 0 & \frac{1}{2} \end{bmatrix}$

$\qquad\quad Y_2 = \frac{1}{2}Z_2$

Por este cambio de coordenadas se tiene $f_2(Y) = Y_1^2 - Y_2^2 = g(Y)$.

14 Si $P = P_2 \cdot P_1$ denota la matriz de cambio de f en g obsérvese que:

$$P^t \cdot m_g \cdot P = \begin{bmatrix} \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \cdot \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{bmatrix} = \begin{bmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 0 \end{bmatrix} = m_f.$$

1.2. SUMA ORTOGONAL DE ESPACIOS CUADRÁTICOS

Consideremos (V_1, B_1) y (V_2, B_2) F-espacios cuadráticos de dimensiones n y m, respectivamente. Definimos el espacio cuadrático suma ortogonal de los espacios dados y denotamos por $V_1 \perp V_2$ el F-espacio cuadrático (V, B), donde $V = V_1 \oplus V_2$ y $B: V \times V \to F$ se define como $B((x_1, x_2), (y_1, y_2)) = B_1(x_1, y_1) + B_2(x_2, y_2)$. Un cálculo directo muestra que B es bilineal y sus restricciones a los subespacios V_i, $i = 1, 2$ coinciden con B_i. A modo de ejemplo cabe notar que la descomposición ortogonal $f \simeq \langle a_1, \ldots, a_n \rangle$ es una suma ortogonal $\langle a_1 \rangle \perp \ldots \perp \langle a_n \rangle$. Si f y g son F-formas, entonces $f \perp g$ denota la F-forma correspondiente a la clase de isometría del espacio suma ortogonal de (F^n, B_f) y (F^m, B_g). Es así que se pueden sumar clases de isometría de formas cuadráticas, pues si $f \simeq f'$ y $g \simeq g'$, entonces $f \perp g \simeq f' \perp g'$.

Proposición 1.2.1. Sea (V, B) un F-espacio cuadrático y U un subespacio regular de V, entonces $V = U \perp U^\perp$.

Demostración. Como $U \cap U^\perp = 0 = r(U)$, queda por demostrar que $U + U^\perp$ es igual a V. Sea $v_1, \ldots, v_k$ una base ortogonal de U, entonces por la regularidad de U, $B(v_i, v_i) \neq 0$. Así, para cualquier $z \in V$, si se

escribe $y = z - \sum_{i=1}^{k} \frac{B(z, v_i)}{B(v_i, v_i)} v_i$, se tiene que $B(y, v_j) = 0$, $j = 1, \ldots, k$ y entonces $B(y, U) = 0$, con lo que finaliza la demostración.

Corolario 1.2.2. Sea (V, B) un espacio cuadrático y U un subespacio regular, luego si $V = U \perp W$, entonces $W = U^{\perp}$.

Demostración. De la anterior proposición se tiene que $V = U \perp U^{\perp}$, luego $\dim(V) = \dim(U) + \dim(U^{\perp})$ y, como $V = U \perp W$ implica que $W \subseteq U^{\perp}$, entonces $W = U^{\perp}$.

Ejemplo 6

a) Dos formas binarias $\langle a, b\rangle$ y $\langle c, d\rangle$ son isométricas si, y sólo si, tienen el mismo determinante y representan un elemento en común. En este caso, si ambas representan el elemento e, cabe escribir $\langle a, b\rangle \simeq \langle e, x\rangle$ y $\langle c, d\rangle \simeq \langle e, y\rangle$, donde $ex = ey$ mód $(\dot{F}^2)$, luego $\langle x\rangle \simeq \langle y\rangle$, de donde se tiene $\langle e, x\rangle \simeq \langle e, y\rangle$, y entonces $\langle a, b\rangle \simeq \langle c, d\rangle$.

b) $\langle 1, -1\rangle \simeq \langle a, -a\rangle \ \forall\, a \in \dot{F}$.

Es inmediato ver que tienen el mismo determinante y puesto que:

$$a = \frac{(a+1)^2}{4} - \frac{(a-1)^2}{4} \quad \forall\, a \in \dot{F}$$

ambas formas representan un elemento en común.

La forma cuadrática $\langle 1, -1\rangle$ es claramente isótropa y representa todo $\dot{F}$; el espacio cuadrático correspondiente recibe el nombre de *plano hiperbólico* sobre F y se denota por H (o por H_F, cuando es necesario precisar el cuerpo en referencia). Se llama *espacio hiperbólico* a todo espacio cuadrático que sea suma ortogonal de planos hiperbólicos. Adviértase asimismo que H es espacio regular de dimensión 2.

Proposición 1.2.3. Sea f una F-forma cuadrática regular, f es isótropa si, y sólo si, contiene un plano hiperbólico.

Demostración. Consideremos una diagonalización de f, $f \simeq \langle a_1, \ldots, a_n\rangle$ Si f contiene un plano hiperbólico (es decir, si $f \simeq H \perp f_1$ para alguna F-forma f_1), es claro que f es isótropa. Recíprocamente, si $x = (x_1, \ldots, x_n)$ es vector isótropo para f, entonces $a_1 x_1^2 + \ldots + a_n x_n^2 = 0$. Supongamos que $x_j \neq 0$, dividiendo por x_j^2 resulta que $\langle a_1, \ldots, a_{j-1}, a_{j+1}, \ldots, a_n\rangle$ representa $-a_j$ (obsérvese que todos los a_i son diferentes de cero por la regularidad de f), esto es, existen $b_2, \ldots, b_{j-1}, b_{j+1}, \ldots, b_n$ en $\dot{F}$ tales que:

$$\langle a_1, \ldots, a_{j-1}, a_{j+1}, \ldots, a_n\rangle \simeq \langle -a_j, b_2, \ldots, b_n\rangle,$$

sumando $\langle a_j\rangle$ obtenemos $f \simeq \langle a_j, -a_j\rangle \perp f_1$.

Una forma cuadrática sobre F que representa todo $\dot{F}$ se llama *universal*. De la proposición anterior se sigue que toda forma isótropa

es universal; lo recíproco no es verdadero, por ejemplo la forma $\langle 1, 2, 5, -10\rangle$ sobre el cuerpo racional Q es universal y anisótropa (para la respectiva justificación véase el Apéndice al capítulo 1, A. 6. ejemplo 7). Igualmente, si F es un cuerpo que satisface las dos propiedades siguientes:

i) toda forma cuadrática de dimensión ≥ 5 es isótropa,

ii) existen formas anisótropas de dimensión 4,

entonces toda forma anisótropa de dimensión 4 es universal. La demostración es inmediata y se deja como ejercicio para el lector. Puede verse en el mencionado Apéndice (A. 5. Aplic. 4) que los cuerpos p-ádicos satisfacen las propiedades i) e ii).

1.3. TEOREMA DE CANCELACIÓN DE WITT

Uno de los resultados más importantes de la teoría de formas cuadráticas sobre cuerpos es el llamado teorema de Cancelación de Witt. Hay diversas versiones de este teorema y su demostración se puede realizar prescindiendo de la hipótesis de regularidad que aquí mantendremos (nuestro interés es el estudio de las clases de equivalencia de formas regulares). En adelante, sólo consideraremos clases de isometría de formas regulares, salvo aclaración expresa de lo contrario. Veamos antes un lema.

Lema. Sea (V,B) un F-espacio cuadrático y sea $y \in V$ tal que $B(y,y) \neq 0$. Definimos

$$t_y(x) = x - \frac{2B(x,y)}{q(y)}\, y;\ \forall\, x \in V.$$

Observamos lo siguiente:

a) t_y es un endomorfismo del F-espacio vectorial V.

b) $t_y(x) = x;\ \forall\, x \in (F\cdot y)^{\perp}$.

c) $B(t_y(x),\ t_y(x')) = B(x,x')$, $\forall\ x,\ x' \in V$ (se obtiene por cálculo directo de la definición de t_y). Luego si $t_y(x) = 0$, entonces $x \in r(V) = 0$ por la regularidad de (V,B). Por lo tanto:

d) t_y es un automorfismo de V.

e) $t_y(y) = -y$.

En consecuencia, t_y es una isometría del espacio (V,B) que deja invariante el subespacio $(F\cdot y)^{\perp}$, y aplica y en $-y$. Por este motivo, t_y se denomina reflexión.

Lema 1, 3.1 Sean (V,B) un F-espacio cuadrático y $x, y \in V$ tales que $q(x) = q(y) \neq 0$. Existe una isometría t de V en sí mismo tal que $t(x) = y$.

Demostración. Puesto que $q(x+y)+q(x-y)=4q(x)\neq 0$, entonces $q(x+y)$ y $q(x-y)$ no pueden ser ambos cero; se supone entonces que $q(x-y)\neq 0$ (en caso contrario basta sustituir y por $-y$, y observar que la aplicación definida por $x \to -x$ es una isometría). Considérese la reflexión t_{x-y}. Entonces t_{x-y} es una isometría de V en sí mismo y, como:

$$q(x-y) = B(x,x)+B(y,y)-2B(x,y) = 2(B(x,x)-B(x,y)) =$$

$$= 2B(x,x-y), \text{ se obtiene:}$$

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

Teorema 1.3.2. (Teorema de Cancelación de Witt). Sean f_1, f_2 y f_3 F-formas tales que $f_1 \perp f_2 \simeq f_1 \perp f_3$, entonces $f_2 \simeq f_3$.

Demostración. Supongamos una diagonalización de f_1; $f_1 \simeq \langle a_1, \ldots, a_n \rangle$. Procediendo en forma inductiva sobre la dimensión de f_1, se observa a las claras que es posible reducirse al caso: $\langle a_1 \rangle \perp f_2 \simeq \langle a_1 \rangle \perp f_3$ implica $f_2 \simeq f_3$. La isometría de la hipótesis permite identificar los espacios cuadráticos de $\langle a_1 \rangle \perp f_2$ y de $\langle a_1 \rangle \perp f_3$; sea (V,B) el espacio obtenido con la mencionada identificación. Entonces existen en V elementos x e y tales que $q(x)=q(y)=a_1$, tales que f_2 se identifica con $(F\cdot x)^{\perp}$ y f_3 con $(F\cdot y)^{\perp}$ por el Corolario 1.2.2. Por aplicación del lema obtenemos una isometría t de V en sí mismo que aplica x en y, luego t aplicará $(F\cdot x)^{\perp}$ en $(F\cdot y)^{\perp}$, esto es la restricción de t a $(F\cdot x)^{\perp}$ proporciona una isometría de f_2 con f_3. 17

Corolario 1.3.3. (Teorema de Descomposición de Witt). Toda F-forma cuadrática se descompone en suma ortogonal

$$f \simeq f_a \perp \underbrace{H \perp \ldots \perp H}_{r} = f_a \perp rH$$

donde f_a es una subforma anisótropa de f, r entero no negativo y H denota el plano hiperbólico. f_a está unívocamente determinada (salvo isometría) y se denomina *la parte anisótropa de* f, o la *forma núcleo* de f, y r se llama *el índice de Witt de* f.

Demostración. Si f es anisótropa, tomamos $f=f_a$ y $r=0$. Sea f isótropa, por la Proposición 1.2.3. f puede escribirse $f \simeq H \perp f_1$; si f_1 es anisótropa, el teorema está demostrado. En caso contrario, aplicamos nuevamente el procedimiento anterior y así sucesivamente, y después de un número finito de pasos llegamos a la descomposición buscada. Que f_a está únicamente determinada resulta inmediato de la cancelación establecida en el teorema anterior.

1.4. ANILLO DE WITT

Consideremos f y g F-formas de grados m y n, respectivamente, y supongamos $f=\langle a_1, \ldots, a_m \rangle$ $g=\langle b_1, \ldots, b_n \rangle$. Definimos el *producto tensorial* de las formas diagonales f y g como la forma diagonal siguiente:

$$f \otimes g = \langle a_1 b_1, \ldots, a_1 b_n, a_2 b_1, \ldots, a_m b_n \rangle.$$

Es inmediato observar que el producto tensorial definido es conmutativo, asociativo, distributivo respecto de la suma ortogonal de formas diagonales y posee elemento identidad $\langle 1 \rangle$ F-forma unidimensional. Se verifica también que $f \otimes H \simeq \dim(f) H$. Este producto se extiende de manera natural a las clases de isometría de F-formas, como: $(f) \otimes (g) = (f \otimes g)$. Mediante un cálculo directo se comprueba que la definición es consistente, en el sentido que si $f' \simeq f$ y $g' \simeq g$, formas diagonales, entonces $f' \otimes g' \simeq f \otimes g$.

En forma más general se puede definir el producto tensorial de espacios cuadráticos de la siguiente forma:

Sean (V_1, B_1) y (V_2, B_2) F-espacios cuadráticos de dimensiones m y n respectivamente, si $V = V_1 \underset{F}{\otimes} V_2$ y $B: V \times V \to F$ es la única forma bilineal simétrica que satisface $B(x_1 \otimes y_1, x_2 \otimes y_2) = B_1(x_1, y_1) \cdot B(x_2, y_2)$, entonces el espacio cuadrático (V, B) se llama el *producto tensorial* de los espacios dados.

En particular si $V_1 = \langle a_1, \ldots, a_m \rangle$ y $V_2 = \langle b_1, \ldots, b_n \rangle$ el producto tensorial de V_1 y V_2 coincide con el anteriormente definido.

Nuestro objetivo inmediato es la construcción de una estructura de anillo sobre el conjunto de clases de isometría de F-formas. Para ello se cuenta ya con dos operaciones bien definidas: la suma ortogonal de clases y el producto tensorial de clases. Como señalamos anteriormente nuestro interés es estudiar las clases de isometría, por lo tanto, para simplificar las notaciones, procederemos a identificar las clases con sus representantes. Luego, $=$ significa $\simeq$.

Definición 7. Sean f y g F-formas; diremos que son Witt-equivalentes y escribimos $f \sim g$, si f y g tienen la misma parte anisótropa.

Por ejemplo, la forma 0 tiene la misma parte anisótropa que H y por consiguiente $0 \sim H$. Es inmediato demostrar que la Witt-equivalencia es una relación de equivalencia sobre el conjunto de clases de isometría de F-formas; al conjunto cociente lo denotaremos por WF. Las operaciones de suma ortogonal y producto tensorial tienen natural extensión al conjunto de clases de Witt-equivalencia y $(WF, \perp, \otimes)$ tiene una estructura de anillo conmutativo cuya unidad es $\langle 1 \rangle$. Obsérvese que $\langle a \rangle \perp \langle -a \rangle = \langle a, -a \rangle = 0$ en WF, por lo tanto $-\langle a \rangle = \langle -a \rangle$, y entonces si $f = \langle a_1, \ldots, a_n \rangle$ en WF resulta $-f = \langle -a_1, \ldots, -a_n \rangle$. Además dos F-formas f y g son isométricas si, y sólo si, tienen la misma dimensión y representan el mismo elemento en WF. WF se llama el anillo de Witt de formas cuadráticas sobre el cuerpo F. Cuando trabajemos en el anillo de Witt se usará la notación " + " y " · " para las operaciones de WF.

Por construcción WF se encuentra en correspondencia biyectiva con el conjunto de formas cuadráticas regulares y anisótropas sobre F, y por este motivo a WF se le llama también el anillo de formas anisótropas sobre F. Adviértase, sin embargo, que la suma ortogonal de formas anisótropas no es una forma anisótropa (por ejemplo, $\langle a \rangle \perp \langle -a \rangle \simeq \simeq \langle a, -a \rangle \simeq H$) y por lo tanto ésta es sólo una forma de referirse a WF.

Ejemplo 7. Sea F un cuerpo cuadráticamente cerrado, es decir, en F todo elemento es un cuadrado. Luego si $a \in \dot{F}$, entonces $\langle a \rangle \simeq \langle 1 \rangle$, y por consiguiente $f \simeq g$ si, y sólo si, $\dim(f) = \dim(g)$. Si $\dim(f) =$ par, entonces f es hiperbólica, y si $\dim(f) =$ impar, $f = \langle 1 \rangle$, luego WF es isomorfo a Z_2.

Ejemplo 8. Sea F cuerpo finito con $q = p^n$ elementos; $p \neq 2$ es la característica de F.

a) $\dot{F}/\dot{F}^2$ tiene únicamente dos elementos:

Consideremos la siguiente sucesión de grupos:

$$1 \to \dot{F}^2 \to \dot{F} \xrightarrow{h} \{\pm 1\} \to 1,$$

donde $h(x) = x^{\frac{q-1}{2}}$. $x \in Nu(h)$ si, y sólo si, $x^{\frac{q-1}{2}} = 1$. En la clausura algebraica de F se elige un y tal que $y^2 = x$, entonces $y^{q-1} = 1$. Luego $y \in F$ (puesto que F es el cuerpo de descomposición del polinomio $X^q - X$ sobre su cuerpo primo), entonces x es un cuadrado en F y tenemos $\mathrm{Nu}(h) = \dot{F}^2$.

b) En F todo elemento es suma de dos cuadrados:

Denotemos por 1 y s los representantes de las dos clases cuadradas de F, luego $\dot{F} = \dot{F}^2 \cup s\dot{F}^2$, y en consecuencia basta demostrar que s es la suma de dos cuadrados en F. Si $-1 \in \dot{F}^2$, es $\langle 1, 1 \rangle \simeq \langle 1, -1 \rangle$, de donde $\langle 1, 1 \rangle$ es universal y representa en particular a s. Si $-1 \notin \dot{F}^2$, entonces $1 + \dot{F}^2$ no contiene al cero, como cardinal $(\dot{F}^2) =$ cardinal $(1 + \dot{F}^2)$ se tiene que $1 + \dot{F}^2$ no está contenido en $\dot{F}^2$, y en consecuencia existe un $u \in \dot{F}$ tal que $1 + u^2 \notin \dot{F}^2$, luego $1 + u^2$ está en $s\dot{F}^2$, de donde resulta s suma de cuadrados. 19

c) $-1 \in \dot{F}^2$ si, y sólo si, $q \equiv 1$ mód (4)
$-1 \in s\dot{F}^2$ si, y sólo si, $q \equiv 3$ mód (4).

d) Sobre un cuerpo finito toda forma ternaria es isótropa.

Las formas binarias sobre F son $\langle 1, 1 \rangle$, $\langle s, s \rangle$, $\langle 1, s \rangle$. $\langle 1, 1 \rangle$ y $\langle s, s \rangle$, y son universales por b). Como $\dot{F} = \dot{F}^2 \cup s\dot{F}^2$, es claro también que $\langle 1, s \rangle$ es universal. Sea $\langle a, b, c \rangle$ una F-forma ternaria; $\langle b, c \rangle$ representa $-a$, luego $\langle b, c \rangle \simeq \langle -a, x \rangle$, entonces $\langle a, b, c \rangle \simeq \langle -a, a, x \rangle$ y por lo tanto $\langle a, b, c \rangle$ es isótropa.

e) Para F cuerpo finito de q elementos es:

WF isomorfo a $Z_2\,[\dot{F}/\dot{F}^2]$, si $q \equiv 1$ mód (4).
WF isomorfo a Z_4, si $q \equiv 3$ mód (4).

Demostración. Si $q \equiv 1(4)$, entonces las formas anisótropas sobre F son 0, $\langle 1 \rangle$, $\langle s \rangle$, $\langle 1, s \rangle$, por c) y d). Luego identificando el grupo de unidades de WF, esto es $\langle 1 \rangle$, $\langle s \rangle$ con $\dot{F}/\dot{F}^2$, concluimos lo afirmado.

Si $q = 3$ mód (4), entonces las formas anisótropas sobre F son 0, $\langle 1 \rangle$, $\langle -1 \rangle$ y $\langle 1, 1 \rangle$. Pero $\langle -1 \rangle$ es la parte anisótropa de $\langle 1, 1, 1 \rangle$, y en

consecuencia las clases en WF pueden representarse 0, $\langle 1\rangle$, $\langle 1, 1\rangle$ y $\langle 1, 1, 1\rangle$, de donde resulta que WF es isomorfo a Z_4.

Ejemplo 9. Sea F un cuerpo con sólo dos clases módulo cuadrados y con la propiedad de que la forma $\langle 1, \ldots, 1\rangle$ (suma ortogonal de n veces la forma $\langle 1\rangle$), que se denota por $n\langle 1\rangle$, es anisótropa para todo entero positivo n. Un ejemplo es el cuerpo R de los números reales. Un cuerpo F con las propiedades citadas se denomina un *cuerpo euclidiano*.

Como $\dot{F}/\dot{F}^2 = \{\pm 1\}$, tenemos que toda forma cuadrática f sobre F tiene una diagonalización $f \simeq \langle a_1, \ldots, a_n\rangle$, donde $a_1 = a_2 = \ldots = a_r = 1$ y $a_{r+1} = \ldots = a_n = -1$.

Si $0 < r < n$, entonces f es isótropa.

Si $r = 0$ ó $r = n$, f es anisótropa.

Escribiendo $s = n - r$, se define para f:

$\mathrm{Sig}(f) = r - s =$ (número de términos iguales a 1) - (número de términos iguales a -1).

$\mathrm{Sig}(f)$ es un entero llamado la *signatura de* f. Probemos que $\mathrm{Sig}(f)$ es independiente de la diagonalización empleada para definirlo. Si consideramos dos diagonalizaciones de f sobre F escribimos:

$$f \simeq r\langle 1\rangle \perp s\langle -1\rangle \simeq r_1\langle 1\rangle \perp s_1\langle -1\rangle.$$

Demostraremos que $r = r_1$ y $s = s_1$. Si $s \geq s_1$, por el teorema de Cancelación de Witt $r\langle 1\rangle \perp (s - s_1)\langle -1\rangle \simeq r_1\langle 1\rangle$. Se observa que si $s - s_1 > 0$, el miembro izquierdo es forma isótropa, y, por lo tanto, $r_1\langle 1\rangle$ es isótropa, lo que no es posible en F (recuérdese que la forma 0 es anisótropa), entonces $s = s_1$, y por el teorema de cancelación se obtiene $r\langle 1\rangle \simeq r_1\langle 1\rangle$. A partir del mismo argumento se concluye que $r = r_1$.

El resultado anterior se conoce como la *ley de inercia*, la cual puede enunciarse de la forma siguiente:

Ley de Inercia de Sylvester. "Sobre un cuerpo euclidiano F, dos formas cuadráticas f y g son isométricas si, y sólo si, tienen la misma dimensión y la misma signatura".

Podemos definir $\mathrm{Sig}: WF \to Z$ como la aplicación "signatura" que a cada $q \in WF$ le asocia el entero $\mathrm{Sig}(q)$. Basta observar que la signatura de H es 0 para ver que la definición es consistente. Es un cálculo fácil comprobar que Sig es un homomorfismo de anillos y que, si $\mathrm{Sig}(q) = 0$, q es hiperbólica y en consecuencia Sig es un isomorfismo del anillo WF (F euclidiano) sobre el anillo de los enteros Z.

1.5 FORMAS DE PFISTER

El estudio de la teoría algebraica de formas cuadráticas sobre cuerpos, y más generalmente sobre anillos, se ha desarrollado mucho en los últimos años debido fundamentalmente a los trabajos del matemáti-

co alemán A. Pfister. Pfister, tomando como base las ideas de Witt (expuestas en una célebre memoria el año 1937), hizo importantes contribuciones a la teoría de formas cuadráticas sobre cuerpos utilizando las formas multiplicativas (introducidas por él, hoy conocidas como formas de Pfister) en el estudio del anillo de Witt de formas anisótropas sobre un cuerpo.

En esta sección estudiaremos algunos resultados básicos referentes a las formas de Pfister y, en los capítulos siguientes, podremos formarnos una idea más precisa de su importancia en la teoría de formas cuadráticas.

Con IF se denota el ideal de WF formado por todos los elementos de WF de dimensión par que se denomina el ideal fundamental de WF. De la definición se tiene de inmediato que WF/IF es isomorfo a Z_2, y por lo tanto IF es un ideal maximal de WF. Toda forma $\langle a, b\rangle$ en WF puede escribirse $\langle a, b\rangle = \langle 1, a\rangle + \langle -1, b\rangle = \langle 1, a\rangle - \langle 1, -b\rangle$, y en consecuencia, IF es generado "aditivamente" por formas binarias del tipo $\langle 1, a\rangle$, $a \in \dot{F}$. Conviene resumir lo demostrado en la siguiente proposición:

Proposición 1.5.1. *IF es un ideal maximal de WF generado aditivamente por formas binarias del tipo $\langle 1, a\rangle$, $a \in \dot{F}$. Además, IF es el único ideal primo de WF que contiene a $\langle 1, 1\rangle$.*

Demostración. Sea P un ideal primo de WF tal que $\langle 1, 1\rangle \in P$, entonces $2\langle 1\rangle = 0$ en WF/P, es decir WF/P es un dominio de integridad de característica 2. Como $(\langle a\rangle + \langle 1\rangle)(\langle a\rangle - \langle 1\rangle) = 0$ en WF, se tiene que $\langle a\rangle = \langle 1\rangle$ o $\langle a\rangle = -\langle 1\rangle$, luego si $q = \langle a_1, \ldots, a_n\rangle \in IF$, en WF/P es $q = 0$, entonces $IF \subset P$ y, por maximalidad, $IF = P$.

Más generalmente, si P es un ideal primo de WF, se dice que P *tiene característica* p si el dominio de integridad WF/P tiene característica p. Luego p es un número primo o cero. Por ejemplo, IF es ideal de característica 2 y, aún más, es el único ideal primo de característica 2 en WF.

Proposición 1.5.2. *Si P es un ideal primo de WF y carac$(P) = p$, entonces WF/P es isomorfo a Z_p.*

Demostración. Como WF es generado aditivamente por las formas $\langle a\rangle$ $(a \in F)$, y en WF/P es $\langle a\rangle = \langle 1\rangle$ o $\langle a\rangle = -\langle 1\rangle$, se tiene que la imagen de WF en WF/P es generada aditivamente por $\langle 1\rangle$, y como la característica de WF/P es p, se concluye que WF/P es isomorfo a Z_p.

Como IF es generado aditivamente por las formas $\langle 1, a\rangle$, $a \in \dot{F}$, entonces para $n \geq 1$ será $(IF)^n = I^nF$ generado aditivamente por las formas $\langle 1, a_1\rangle \otimes \langle 1, a_2\rangle \otimes \ldots \otimes \langle 1, a_n\rangle$; estas formas se denotan por $\ll a_1, \ldots, a_n\gg$ y se denominan n-formas de Pfister sobre F. Es inmediato observar:

a) Toda n-forma de Pfister es de dimensión 2^n.

b) Toda n-forma de Pfister representa 1.

c) $\ll 1, a_2, \ldots, a_n\gg \simeq 2\ll a_2, \ldots a_n\gg$.

d) $\ll -1, a_2, \ldots, a_n\gg \simeq 2^{n-1}H$.

Se conviene en considerar como 0-forma de Pfister la forma unidimensional $\langle 1\rangle$. Vamos a presentar aquí dos propiedades capitales de las formas de Pfister, a saber:

i) Toda forma de Pfister isótropa es hiperbólica.

ii) Los elementos no nulos representados por una forma de Pfister forman un grupo multiplicativo (véase el teorema 1.5.5).

Lema 1.5.3. Sobre un cuerpo F se tiene:

a) $\ll a_1, a_2\gg \simeq \ll a_1, a_2 b\gg$, si $b \in D_F(\ll a_1\gg)$.

b) $\ll a_1, a_2\gg \simeq \ll c, a_1 a_2\gg$, si $c \in D_F(\langle a_1, a_2\rangle)$.

Demostración

a) Como $b \in D_F(\ll a_1\gg)$, entonces $\langle 1, a_1\rangle$ y $\langle b, a_1 b\rangle$ son isométricas pues tienen el mismo determinante y representan un elemento en común. Luego:

$$\begin{aligned}\ll a_1, a_2\gg &\simeq \langle 1, a_1\rangle \otimes \langle 1, a_2\rangle \simeq \langle 1, a_1\rangle \perp \langle a_2\rangle \otimes \langle 1, a_1\rangle \\ &\simeq \langle 1, a_1\rangle \perp \langle a_2\rangle \otimes \langle b, a_1 b\rangle \simeq \langle 1, a_1, a_2 b, a_1 a_2 b\rangle \\ &\simeq \ll a_1, a_2 b\gg.\end{aligned}$$

b) $\ll a_1, a_2\gg \simeq \langle 1\rangle \perp \langle a_1, a_2\rangle \perp \langle a_1 a_2\rangle$. Como $\langle a_1, a_2\rangle \simeq \langle c, c a_1 a_2\rangle$, entonces:

$$\ll a_1, a_2\gg \simeq \langle 1, c, c a_1 a_2, a_1 a_2\rangle \simeq \ll c, a_1 a_2\gg.$$

Si f es una n-forma de Pfister, podemos escribir $f \simeq \langle 1\rangle \perp f'$; f' se llama la *subforma pura* de f y es determinada en forma única por f, salvo isometrías.

Teorema 1.5.4. (Teorema de la Subforma Pura). Sean $f \simeq \ll a_1, \ldots, a_n\gg$ una n-forma de Pfister y $b \in \dot{F}$, entonces $b \in D_F(f')$ si, y sólo si, $f \simeq \ll b, b_2, \ldots, b_n\gg$ para ciertos $b_i \in \dot{F}$.

Demostración. Si $f \simeq \ll b, b_2, \ldots, b_n\gg$, entonces:

$$\langle 1\rangle \perp f' \simeq f \simeq \langle 1, b\rangle \otimes \langle 1, b_2\rangle \otimes \ldots \otimes \langle 1, b_n\rangle \simeq \langle 1, b, b_2, \ldots\rangle \simeq$$

$$\simeq \langle 1\rangle \perp \langle b, b_2, \ldots\rangle.$$ Cancelando $\langle 1\rangle$, se obtiene que $b \in D_F(f')$.

Realizaremos la demostración del recíproco por inducción sobre n. Si $n = 1$, entonces $f \simeq \ll a_1\gg$ y $f' \simeq \langle a_1\rangle$, luego $b \in D_F(\langle a_1\rangle)$ implica que $\langle a_1\rangle \simeq \langle b\rangle$ y entonces $f \simeq \ll b\gg$. Definimos $g \simeq \ll a_1, \ldots, a_{n-1}\gg$; tenemos que: $f \simeq g \otimes \langle 1, a_n\rangle \simeq g \perp \langle a_n\rangle \otimes g$, luego $f' \simeq g' \perp \langle a_n\rangle \otimes g$. Como $b \in D_F(f')$, entonces $b = u' + a_n v$, donde $u' \in D_F(g') \cup \{0\}$ y $v \in D_F(g) \cup \{0\}$. Asimismo, como $v \in D_F(g) \cup \{0\}$, podemos escribir $v = t^2 + v'$, donde $v' \in D_F(g') \cup \{0\}$. Por la hipótesis inductiva:

$$g \simeq \ll u', c_2, \ldots, c_{n-1}\gg, \text{ si } u' \neq 0, \text{ y}$$

$$g \simeq \ll v', d_2, \ldots d_{n-1} \gg, \text{ si } v' \neq 0.$$

Si fuese $v = 0$, entonces $u' = b \in \dot{F}$ y $f \simeq g \otimes \ll a_n \gg \simeq \ll b, c_2, \ldots, c_{n-1}, a_n \gg$, con lo que el teorema estaría demostrado. Supondremos, por lo tanto, que $v \neq 0$ y vamos a probar que:

$$f \simeq \ll a_1, \ldots, a_{n-1}, v a_n \gg. \qquad (')$$

Podemos suponer que $v' \neq 0$, puesto que en caso contrario $v = t^2$ y (') es obvio. Luego:

$$f \simeq g \otimes \ll a_n \gg \simeq \ll v', d_2, \ldots, d_{n-1}, a_n \gg$$

$$\simeq \ll d_2, \ldots, d_{n-1} \gg \otimes \ll v', a_n \gg$$

$$\simeq \ll d_2, \ldots, d_{n-1} \gg \otimes \ll v', a_n v \gg \text{ por el lema 1.5.3-a}$$

$$\simeq \ll v', d_2, \ldots, d_{n-1}, a_n v \gg$$

$$\simeq \ll a_1, \ldots, a_{n-1}, a_n v \gg.$$

Ahora, si fuese $u' = 0$, entonces $b = a_n v$, con lo que (') establecería la demostración del teorema. Supongamos finalmente que $u' \neq 0$, entonces:

$$f \simeq \ll u', c_2, \ldots, c_{n-1}, a_n v \gg \text{ por (')}$$

$$\simeq \ll u', a_n v \gg \otimes \ll c_2, \ldots, c_{n-1} \gg$$

$$\simeq \ll u' + a_n v, u' a_n v \gg \otimes \ll c_2, \ldots, c_{n-1} \gg \text{ por el lema 1.5.3-b}$$

$$\simeq \ll b, c_2, \ldots, c_{n-1}, u' a_n v \gg, \text{ con lo que finaliza la demostración.}$$

Denotaremos por $G_F(f) = \{a \in \dot{F} / \langle a \rangle \otimes f \simeq f\}$, donde f es una forma cuadrática sobre F. Es fácil ver que $G_F(f)$ es un subgrupo de $\dot{F}$ y se denomina el grupo de isotropía de f.

Teorema 1.5.5. Sea f una n-forma de Pfister sobre F, entonces:

a) Si f es isótropa, entonces f es hiperbólica

b) $D_F(f)$ es subgrupo del grupo multiplicativo $\dot{F}$.

Demostración

a) Si f es isótropa, entonces contiene un plano hiperbólico y se puede escribir $\langle 1 \rangle \perp f' \simeq f \simeq \langle 1, -1 \rangle \perp g$. Cancelando $-1 \in D_F(f')$, y aplicando el teorema anterior se tiene $f \simeq \ll -1, \ldots \gg \simeq 2^{n-1}H$.

b) Que $G_F(f) \subset D_F(f)$ es inmediato. Supongamos que $a \in D_F(f)$, luego $\langle 1, -a \rangle \otimes f \simeq f \perp \langle -a \rangle \otimes f \simeq f \perp \langle -a, \ldots \rangle$, y en consecuencia $\langle 1, -a \rangle \otimes f$ es isótropa y, por consiguiente, hiperbólica, es decir que en WF será $f = \langle a \rangle \cdot f$, luego, por dimensión, se tiene $f \simeq \langle a \rangle \otimes f$ y $a \in G_F(f)$. Con lo que $D_F(f) = G_F(f)$ y, en particular, $D_F(f)$ es un subgrupo de $\dot{F}$.

Nota: Observamos que $2^n\langle 1\rangle$ es una n-forma de Pfister sobre F y que $a \in D_F(2^n\langle 1\rangle)$, si, y sólo si, a es suma de 2^n cuadrados en $\dot{F}$. Como consecuencia del teorema anterior tenemos que, en particular, las sumas de 2^n cuadrados forman un grupo multiplicativo en $\dot{F}$. Este resultado, aunque inmediata consecuencia del teorema 1.5.5., está vinculado a un problema que fue de gran interés en la teoría de los números, el cual consistía en resolver la siguiente conjetura: Si la suma de m cuadrados multiplicada por la suma de m cuadrados es siempre una suma de m cuadrados (en un cuerpo), entonces m es potencia de dos y recíprocamente. Los casos 1, 2, 4 y 8 son resultados conocidos desde hace muchos años, en particular el caso $m = 4$ se conoce como la identidad de Euler-Lagrange y el $m = 8$ como la identidad de Cayley. Después de grandes esfuerzos realizados por matemáticos del siglo pasado, A. Hurwitz demostró que si el producto de la suma de m cuadrados por la suma de m cuadrados es siempre una suma de m cuadrados, donde además estos últimos dependen linealmente de los primeros, entonces, necesariamente, m es 1, 2, 4 ó 8. En 1965, A. Pfister demostró que, si no pedimos la condición de "linealidad" mencionada, entonces para todo m potencia de dos y sobre cualquier cuerpo las sumas de $2^n = m$ cuadrados forman un grupo.

Ejemplo 10. Álgebras de Cuaterniones como Espacios Cuadráticos. Para finalizar este capítulo nos referiremos, a manera de ejemplo, a las álgebras de cuaterniones como espacios cuadráticos y veremos que corresponden a 2-formas de Pfister.

El papel que estas álgebras desempeñan en el estudio de las formas cuadráticas sobre cuerpos es importantísimo, si bien el exponer algunos de estos resultados excede los límites de esta monografía.

Sean $a, b \in \dot{F}$ y V un F-espacio vectorial de dimensión 4. Se elige una base de V, la que se denota por $\{1, x_1, x_2, x_3\}$ (1 denota un vector de V), y se introduce una multiplicación en V por medio de la siguiente tabla:

$\cdot$	1	x_1	x_2	x_3
1	1	x_1	x_2	x_3
x_1	x_1	a	x_3	ax_2
x_2	x_2	$-x_3$	b	$-bx_1$
x_3	x_3	$-ax_2$	bx_1	$-ab$

donde los escalares se han identificado con su producto con 1, es decir, ponemos a por $a \cdot 1$ (producto escalar). De esta forma V tiene una estructura de F-álgebra, donde: $w = a_0 + a_1x_1 + a_2x_2 + a_3x_3 \in V$ se llama un cuaternión; los cuaterniones se multiplican según la tabla dada más arriba. $(V, +, .)$ es una F-álgebra que se denota por $(\frac{a, b}{F})$ y se llama *álgebra de cuaterniones* sobre F definida por a, b. La base elegida $\{1, x_1, x_2, x_3\}$ se llama la base de definición del álgebra. Si $w = a_0 + a_1x_1 + a_2x_2 + a_3x_3$, con $a_0 = 0$, entonces w se denomina un *cuaternión puro*. El conjunto de cuaterniones puros se denota por $(\frac{a, b}{F})_0$.

Observamos que $x_i x_j = -x_j x_i \in \dot{F} x_k$, para $i, j \in \{1, 2, 3\}$, $i \neq j$, por lo que $(\frac{a, b}{F})$ es un álgebra no conmutativa.

Para $w = a_0 + a_1 x_1 + a_2 x_2 + a_3 x_3$, definimos el cuaternión $\bar{w} = a_0 - (a_1 x_1 + a_2 x_2 + a_3 x_3)$, y resultan las siguientes propiedades de fácil verificación:

a) $\overline{\alpha w} = \alpha \bar{w}$

b) $\overline{w_1 + w_2} = \bar{w}_1 + \bar{w}_2$

c) $\overline{w_1 w_2} = \bar{w}_2 \bar{w}_1$

donde $\alpha \in F$, $w, w_1, w_2 \in (\frac{a, b}{F})$.

Basados en esta "conjugación" definimos:

$$N(w) = w\bar{w} \quad \text{y} \quad T(w) = w + \bar{w}; \quad w \in (\frac{a, b}{F});$$

donde $N(w)$ se llama la "norma de w" y $T(w)$ la "traza de w". Podemos calcular directamente que:

$$N(w) = a_0^2 - a_1^2 a - a_2^2 b + a_3^2 ab$$

$$T(w) = 2a_0.$$

Definimos B: $(\frac{a, b}{F}) \times (\frac{a, b}{F}) \to F$ como: $B(x, y) = \frac{x\bar{y} + y\bar{x}}{2} = \frac{1}{2} T(x\bar{y}) \in F$. B es una F-forma bilineal simétrica sobre $(\frac{a, b}{F})$. En $(\frac{a, b}{F})_o$ es $B(x, y) = 0$ si, y sólo si, x e y anticonmutan; de esto resulta que $(\frac{a, b}{F})$ es un F-espacio cuadrático de dimensión 4 y que la base de definición del álgebra es una base ortogonal. La matriz asociada en esta base será, por lo tanto, la matriz diagonal correspondiente a $\langle 1, -a, -b, ab \rangle$, luego $((\frac{a, b}{F}), B)$ como espacio cuadrático corresponde a $\ll -a, -b \gg$. Se denomina a $\ll -a, -b \gg$ la forma norma del álgebra $(\frac{a, b}{F})$.

Finalmente, a modo de aplicación de lo expuesto demostraremos que sobre el cuerpo racional Q existen infinitas álgebras de cuaterniones no isomorfas. Para ello recordamos dos resultados de la teoría de los números, a saber:

a) Existen infinitos primos en Z de la forma $4n + 3$, $n \in Z^+$.

b) Si un primo de la forma $4n + 3$ divide a la suma de dos cuadrados en Z divide a cada uno de los sumandos.

La demostración no es difícil y la dejamos como ejercicio para el lector.

Aplicación. Si p y q son primos positivos de la forma $4n + 3$ con $p \neq q$, entonces las álgebras de cuaterniones $(\frac{-1, -p}{Q})$ y $(\frac{-1, -q}{Q})$ son no isomorfas.

Demostración. Por comodidad se suprime en la notación la referencia a Q. Si fuesen $(-1, -p)$ y $(-1, -q)$ isomorfas como álgebras, lo serán como espacios cuadráticos (véase el ejercicio 17), y en consecuencia $\ll 1, p\gg \simeq \ll 1, q\gg$, y si se aplica el teorema de cancelación es $\langle p, p\rangle \simeq \simeq \langle q, q\rangle$. Existen entonces x_1 y x_2 racionales tales que $p = (x_1^2 + x_2^2)\cdot q$, y eliminando denominadores resulta $p \cdot h^2 = (m^2 + r^2)\cdot q$ en Z, luego p divide $m^2 + r^2$ y por (b) p divide m^2 y p divide r^2, entonces p divide m y r, luego p^2 divide $p \cdot h^2$, esto es p divide a h. Supongamos que en la factorización en primos de h aparezca p^s, entonces en la factorización de ph^2 aparece p^{2s+1}; por otra parte, en la factorización de $(m^2 + r^2)\cdot q$ aparece p a una potencia par, lo cual no es posible. Luego $(-1, -p)$ y $(-1, -q)$ no son isomorfas.

De lo demostrado y de a) se concluye que existen infinitas álgebras de cuaterniones no isomorfas sobre Q.

EJERCICIOS

1. Demostrar que la suma y producto de clases de isometría de formas cuadráticas es una operación bien definida, así como su extensión al conjunto de clases de Witt-equivalencia.

2. Si (V, B) es un espacio cuadrático regular y U un subespacio de V, demostrar que:

a) $\dim(U) + \dim(U^\perp) = \dim(V)$.

b) $(U^\perp)^\perp = U$.

3. Sea (V, B) un espacio cuadrático regular, entonces un subespacio U de V es regular si, y sólo si, existe W subespacio de V tal que $V = U \perp W$. (Sug. usar el Corolario 1. 2. 2.).

4. Si (V, B) es un F-espacio cuadrático de dimensión 2, demostrar que son equivalentes:

a) V es regular e isótropo (es decir, plano hiperbólico).

b) V es regular con $d(V) = -1$.

5. Considerar el F-espacio unidimensional $\langle a\rangle$, $a \in \dot{F}$, ϱ un automorfismo de F como un F-espacio con la acción de escalares $c \cdot x = \varrho(c)x$ y $c, x \in \dot{F}$, y definir $B(x, y) = \varrho^{-1}(axy)$. Demostrar que (F, B) es isométrico al espacio $\langle \varrho^{-1}(a)\rangle$.

6. Sea (V, B) un espacio cuadrático regular. Si U es un subespacio de V totalmente isótropo, es decir, la restricción de B a $U\times U$ es 0, demostrar que existe un subespacio T de V, cuya dimensión es $2\dim(U) \neq \neq 0$, tal que U está contenido en T. (Sug. tomar $x_1, \ldots, x_s$ F-base de U y sea S el subespacio generado por $x_2, \ldots, x_s$. Aplicar el ejercicio 2-a para demostrar que existe un vector y_1 ortogonal a S pero no a x_1; en particular x_1 e y_1 son linealmente independientes y por el ejercicio 4 se sigue que ellos generan un plano hiperbólico, por lo tanto $V = H \perp V_1$, donde $S \subseteq V_1$. Usar el Corolario 1. 2. 2. para ver que V_1 es regular y aplicar la hipótesis inductiva para llegar a la conclusión).

7. Sobre un cuerpo F, demostrar la equivalencia de los siguientes enunciados:

a) Toda F-forma de dimensión 4 y determinante -1 es isótropa.

b) Toda F-forma de dimensión par y determinante -1 es isótropa.

c) Toda F-forma de dimensión 3 representa su determinante.

d) Toda F-forma de dimensión impar representa su determinante.

8. (Pfister).[13] Demostrar que I^2F está formado por las formas f de dimensión par $= n$ tales que: $d(f) = (-1)^{\frac{n(n-1)}{2}}$. (Sug. definir la aplicación $d_\pm : WF \to \dot{F}/\dot{F}^2$, como:

$$d_\pm(f) = d(f)(-1)^{\frac{n(n-1)}{2}} = \begin{cases} d(f), & \text{si } n \equiv 0, 1 \text{ mód. } (4) \\ -d(f), & \text{si } n \equiv 2, 3 \text{ mód. } (4) \end{cases}$$

Mostrar que la definición es consistente y que la restricción a IF es un epimorfismo de grupos, cuyo núcleo es I^2F).

9. Demostrar que WF es un anillo noetheriano si, y sólo si, F tiene un número finito de clases módulo cuadrados (Sug. usar el ejercicio 8).

10. Demostrar que en WF se tiene:

$$\langle a \rangle + \langle b \rangle = \langle a + b \rangle (\langle 1 \rangle + \langle ab \rangle); \; a, b, a + b \in \dot{F}.$$

11. Demostrar que si K/F es una extensión de cuerpos, entonces $(\frac{a, b}{K}) \simeq$ $\approx K \otimes_F (\frac{a, b}{F})$.

12. Verificar las fórmulas siguientes:

a) $N(w) = a_0^2 - a_1^2 a - a_2^2 b + a_3^2 ab$.

b) $T(w) = 2a_0$.

c) $N(u \cdot w) = N(u) N(w)$.

d) $T(u + w) = T(u) + T(w)$.

e) $w^2 = -N(w)$, si w es puro, y $w^2 = N(w)$, si w escalar. Donde $u, w \in$ $\in (\frac{a, b}{F})$ y $w = a_0 + a_1x_1 + a_2x_2 + a_3x_3$, $\{1, x_1, x_2, x_3\}$ es la F-base de definición.

13. $w \in (\frac{a, b}{F})$; w es inversible si, y sólo si, $N(w)$ es escalar no nulo. Si w inversible, $w^{-1} = (N(w))^{-1}w$.

14. Demostrar que $(\frac{a, b}{F})$ es central simple, es decir, que los elementos del álgebra que conmutan con todo elemento del álgebra son los escalares y que $(\frac{a, b}{F})$ no tiene ideales biláteros no triviales.

15. Sean A una F-álgebra e $y, z \in A$ tales que $y^2 = a$, $z^2 = b$ (en A estamos también identificando los escalares c con $c \cdot 1 \in A$, donde 1 es la identidad multiplicativa de A), $yz = -zy$ donde $a, b \in \dot{F}$. Demostrar que el subespacio vectorial del F-espacio A, generado por $\{1, y, z, yz\}$ es una F-álgebra isomorfa a $(\frac{a, b}{F})$. (Sug. definir $h: (\frac{a, b}{F}) \to A$ tal que $h(1) = 1$, $h(x_1) = y$, $h(x_2) = z$, $h(x_3) = yz$, donde $1, x_1, x_2, x_3$ es la F-base de definición de $(\frac{a, b}{F})$ y aplicar el ejercicio 14 para mostrar que h es un isomorfismo.

16. Aplicar el ejercicio 15 para demostrar que si $a, b, x, y \in F$, entonces:

a) $M_2(F)$ isomorfo $(\frac{1, -1}{F})$.

b) $(\frac{a, b}{F}) \approx (\frac{ax_2^2 - by^2}{F})$.

(Sug. considerar $e_{11} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, $e_{12} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$, $e_{21} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$, $e_{22} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$, y tomar en el ejercicio 15, $y = e_{21} + e_{12}$ y $z = e_{21} - e_{12}$.)

17. Sea $h: A \to A'$ un isomorfismo de A sobre A', donde A y A' son álgebras de cuaterniones sobre F. Demostrar que $h(A_0) = A_0'$ y que satisface: $\overline{h(x)} = h(\bar{x})$, $N(h(x)) = N(x) = h(N(x))$, $T(h(x)) = h(T(x)) = T(x)$. En particular, como $N(h(x)) = N(x)$, se tiene que h es una isometría de los F-espacios cuadráticos A y A'. Probar también lo recíproco, es decir si A y A' son isométricos, entonces son isomorfos como álgebras.

18. Sea $A = (\frac{a, b}{F})$. Demostrar que son equivalentes:

a) A es isomorfo a $M_2(F)$.

b) A no es álgebra de división.

c) A es isótropo como espacio cuadrático.

d) A_0 es hiperbólico como espacio cuadrático.

e) La forma $\langle a, b \rangle$ representa 1.

19. Sea F un cuerpo finito cuya característica es $\neq 2$, demostrar que $\forall\, a, b \in \dot{F}$ es $(\frac{a, b}{F}) \simeq M_2(F)$.

20. Sea $a, b, c \in \dot{F}$. Demostrar que:

$$(\frac{a, bc}{F}) \otimes_F (\frac{c, -a^2c}{F}) \simeq (\frac{a, bc}{F}) \otimes_F M_2(F).$$

21. Sea $A = (\frac{a, a'}{F})$, $B = (\frac{b, b'}{F})$. Demostrar que existe $c \in \dot{F}$ tal que $A = (\frac{a, c}{F})$ y $B = (\frac{b, c}{F})$, si $A \simeq B$.

22. Sean F un cuerpo y f una F-forma, se define $G(f) = G_F(f)$ el "subgrupo de isotropía" de f de igual manera que en la página 23; demostrar que:

a) $G(f)$ es un subgrupo de $\dot{F}$, tal que $\dot{F}^2 \subseteq G(f)$.

b) $G(f) = \dot{F}$, si f es hiperbólica.

c) $G(f) = \dot{F}^2$, si f es de dimensión impar.

d) Si $a \in D_F(f)$, entonces $aG(f) \subseteq D_F(f)$.

e) $-1 \in G(f)$ si, y sólo si, $f \perp f$ es hiperbólica.

23. Demostrar que dos formas ternarias isótropas que tienen el mismo determinante son isométricas.

24. Sean $f = \langle a_1, \ldots, a_n \rangle$ y $g = \langle b_1, \ldots, b_n \rangle$ formas diagonales. Se dice que f *es equivalente-simple a* g si existen índices i, j *tales que* $\langle a_i, a_j \rangle \simeq \langle b_i, b_j \rangle$ (conviniendo en que si $i = j$, por $\langle a_i, a_j \rangle$, se entiende $\langle a_i \rangle$) y $a_r = b_r$, si $r \neq i, j$. Se dice que la forma diagonal f *es equivalente en cadena a la forma diagonal* g si existe una sucesión $f_0, f_1, \ldots, f_m$ tal que $f_0 = f$, $f_m = g$, y cada f_j es equivalente-simple a f_{j+1} $j = 0, \ldots, m - 1$. Demostrar:

a) La equivalencia en cadena es una relación de equivalencia en el conjunto de formas diagonales de la misma dimensión.

b) Dos formas f y g diagonales, de la misma dimensión, son equivalentes si, y sólo si, son equivalentes en cadena. (Sug. suponer que f y g son formas regulares, y aplicar inducción sobre la dimensión n de f y g. Si $n = 1, 2$ no hay nada que demostrar; supóngase $n \geq 3$. Se elige, en el conjunto de formas diagonales que son equivalentes en cadena con f, una forma $f' = \langle c_1, \ldots, c_n \rangle$ con la propiedad de que la subforma $\langle c_1, \ldots, c_r \rangle$ representa a b_1 y r mínimo. Demuéstrese que $r = 1$ y por lo tanto f es equivalente en cadena con $\langle b_1, c_2, \ldots, c_n \rangle$. Como la equivalencia en cadena implica la equivalencia de formas cuadráticas, por aplicación del teorema de cancelación se tiene $\langle c_2, \ldots, c_n \rangle \simeq \langle b_2, \ldots, b_n \rangle$, y por la hipótesis inductiva, obtenemos $\langle c_2, \ldots, c_n \rangle$ equivalente en cadena con $\langle b_2, \ldots, b_n \rangle$. De esto se puede concluir que f es equivalente en cadena con g).

2

FORMAS CUADRÁTICAS SOBRE EXTENSIONES ALGEBRAICAS DE CUERPOS

2.1. LA APLICACIÓN $r: WF \to WK$

Consideremos K/F una extensión de cuerpos, toda F-forma cuadrática f es también una K-forma; sin embargo, las propiedades de f como F-forma serán en general diferentes de las propiedades de f como K-forma. Así, por ejemplo, sobre el cuerpo Q de los racionales $f = X_1^2 - 2X_2^2$ es anisótropa puesto que la raíz cuadrada de 2 no es racional, pero sobre la extensión $Q(\sqrt{2})$ es inmediato ver que f es isótropa. En este capítulo vamos a estudiar una forma f sobre K suponiendo que conocemos el comportamiento de f sobre el cuerpo de base F, y en particular en el caso en que K/F es una extensión algebraica. En vista de ello establecemos el siguiente lema.

Lema 2.1.1. Sean (V, B) un F-espacio cuadrático, K/F una extensión de cuerpos y (V_K, B_K), donde $V_K = K \otimes_F V$ se considera con su estructura de K-espacio vectorial y $B_K: V_K \times V_K \to K$ se define por:

$B_K(a \otimes u, b \otimes v) = abB(u, v)$; $a, b \in K$; $u, v \in V$. Entonces (V_K, B_K) es un K-espacio cuadrático y si f es una F-forma correspondiente a (V, B), entonces (V_K, B_K) es un K-espacio correspondiente a f como K-forma cuadrática.

Demostración. La acción de K sobre V_K se define por $a \cdot (b \otimes v) = ab \otimes v$; $a, b \in K$, $v \in V$. Un cálculo directo demuestra que B_K es una forma K-bilineal simétrica. Si $x_1, \ldots, x_n$ es una F-base de V, ortogonal con relación a B, entonces $1 \otimes x_1, \ldots, 1 \otimes x_n$ es una K-base ortogonal en V_K, luego la matriz $(B_K(1 \otimes x_i, 1 \otimes x_j))$ correspondiente a (V_K, B_K) es justamente la matriz que define f como K-forma.

Denotaremos por f_K o $K \otimes_F f$ la forma f considerada como K-forma y según las identificaciones acordadas se tiene que $f_K \simeq (V_K, B_K) \simeq K \otimes_F f$.

Considerando los anillos de Witt asociados a F y a K, las consideraciones expuestas permiten definir una aplicación $r: WF \to WK$ tal que $r(f) = f_K$. Obsérvese que:

a) r es un homomorfismo de anillos.

b) Si toda forma sobre F que es anisótropa permanece anisótropa sobre K, entonces r es un monomorfismo.

c) En general lo recíproco no es verdadero, esto es, si r es inyectivo no implica que las formas anisótropas sobre F permanezcan anisótropas sobre K. Roger Ware[15] formuló tal pregunta en 1975, y recientemente halló un contraejemplo, es decir, un ejemplo de una extensión (alge-

braica) K/F donde r es inyectivo y existe sobre F una forma anisótropa que sobre K es isótropa.[18] Al final del capítulo se verán algunos casos en los que la inyectividad de r implica la preservación de las formas anisótropas de F a K. Este problema de la preservación de formas anisótropas es estudiado con mayor generalidad por Gentile-Shapiro.[6]

Se denota por $W(K/F)$ el núcleo de r, ideal de gran importancia en el estudio de las formas cuadráticas sobre extensiones de cuerpos, cuando dichas extensiones son algebraicas.

d) Si K/F es una extensión de cuerpos, donde $K = F(X)$, X elemento trascendente sobre F, veamos qué es $W(K/F)$. Sea f una F-forma anisótropa, $f \simeq \langle a_1, \ldots, a_n \rangle$, donde $a_i \in \dot{F}$. Si f es isótropa sobre K, podemos entonces hallar $f_1(X), \ldots, f_n(X)$, expresiones polinómicas en X, no todas nulas y no divisibles simultáneamente por X tales que $\sum_{i=1}^{n} a_i f_i^2(X) = 0$; luego especializando en $X = 0$, la relación anterior se transforma en $\sum_{i=1}^{n} a_i f_i^2(0) = 0$, donde algún $f_j(0) \neq 0$, lo que es contrario a nuestra suposición sobre f. Se concluye pues que f es anisótropa sobre K y, en particular, $W(K/F) = 0$. Más generalmente, se ha demostrado que si K/F es una extensión trascendente pura, de grado finito, entonces las formas anisótropas sobre F se preservan a K, esto es, continúan siendo anisótropas sobre K.

Por lo dicho en d), en el presente capítulo sólo se considerarán extensiones algebraicas.

2.2. LA "TRANSFERENCIA" DE SCHARLAU

Supongamos K/F algebraica de grado finito y $S: K \to F$ una aplicación F-lineal no nula. Para (V, B) K-espacio cuadrático se puede definir el par (V, SB), donde V se considera F-espacio vectorial (por lo tanto, $\dim_F V = [K:F] \dim_K V$) y $SB: V \times V \to F$ se define $SB(u, v) = S(B(u, v))$. Con estas notaciones:

Lema 2.2.1. (V, SB) es un F-espacio cuadrático.

Demostración. $SB = SoB$ es claramente bilineal simétrica. Si (V, SB) no fuese regular existiría un elemento $w \in V$ tal que $S(B(w, y)) = 0$ $\forall\, y \in V$, pero como (V, B) es regular, existe un $y' \in V$ tal que $B(w, y') \neq 0$, luego para todo $a \in K$ se tiene: $B(w, \frac{a}{B(w, y')} y') = a$ y, por lo tanto, $S(a) = SB(w, \frac{a}{B(w, y')} y') = 0$, luego S es nula. Lo que es contrario a nuestra suposición.

Se denomina el par (V, SB) la "transferencia" de (V, B) por S. Más simplemente, se denota por $S(V)$ el par (V, SB). Tenemos una aplicación de WK en WF definida por: $(V, B) \to S(V)$, la que se denomina también

por S; S es llamada la aplicación de transferencia. Se observa inmediatamente que S es homomorfismo de grupos aditivos, esto es $S(V_1 \perp V_2) \simeq S(V_1) \perp S(V_2)$.

Ejemplo 1. Sea K/F, donde $[K:F] = n$, K es provisto de una estructura de espacio cuadrático sobre K por la forma bilineal $B:K\times K \to K$ tal que $B(x,y) = x \cdot y$. Luego (K,B) es K-espacio de dimensión 1, esto es $\langle 1\rangle_K$. Sea S una aplicación F-lineal no nula de K en F, $SB(x,y) = S(xy)$ y por tanto $S(\langle 1\rangle_K) = (K, SB)$.

A continuación se considerará un importante teorema:

Teorema 2.2.2. Sean K/F una extensión de grado finito y $S:K \to F$ una aplicación F-lineal no nula, luego para todo V, F-espacio, y U, K-espacio, se tiene la siguiente isometría:

$$S((K \underset{F}{\otimes} V) \underset{K}{\otimes} U) \simeq V \underset{F}{\otimes} S(U),$$

Demostración. Definimos: $h:S(V_K \underset{K}{\otimes} U) \to V \underset{F}{\otimes} S(U)$ por $h((a \otimes v) \otimes u) = v \otimes (au)$; $a \in K$, $v \in V$, $u \in U$. Un cálculo directo demuestra que h es un homomorfismo sobre F, cuyo inverso es $v \otimes u \to (1 \otimes v) \otimes u$. Veamos que h es una isometría. Sean $a, a' \in K$, $v, v' \in V$ y $u, u' \in U$ y denotemos por B la forma bilineal en $V \underset{F}{\otimes} S(U)$ y por B' la forma bilineal en $V_K \otimes U$. Entonces si se usa B_V para la forma bilineal de V, se tiene que:

$$B(h((a \otimes v) \otimes u),\ h((a' \otimes v') \otimes u') = B(v \otimes au,\ v' \otimes a'v') = B_V(v, v').$$

$$B_{SU}(au, a'u') = B_V(v, v') \cdot S(aa'B_U(u, u').$$

Por otra parte, como la forma bilineal en $V_K \otimes U$ es B', entonces la forma bilineal asociada a $S(V_K \otimes U)$ es SB', y $SB'((a \otimes v) \otimes u,\ (a' \otimes v') \otimes u') = S(B_{V_K}(a \otimes v,\ a' \otimes v')\, B_U(u, u')) = S(aa'B_V(v, v')\ B_U(u, u')) = B_V(v, v')\, S(aa'B_U(u, u'))$. Comparando ambas expresiones se concluye que h preserva los productos bilineales y es por tanto una isometría.

Corolario 2.2.3. Con las notaciones del teorema anterior se tiene $S(V_K) \simeq V \underset{F}{\otimes} S(\langle 1\rangle_K)$.

Demostración. Basta tomar $U = \langle 1\rangle_K$.

Corolario 2.2.4. Sean K/F una extensión algebraica de grado finito, $S:K \to F$, F-lineal no nula, entonces si U es un K-espacio hiperbólico, $S(U)$ es un F-espacio hiperbólico.

Demostración. Como S es homomorfismo aditivo, será suficiente demostrar que $S(H_K)$ es hiperbólico, y esto resulta si se reemplaza en el corolario anterior $V = H_F$, ya que $H_F \underset{F}{\otimes} S(\langle 1\rangle_K) \simeq [K:F] \cdot H_F$.

2.3. EXTENSIONES DE GRADO IMPAR

En esta sección nos limitaremos a demostrar un resultado de T. A. Springer, que establece que las formas anisótropas sobre F se preser-

van a la extensión K si la dimensión es impar, en particular $W(K/F) = 0$, y por lo tanto el estudio del núcleo de $r: WF \to WK$ se trivializa.

Teorema 2.3.1. Sea K/F una extensión algebraica de grado impar, entonces las formas anisótropas sobre F permanecen anisótropas sobre K.

Demostración. Se puede suponer que $K = F(a)$, con $[K:F] = m$ impar, pues $K = F(x_1, \ldots, x_n)$ para ciertos $x_i \in K$, y K se obtiene "coronando" una "torre" cuyos pisos son extensiones monógenas de grado impar.

Sea f una F-forma de grado n, la cual suponemos anisótropa, y además elijamos una representación diagonal de f. La demostración la haremos por inducción sobre $[K:F] = m$. Para $m = 1$, no hay nada que probar. Sea $m > 1$ y supongamos la validez del teorema para extensiones de grado impar menor que m, que son monógenas. Denotemos por $p(X)$ el F-polinomio minimal de a. Si f fuese isótropa sobre K, entonces existirían $x_1, \ldots, x_n$, en K, no todos nulos, tales que $f(x_1, \ldots, x_n) = 0$, de donde se obtendría:

$$f(\varphi_1(a), \ldots, \varphi_n(a)) = 0, \text{ con } \varphi_j(X) \in F[X] \qquad (')$$

expresando cada x_j en la base $1, a, \ldots, a^{m-1}$.

De (') se sigue que $f(\varphi_1(X), \ldots, \varphi_n(X)) = p(X)q(X)$, donde $q(X) \in F[X]$. Ahora bien, si existiera un polinomio $s(X)$ en $F[X]$, irreducible, dividiendo todos los $\varphi_j(X)$ tendríamos $f(\varphi_1(X), \ldots, \varphi_n(X)) = s(X)^2 f(\varphi_1'(X), \ldots, \varphi_n'(X))$, $\varphi_j'(X)$ en $F[X]$, pero $\operatorname{gr}(s(X)) \leq \max_j\{\operatorname{gr}(\varphi_j(X))\} = m_1 \leq m - 1$, luego la factorización única y $\operatorname{gr}(s) < \operatorname{gr}(p)$ implican que $q(X) = s(X)^2 q'(X)$ para algún $q'(X)$ en $F[X]$, de donde se obtendría $f(\varphi_1'(X), \ldots, \varphi_n'(X)) = p(X)q'(X)$ en $F[X]$. Cabe suponer en consecuencia que en:

$$f(\varphi_1(X), \ldots, \varphi_n(X)) = p(X)q(X) \qquad (")$$

no existe un factor irreducible en $F[X]$ que divida simultáneamente los φ_j. Luego $F[X] = \sum_{j=1}^{n} F[X]\varphi_j(X)$, y de esta representación podemos observar que los φ_j no pueden tener una raíz en la clausura algebraica de K que sea común a todos, y también que $q(X) \neq 0$, pues bastaría tomar un $c \in F$ y reemplazar en (") para ver que f sería isótropa sobre F. Observamos que $\operatorname{gr}(q) = 2m_1 - m \leq 2(m-1) - m = m - 2$, esto es $q(X)$ es polinomio de grado impar y menor que m. Tomemos b raíz de un factor irreducible de $q(X)$, que tenga grado impar, entonces $F(b)/F$ es de grado impar menor que m, luego por nuestra hipótesis de inducción f es anisótropa sobre $F(b)$, pero $(\varphi_1(b), \ldots, \varphi_n(b)) \neq 0$ es un vector isótropo para f sobre $F(b)$, lo que es una contradicción, en consecuencia debe ser f anisótropa sobre K.

2.4. EXTENSIONES DE GRADO PAR

Si K/F es una extensión algebraica de grado finito, en la sección anterior hemos visto que si $[K:F]$ es impar, el problema de caracterizar

$W(K/F)$ es trivial en virtud del teorema de Springer. Si $[K:F]$ es par, el problema está aún sin resolver. En esta sección se expondrán los principales resultados para el caso $[K:F] = 2$, que está totalmente resuelto.

Teorema 2.4.1. Sean $K = F(\sqrt{d})$ una extensión cuadrática de F y q una F-forma anisótropa. Entonces:

a) q_K es isótropa si, y sólo si, q contiene una subforma del tipo $\langle a\rangle \otimes \langle 1, -d\rangle$, $a \in \dot{F}$.

b) q_K es hiperbólica si, y sólo si, existe una F-forma h tal que $q \simeq \langle 1, -d\rangle \otimes h$.

c) $W(K/F) = WF\langle 1, -d\rangle = WF\ll -d\gg$.

Demostración. a) Si $q \simeq \langle a\rangle \otimes \langle 1, -d\rangle \perp f$ sobre F, entonces $q_K \simeq \langle a\rangle_K \otimes \langle 1, -d\rangle_K \perp f_K \simeq H_K \perp f_K$.

Recíprocamente, sea $q = \langle a_1, \ldots, a_n\rangle$ y supongamos que q_K es isótropa; luego, puesto que $\{1, \sqrt{d}\}$ es una F-base de K, podemos obtener una relación de la forma siguiente $\sum_{i=1}^{n} a_i(x_i + y_i\sqrt{d})^2 = 0$, con $x_i, y_i \in F$ no todos nulos, de donde:

$$\sum_{i=1}^{n} a_i x_i^2 + d\sum_{i=1}^{n} a_i y_i^2 = 0 \text{ y } \sum_{i=1}^{n} a_i x_i y_i = 0.$$

En consecuencia, los vectores $x_1 = (x_1, \ldots, x_n)$ e $y = (y_1, \ldots, y_n)$ son ortogonales en el F-espacio cuadrático (F^n, B_q) (Véase el ejemplo 2, cap. 1), y además $q(x) = -dq(y)$, si $x = 0$, entonces $y = 0$ por ser q anisótropa, contrario a la elección de los x_i e y_i, entonces $x \neq 0$ e $y \neq 0$, y podemos considerar una diagonalización de q en una base que contenga a x e y, es decir $q \simeq \langle q(x), q(y), b_3, \ldots, b_n\rangle \simeq \langle q(x), q(y)\rangle \perp f$. Por consiguiente $q \simeq \langle q(y)\rangle \otimes \langle 1, q(x)/q(y)\rangle \perp f$, $q \simeq \langle a\rangle \otimes \langle 1, -d\rangle \perp f$, donde $q(y) = a \in \dot{F}$.

b) Si $q \simeq \langle 1, -a\rangle \otimes h$, entonces $q_K \simeq \langle 1, -d\rangle_K \otimes h_K \simeq \dim(h)\, H_K$, es decir q_K es hiperbólica. Recíprocamente, supongamos que q_K es hiperbólica y procedamos por inducción sobre $\dim(q)$. Si $\dim(q) = 0$, entonces $q = 0$ (anisótropa) y la conclusión es trivial; supongamos que $\dim(q) > 0$, por a) se obtiene: $q \simeq \langle a\rangle \otimes \langle 1, -d\rangle \perp f$; $a \in \dot{F}$ y $\dim(f) = \dim(q) - 2$. Como $q_K \simeq \langle a\rangle_K \otimes H_K \perp f_K$, tenemos, cancelando planos hiperbólicos, que f_K es hiperbólica, y si aplicamos la hipótesis inductiva a la F-forma f (que es anisótropa) hallamos:

$$f \simeq \langle 1, -d\rangle \otimes h_1 \text{ y } q \simeq \langle a\rangle \otimes \langle 1, -d\rangle \perp \langle 1, -d\rangle \otimes h_1 \simeq \langle 1, -d\rangle \otimes h.$$

c) Es inmediata por b).

Con más generalidad, si $K = F(\sqrt{a_1}, \ldots, \sqrt{a_n})$ es una extensión multicuadrática, entonces las formas $\langle 1, -a_i\rangle = \ll -a_i\gg$ se hacen hiperbólicas sobre K. Sabemos que en el caso $n = 1$, $W(K/F) = WF\ll -a_1\gg$, no se conoce

si en el caso multicuadrático el ideal generado por las formas $\langle 1, -a_1\rangle$, ..., $\langle 1, -a_n\rangle$ es $W(K/F)$. Cuando esto ocurre se dice que el cuerpo F es "1- amenable field" (notación de Elman y Lam). Se sabe, sin embargo, que si $K = F(\sqrt{a}, \sqrt{b})$, entonces $W(K/F) = WF \ll -a\gg + WF \ll -b\gg$. Adviértase que si a un ideal generado por formas de Pfister lo denominamos un ideal de Pfister, lo anterior significa que tanto en el caso cuadrático, como en el $K = F(\sqrt{a}, \sqrt{b})$, el núcleo de $r: WF \to WK$ es un ideal de Pfister. Un problema que en la actualidad es objeto de investigación es en qué casos $W(K/F)$ es un ideal de Pfister. Se tienen algunos resultados al respecto,[2-3] los cuales pueden consultarse en las referencias citadas.

Corolario 2.4.2. Si q es una F-forma tal que q_K es hiperbólica sobre $K = F(\sqrt{d})$, extensión cuadrática de F, entonces $\langle -d\rangle \otimes q \simeq q$ sobre F.

Demostración. Sea $q \simeq rH \perp q_a$ una descomposición de Witt de q sobre F, donde q_a es anisótropa, entonces $(q_a)_K$ es hiperbólica por el teorema de cancelación de Witt, y en consecuencia $q_a \simeq \langle 1, -d\rangle \otimes h$ en F, y como $\langle -d\rangle \otimes \langle 1, -d\rangle \simeq \langle 1, -d\rangle$, se tiene:

$$\langle -d\rangle \otimes \langle 1, -d\rangle \otimes h \simeq \langle 1, -d\rangle \otimes h, \text{ esto es } \langle -d\rangle \otimes q_a \simeq q_a,$$

de donde $\langle -d\rangle \otimes q \simeq \langle -d\rangle \otimes rH \perp \langle -d\rangle \otimes q_a \simeq q$.

2.5. FORMAS CUADRÁTICAS SOBRE EXTENSIONES DE GALOIS

Sea G un grupo de automorfismos de un cuerpo K, luego si (V, B) es un K-espacio cuadrático, entonces para cada $g \in G$, definimos el par (V^g, B^g), donde V como grupo abeliano coincide con V^g, si bien V^g está provisto de una multiplicación por escalares definida por $a \cdot v = g(a)v$, $a \in K$. $B^g: V^g \times V^g \to K$ es la aplicación definida por:

$$B^g(u, v) = g^{-1}(B(u, v)).$$

Es fácil verificar que (V^g, B^g) es un K-espacio cuadrático. Si q es una forma cuadrática que representa a (V, B), entonces se denota por q^g la forma correspondiente a (V^g, B^g).

Sea K/F una extensión de Galois finita, entonces por ser K/F separable, la aplicación traza de la extensión (véase el apéndice A) $T_{K/F}: K \to F$ es F-lineal no nula; por lo tanto, podemos considerar la "transferencia" asociada que denotaremos por Tr. A partir de estas consideraciones pasamos a demostrar un teorema debido a Scharlau-Knebusch.

Teorema 2.5.1. Sea $G = G(K/F)$ el grupo de Galois de la extensión Galois finita K/F, entonces para toda forma cuadrática q sobre K se tiene la siguiente isometría:

$$(\mathrm{Tr}(q))_K \simeq \perp_{g \in G} q^g$$

donde $\perp_{g \in G} q^g$ denota la suma ortogonal de los espacios cuadráticos q^g.

Demostración. Sea (V, B) un K-espacio cuadrático asociado a q, entonces es espacio de soporte de $\perp_{g \in G} q^g$ es $\perp_{g \in G} V^g$ y el de $\mathrm{Tr}(q)$ es V como F-espacio con la aplicación bilineal $(x, y) \to \mathrm{Tr}(B(x, y))$. Definimos:

$$f: K \otimes_F V \to \perp_{g \in G} V^g \text{ tal que } f(a \otimes v) = \sum_{g \in G} a \cdot v,$$

donde $a \cdot v$ denota el producto por escalares definido por cada $g \in G$ sobre el grupo aditivo V. Para ver si f está bien definida basta demostrar que $f(ba \otimes v) = f(b \otimes av)$, donde $b \in K$, $a \in F$ y $v \in V$. Pues si $x_1, \ldots, x_n$ es una F-base de K y $y_1, \ldots, y_m$ es una F-base de V, todo elemento $w \in K \otimes_F V$ puede escribirse $w = \sum_{i,j} a_{ij} x_i \otimes y_j = \sum_{i,j} (a_{ij} x_i) \otimes y_j =$ $= \sum_{i,j} x_i \otimes (a_{ij} y_j)$, donde $a_{ij} \in F$. Volviendo a la igualdad por probar tenemos que $f(ba \otimes v) = \sum_{g \in G} ba \cdot v = \sum_{g \in G} g(ba)v = \sum_{g \in G} g(b)av = \sum_{g \in G} b \cdot av = f(b \otimes av)$. Es fácil verificar que f es K-lineal y veamos que preserva los productos bilineales. Sean $b, b' \in K$ y $v, v' \in V$, entonces denotando por B' la forma bilineal sobre $\perp V^g$, tenemos:

$$B'(f(b \otimes v), f(b' \otimes v')) = \sum_{g \in G} B^g(b \cdot v, b' \cdot v') = \sum_{g \in G} g^{-1}(B(g(b)v, g(b')v') =$$

$$= \sum_{g \in G} g^{-1}(g(b)g(b')B(v, v')) = bb' \sum_{g \in G} g(B(v, v')) = bb' \operatorname{Tr}(B(v, v')) = (K \otimes$$

$$\otimes \operatorname{Tr}(B))(b \otimes v, b' \otimes v').$$

Como $\dim_K(K \otimes_F V) = \dim_F V = [K:F] \dim_K V = o(G)\dim_K V = \dim_K(\frac{\perp}{G} V^g)$ y al ser f lineal que preserva las formas bilineales (espacios regulares) se concluye que f es una isometría.

Retornemos a las extensiones de grado impar tomando en cuenta el siguiente resultado de Rosenberg-Ware. Denotemos por WK^G el conjunto de los elementos $f \in WF$ tales que $f^g = f$, donde K/F es una extensión de Galois con grupo G. Observamos que $\operatorname{Im}(r) \subseteq WK^G$, donde $r: WK \to WK$.

Teorema 2.5.2. Sea K/F extensión de Galois de grado impar, donde $G = G(K/F)$, luego $r: WF \to WK^G$ es un isomorfismo.

Demostración. Como la extensión es de Galois de grado finito, entonces podemos suponer que $K = F(a)$, sea $[K:F] = 2m + 1$. Definimos $S: K \to F$ por $S(1) = 1$, $S(a^2) = \ldots = S(a^{2m}) = 0$, que es una aplicación F-lineal. La forma $(x, y) \to \operatorname{Tr}(xy)$ es regular y por lo tanto existe un $b \in K$ tal que $S(y) = \operatorname{Tr}(by)$, $\forall\, y \in K$. De aquí, si (V, B) es un K-espacio cuadrático, entonces el soporte de $S(q)$ (donde q es la aplicación cuadrática asociada a (V, B)) es V, y la forma bilineal $S(q)(v) = S(q(v)) = \operatorname{Tr}(bq(v))$, entonces $S(q) \simeq \operatorname{Tr}(b \cdot q)$; en particular si $(V, B) \in WK^G$, tenemos:

$$r(S(q)) = K \otimes \operatorname{Tr}(b \cdot q) = \perp_{g \in G} (b \cdot q)^g = (\perp_{g \in G} \langle b \rangle^g) \cdot q$$

de acuerdo con el teorema anterior. Como q es cualquiera en WK^G, entonces obtenemos que $r(S(q)) = hq$, donde $h = \sum_{s \in G} \langle b \rangle^s$. Para determinar h basta reemplazar $q = \langle 1 \rangle_K$ en la relación obtenida, esto es $h = r(S(\langle 1 \rangle_K)) = r(\langle 1 \rangle_F) = \langle 1 \rangle_K$. Esto significa que $r \cdot S$ = identidad sobre WK^G, de lo que resulta r suryectiva y como la dimensión de K/F es impar, se tiene por el teorema de Springer que r es inyectiva, luego r es un isomorfismo sobre WK^G.

Se dijo en 2.1-c que, en general, no se cumple que si r es inyectivo para una extensión K/F arbitraria, entonces las formas anisótropas sobre F permanezcan anisótropas sobre K. Finalizamos este capítulo demostrando un resultado de Ware[18] que establece que si el cuerpo de base, F, es pitagórico y K/F es Galois finita, entonces la inyectividad de r equivale a que las formas anisótropas sobre F permanezcan anisótropas sobre K. Se harán primero algunas consideraciones sobre cuerpos. Diremos que F *es formalmente real* si la forma sobre F, $n\langle 1 \rangle$ (suma ortogonal de $\langle 1 \rangle$, n veces), es anisótropa para todo $n \geq 1$. Es fácil ver que esta condición es equivalente a que -1 no sea suma de cuadrados en F. Si F no es formalmente real, se dice simplemente que F es *no real*. Definimos F *pitagórico*, si toda suma de cuadrados en F es un cuadrado en F. Más adelante (en el capítulo siguiente) estudiaremos estos cuerpos.

Lema 2.5.1. Sea F un cuerpo no real y pitagórico, entonces F es cuadráticamente cerrado, por lo tanto $WF = Z_2$ e $IF = 0$.

Demostración. Todo $x \in F$ puede escribirse:

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

al ser -1 una suma de cuadrados, x es también una suma de cuadrados y por lo tanto un cuadrado, desde que F es pitagórico, luego F es cuadráticamente cerrado con lo que se concluye la demostración (véase el ejemplo 7, cap. 1).

Teorema 2.5.3. Sean F un cuerpo pitagórico y K/F una extensión de Galois finita. Son equivalentes:

a) $r: W \to WK$ es inyectiva.

b) Toda forma anisótropa sobre F permanece anisótropa sobre K.

Demostración. Basta probar que a) implica b). Si F no es real, por el lema, F es cuadráticamente cerrado, luego una forma q sobre F, anisótropa, debe ser necesariamente $\langle 1 \rangle_F$, pues $WF \cong Z_2$, y es claro que $q_K \simeq \langle 1 \rangle_K$ es anisótropa sobre K. Supongamos entonces que F es formalmente real y consideremos Tr la "transferencia" asociada a la aplicación $T_{K/F}$ traza de la extensión. Entonces, si $q = \langle a_1, \ldots, a_n \rangle$ es F-forma anisótropa, de 2.5.1. se obtiene $(\mathrm{Tr}(q_K))_K \simeq \sum_{s \in G} q_K^s \simeq [K:F] q_K$ puesto que $\mathrm{Im}(r) \subseteq WK^G$, donde $G = G(K/F)$. Por la inyectividad de r, se tiene $\mathrm{Tr}(q_K) \simeq [K:F]q$. Al ser q anisótropa y F pitagórico real es $[K:F]q$ también anisótropa, pues, en caso contrario, existirían elementos $x_1, \ldots, x_n$,

$n = \dim(q)$, donde cada x_j es suma de $[K:F]$ cuadrados en F y algún $x_j \neq 0$ (pues al ser formalmente real F, si una suma de cuadrados es cero, entonces todos los sumandos son ceros), tal que $a_1x_1 + \ldots + a_nx_n = 0$. Pero, por ser F pitagórico, cada x_j es un cuadrado, luego q es isótropa, contrario a nuestra hipótesis sobre q, por lo tanto debe ser $[K:F]q$ anisótropa y entonces $\mathrm{Tr}(q_K)$ anisótropa, de donde es inmediato ver que q_K es anisótropa.

EJERCICIOS

1. Si $V \simeq V_1 \perp V_2$, F-espacios cuadráticos, demostrar que $V_K \simeq (V_1)_K \perp \perp (V_2)_K$, donde K/F es una extensión de cuerpos arbitraria.

2. Demostrar:

a) $r: WF \to WK$ es un homomorfismo de anillos.

b) $S: WK \to WF$ es un homomorfismo de grupos aditivos para K/F extensión de grado finito. Además, si K/F y L/K son extensiones de grado finito, S y T aplicaciones $S: K \to F$ y $T: L \to K$, F-lineal y K-lineal, respectivamente, no nulas, entonces las aplicaciones de "transferencia" asociadas, S' y T', verifican $(S \circ T)' = S' \circ T'$.

3. Si K/F es una extensión de grado finita y $S: K \to F$ una aplicación F-lineal no nula, demostrar que si S' es la "transferencia" asociada, entonces $\mathrm{Im}(S')$ es un ideal en WF.

4. Sea K/F extensión de cuerpos y denotemos por $R = \mathrm{Im}(r)$, donde $r: WF \to WK$. Decimos que *g es una K-forma definida sobre F*, si existe una F-forma f tal que $g \simeq f_K$. Demostrar la equivalencia de las siguientes proporciones:

a) Si g es una K-forma definida sobre F, entonces su parte anisótropa g_a es definida sobre F.

b) Si g y $g \perp h$ son definidas sobre F, y g y h son K-formas, entonces h es definida sobre F.

c) Si $g \in R$, entonces g es definida sobre F.

d) Si f_K es isótropa, donde f es una F-forma, entonces existe una F-forma q tal que $f_K \simeq q_K$ y q es isótropa.

e) Si $g \in R$, entonces existe un $a \in \dot{F}$ tal que a está representada por g, salvo el caso en que $\dim(g) = 0$.

5. Si K/F es una extensión de cuerpos que satisface cualquiera de los enunciados del ejercicio anterior, se dice que K/F es una *extensión excelente*.

a) Demostrar que si toda forma anisótropa sobre F permanece anisótropa sobre K, entonces K/F es una extensión excelente (luego toda extensión de grado impar, toda extensión trascendente pura, toda extensión K/F, Galois finita con F pitagórico y $W(K/F) = 0$ son ejemplos de extensiones excelentes).

b) Supongamos que $W(K/F) = 0$, pero las formas anisótropas de F no se preservan a K, entonces demostrar que K/F no es una extensión excelente.

6. Si K/F es una extensión algebraica de grado n, demostrar que K/F es excelente si la condición d) en el ejercicio 4, o cualquiera de sus equivalentes, se verifica para toda forma de dimensión menor o igual que n. (Sug: sea φ una F-forma anisótropa sobre F con φ_K isótropa, probar que φ contiene una subforma φ_0, con $\dim(\varphi_0) \leq n$ tal que $(\varphi_0)_K$ es isótropa. Para ello tomar w vector isótropo para $\varphi_K \simeq V \otimes K$, luego $w = v_1 \otimes \sigma_1 + \ldots + v_n \otimes \sigma_n$, donde $v_i \in V$ y $\sigma_1, \ldots, \sigma_n$ es una F-base de K. Definir V_0 como el subespacio generado por $v_1, \ldots, v_n$. A V_0 se asocia una subforma φ_0 de φ, considerar luego una descomposición $\varphi \simeq \varphi_0 \perp \varphi_1$).

7. Aplicar el ejercicio 6 para demostrar que toda extensión cuadrática es excelente.

8. Sean K/L y L/F extensiones excelentes tales que $W(K/L)$ contenido en $R_{L/F} = \mathrm{Im}(r: WF \to WL)$. Demostrar que K/F es excelente. Demostrar que la propiedad de ser excelente para una extensión no es transitiva en "torre."

9. Demostrar que si K/F es extensión de Galois con $[K:F] = 2m$, m impar, entonces K/F es excelente. (Sug: usar el ejercicio 8.)

10. Sean K_1 y K_2 extensiones de F que satisfacen:

a) f_{K_2} isótropa implica f_{K_1} isótropa, $\forall f$, F-forma.

b) $W(K_1/F) \subset W(K_2/F)$.

Demostrar que si K_1/F es excelente, entonces K_2/F es excelente. Cuando es verdad a) y b), demostrar que el índice de Witt de f_{K_1} es igual al de f_{K_2} para toda F-forma f. (Sug: tomar h una K_2-forma definida sobra F y demostrar que su parte anisótropa es definida sobre F.)

11. Sean L/F y K/L extensiones. Si K/F es excelente y $W(L/F) = W(K/F)$, demostrar que L/F es excelente. (Sug: aplicar el ejercicio 10.)

12. Sean K/F una extensión algebraica de grado finito y S y T aplicaciones F-lineales no nulas de K en F. Demostrar que existe un automorfismo h del grupo aditivo WK tal que $T = S \cdot h$. (Sug: $S(\langle 1 \rangle_K)$ es F-espacio regular, luego $T(x) = S\beta(x, b)$ para algún $b \in \dot{K}$, definir h tal que $h(f) = \langle b \rangle \cdot f$.)

13. Sea K/F tal que $[K/F] = n$ y $K = F(a)$. Definimos $S(1) = 1$, $S(a) = S(a^2) = \ldots = S(a^{n-2}) = 0$. Demostrar que:

i) $S(\langle 1 \rangle_K) \cong (m - 1)H_F \perp \langle 1, -N_{K/F}(a) \rangle$, si $n = 2m$.

ii) $S(\langle 1 \rangle_K) \cong mH_F \perp \langle 1 \rangle_F$, si $n = 2m + 1$. (Sug: definir $K_0 = Fa + \ldots + Fa^{n-2}$, luego considerar $S(\langle 1 \rangle_K) = F + K_0$, observar que son ortogonales. Si $n = 2m$, demostrar que $a, a^2, \ldots, a^{n-2}$ generan un subespacio totalmente isótropo en K_0 y aplicar el ejercicio 6 del capítulo 1. Se obtiene $K_0 = (m - 1)H_F \perp K_1$. De otro lado, calcular que $d(K_1) = -a_0 F^2(K_1$ como

espacio cuadrático), donde $X^n + \ldots + a_1X + a_0$ es el polinomio minimal de a sobre F).

14. A partir de las mismas consideraciones que en el ejercicio anterior demostrar que:

i) si $n = 2m$, entonces $S(\langle a \rangle_K) = mH_F$.

ii) si $n = 2m + 1$, entonces $S(\langle a \rangle_K) = mH_F \perp N_{K/F}(a)$. (Sug: proceder en forma análoga al ejercicio anterior.)

15. Demostrar que la composición:

$$WF \xrightarrow{r} WK \xrightarrow{S} WF$$

coincide con la multiplicación por $S(\langle 1 \rangle_K)$, donde S es una aplicación F-lineal no nula de K en F.

16. Sea $K = F(\sqrt{d})$ una extensión cuadrática de F, y $T:K \to F$ definida por $T(1) = 0$ y $T(\sqrt{d}) = 1$, F-lineal.

a) Demostrar que la matriz asociada en la base $\{1, d\}$ al espacio $T(\langle x \rangle_K)$, $x \in \dot{K}$, es:

$$\begin{bmatrix} v & u \\ u & dv \end{bmatrix}, \text{ donde } x = u + v\sqrt{d};\ u,\ v \in F.$$

b) Demostrar de a) que $T(\langle x \rangle_K)$ es un plano hiperbólico si x es tal que $N_{K/F}(x)$ es cuadrado en $\dot{F}$.

17. Si $K = F(\sqrt{d})$ es una extensión cuadrática, aplíquese el ejercicio 16 para demostrar que la siguiente sucesión es exacta.

$$1 \longrightarrow \{\dot{F}^2, d\dot{F}^2\} \longrightarrow \dot{F}/\dot{F}^2 \xrightarrow{j} \dot{K}/\dot{K}^2 \xrightarrow{N} \dot{F}/\dot{F}^2$$

donde j es el homomorfismo inducido por la inclusión y N el inducido por $N_{K/F}$. (Sug: usar el ejercicio anterior para la exactitud en $\dot{K}/\dot{K}^2$.)

18. A partir de las mismas consideraciones que en el ejercicio anterior, demostrar que:

$$1/2\ o(\dot{F}/\dot{F}^2) \leq o(\dot{K}/\dot{K}^2) \leq 1/2\ o(\dot{F}/\dot{F}^2)^2.$$

19. Si K/F es una extensión algebraica de grado finito, $o(\dot{K}/\dot{K}^2)$ finito, demostrar que $o(\dot{F}/\dot{F}^2)$ es finito. Lo recíproco no es verdadero, T. Y. Lam ha demostrado el siguiente teorema (del cual construye un ejemplo de cuerpo F que tiene un número finito de clases módulo cuadrados, pero que admite una extensión K de grado finito con infinitas clases módulo cuadrados):

Teorema. (9, cap. 7, apéndice)

Sea F una extensión normal de un cuerpo de números algebraicos (extensión de grado finito de $\mathbb{Q}$). Toda extensión propia de grado finito de F tiene infinitas clases módulo cuadrados.

Aplique el teorema enunciado para demostrar que todo cuerpo de números algebraicos tiene infinitas clases módulo cuadrados.

3

FORMAS CUADRÁTICAS SOBRE CUERPOS FORMALMENTE REALES Y PITAGÓRICOS

La teoría de los cuerpos ordenados tiene sus orígenes en los trabajos de Artin y Schreier en los primeros años del presente siglo. Ellos advirtieron la estrecha relación entre el concepto de representar elementos de un cuerpo como suma de cuadrados y la noción de orden: así, por ejemplo, "la condición necesaria y suficiente para que un cuerpo tenga un orden es que la única representación del cero como suma de cuadrados sea la trivial ($0 = 0^2 + \ldots + 0^2$)", o también "un elemento es suma de cuadrados en un cuerpo ordenado si, y sólo si, es positivo en todos los órdenes del cuerpo". Las principales ideas de esta teoría las desarrollaron con relación al famoso "problema 17 de Hilbert" presentado por Hilbert al Congreso de Matemáticos celebrado en París en el año 1900, el cual se enuncia como sigue: Sea $f(X_1, \ldots, X_n) \in \mathcal{Q}(X_1, \ldots, X_n)$ y supongamos que para toda $(x_1, \ldots, x_n) \in R^n$ para la cual $f(x_1, \ldots, x_n)$ sea definido se tenga que $f(x_1, \ldots, x_n) \geq 0$, entonces ¿es $f(X_1, \ldots, X_n)$ una suma de cuadrados en el cuerpo $\mathcal{Q}(X_1, \ldots, X_n)$? Las respuestas para los casos $n = 1$ y $n = 2$ eran ya conocidas afirmativamente en 1893. En 1927, Artín demostró que la respuesta es afirmativa con mayor generalidad a la planteada por Hilbert, de la forma siguiente:

Sea F un subcuerpo del cuerpo real tal que F posee un único orden, si $f(X_1, \ldots, X_n) \in F(X_1, \ldots, X_n)$ es tal que $f(x_1, \ldots, x_n) \geq 0$ para toda $(x_1, \ldots, x_n) \in \mathcal{Q}^n$ en que está definido, entonces $f(X_1, \ldots, X_n)$ es una suma de cuadrados en $F(X_1, \ldots, X_n)$.

En los últimos años los considerables progresos alcanzados en la teoría de formas cuadráticas han permitido asimismo el desarrollo vigoroso de la teoría de cuerpos ordenados. En el presente capítulo se estudiarán las formas cuadráticas sobre estos cuerpos. Para una lectura más amplia el lector puede consultar la obra citada en la referencia.[14]

3.1. CONOS POSITIVOS Y CUERPOS ORDENADOS

Sea F un cuerpo y $P \subset F$; decimos que P es un precono positivo en F si P satisface las siguientes propiedades:

$P_1)$ $P + P \subseteq P$

$P_2)$ $P \cdot P \subseteq P$

$P_3)$ $-1 \notin P$

$P_4)$ $F^2 \subseteq P$,

donde $F^2 = \{x^2 / x \in F\}$. También, $P \subseteq F$ se llamará un *cono positivo* en F si satisface:

P_1 y P_2, y:

P_3') $P \cap -P = \{0\}$

P_4') $P \cup -P = F$.

Adviértase que todo cono positivo es un precono positivo, pues si $a \in F$, entonces $a \in P$ o $-a \in P$, luego $a^2 = a \cdot a = (-a)(-a) \in P$, en particular, $1 \in P$, luego $-1 \notin P$.

Proposición 3.1.1. Sea P_0 un precono positivo en F, entonces existe un cono positivo P en F que extiende P_0, esto es $P_0 \subset P$.

Demostración. Consideremos la familia de los preconos positivos que extienden P_0. Se ordena parcialmente por inclusión y, aplicando el lema de Zorn se obtienen elementos maximales en esta familia. Sea P uno de ellos; observamos que $\forall x \in F$, se tiene $Px \cap (1 + P) = \phi$ ó $-Px \cap (1 + P) = \phi$. Pues si $p_1 x = 1 + q_1$ y $-p_2 x = 1 + q_2$ con $p_1, q_1 \in P$, entonces $-p_1 p_2 x^2 \in 1 + P$, de donde $-1 \in P$, lo que es contrario a (P_3).

Probemos que $P \cup -P = F$. Sea $x \in F$ y supongamos que $Px \cap (1 + P) = \phi$. Definimos $P_1 = P - Px$ y entonces $P \subseteq P_1$, $-x \in P_1$, $P_1 + P_1 \subseteq P_1$ y $P_1 P_1 \subseteq P_1$. Si $-1 \in P_1$, entonces $Px \cap (1 + P) \neq \phi$, lo que contradice nuestra suposición. Luego $-1 \notin P_1$, y por lo tanto P_1 es un precono positivo que extiende P; entonces por la maximalidad, $P = P_1$, y por consiguiente $-x \in P$. Si fuese $-Px \cap (1 + P) = \phi$, procediendo en forma enteramente análoga, demostramos que $x \in P$. Finalmente, tenemos $P \cap -P = \{0\}$, pues como $P \cup -P = F$ es inmediato ver que $P \cap -P$ es un ideal de F, luego $P \cap -P = \{0\}$ ya que un cuerpo tiene solamente ideales triviales. En consecuencia P es el cono positivo buscado.

Corolario 3.1.2. Sobre un cuerpo F, cualquier precono positivo P_0 es la intersección de todos los conos positivos P que extienden a P_0.

Demostración. Tomemos un $x \notin P_0$, veamos que x no puede pertenecer a todo cono positivo que extiende a P_0. Afirmamos que $P_0 x \cap (1 + P_0) = \phi$, pues si existen $p, q \in P_0$ tales que $px = 1 + q$, entonces $x = (1 + q)\, p\, (\frac{1}{p})^2 \in P_0$. Como en la demostración de la proposición anterior $P_1 = P_0 - P_0 x$ es un precono positivo que extiende P_0; además $-x \in P_1$ y por la proposición anterior se puede extender P_1 a un cono positivo P tal que $-x \in P$, luego $x \notin P$.

Dado un cuerpo F, denotaremos por $\sum F^2$ el conjunto de las sumas de cuadrados en F; las siguientes propiedades de $\sum F^2$ pueden demostrarse en forma inmediata.

Proposición 3.1.3.

a) $\sum F^2$ está contenido en todo precono positivo.

b) $\sum F^2$ es cerrado respecto de la adición.

c) $(\sum F^2) - \{0\}$ es un subgrupo multiplicativo del grupo $\dot{F}$.

Demostración. c) si $a_1^2 + \ldots + a_n^2 \neq 0$, entonces:

$$(a_1^2 + \ldots + a_n^2)^{-1} = \sum \left(\frac{a_j}{\sum a_j^2}\right)^2.$$

Decimos que el *cuerpo F es ordenado (por P)* si existe en F un cono positivo P. Análogamente, F es *preordenado* si existe un precono positivo. Los elementos de P se llaman "positivos" y como es usual escribiremos $a \leq b$ para denotar que $b - a \in P$. Por ejemplo, en el cuerpo R de los números reales $P = \{x \in R / x \geq 0\}$ ($\geq$ ordinario de R) es un cono positivo en R, en cuyo caso la notación usual de R coincide con la que que estamos usando. Aún más, la teoría de cuerpos ordenados es una generalización de las propiedades de orden del cuerpo R, como se podrá apreciar con claridad en el presente capítulo. En la siguiente proposición se vincula el concepto de orden y de cuerpo formalmente real.

Proposición 3.1.4. Sobre un cuerpo F, son equivalentes:

a) F es ordenado

b) F es formalmente real

c) $a_1^2 + \ldots + a_r^2 = 0$ implica $a_1 = \ldots = a_r = 0$

d) $\sum F^2 \neq F$.

Demostración. La equivalencia de b) y c) es inmediata. d) $\rightarrow$ b); si -1 es suma de cuadrados, entonces todo $a \in F$ es suma de cuadrados, esto es $F = \sum F^2$. a) $\rightarrow$ d) es inmediato b) $\rightarrow$ a). Como $-1 \in \sum F^2$, entonces $\sum F^2$ es un precono positivo en F, en consecuencia, por la proposición 3.1.1., existe un cono positivo P extendiendo $\sum F^2$, luego F es ordenado.

Corolario 3.1.5. Sobre un cuerpo F formalmente real $\sum F^2$ es la intersección de todos los conos positivos de F.

Demostración. Como F es formalmente real, entonces $\sum F^2$ es un precono, y en consecuencia por el corolario 3.1.2. y la proposición 3.1.3. a. se concluye esta demostración.

Los elementos positivos en todo orden sobre F se llaman "totalmente positivos". El resultado anterior establece que un elemento es totalmente positivo si, y sólo si, es una suma de cuadrados en F.

Cabe observar que si P es un cono positivo en F, entonces $\dot{P} = P - \{0\}$ es un subgrupo multiplicativo de $\dot{F}$, cerrado aditivamente, de índice 2

en $\dot{F}$. Recíprocamente, si H es un subgrupo de F, cerrado aditivamente, de índice 2 en $\dot{F}$, entonces $P_1 = H \cup \{0\}$ es un cono positivo en F.

Lema 3.1.6. Si P_1 y P_2 son conos positivos sobre un cuerpo F, entonces $P_1 \subseteq P_2$ implica que $P_1 = P_2$.

Demostración. Se deja a cargo del lector.

Proposición 3.1.7. $\sum F^2$ es un cono positivo sobre F, si, y sólo si, F tiene un único orden.

Demostración. Si $\sum F^2$ es un cono positivo, entonces, como cualquier cono P contiene a $\sum F^2$, del lema anterior se tiene que $\sum F^2 = P$. En la hipótesis de que F tiene un único orden, supongamos que $\sum F^2$ no es un cono, luego $\sum F^2 \cup -\sum F^2 \neq F$, y entonces, de acuerdo con el corolario 3.1.2. para $x \notin \sum F^2$ y $x \notin -\sum F^2$ existen conos positivos P_1 y P_2 tales que $x \notin P_1$ y $-x \notin P_2$. Pero, por la hipótesis, $P_1 = P_2$ establece una contradicción, luego es $\sum F^2$ el único orden sobre F.

Ejemplo 1. Consideremos el cuerpo R de los números reales, es fácil establecer que $\sum R^2$ es un cono de orden en R, y por lo tanto, R tiene un único orden. De modo análogo, ocurre en el cuerpo Q de los racionales.

Ejemplo 2. Todo cuerpo formalmente real, con dos clases módulo cuadrados, se llama un *cuerpo euclidiano*. Si F es euclidiano, entonces $\dot{F}/\dot{F}^2 = \{1, -1\}$. Luego, si $x, y \in F$, ambos no nulos, entonces $x^2 + y^2 = u^2$ ó $x^2 + y^2 = -u^2$. Si fuese la segunda posibilidad, supongamos que $x \neq 0$, luego $1 + (y/x)^2 = -(u/x)^2$, de donde -1 es suma de cuadrados, lo que es contrario a que F es formalmente real, entonces debe ser $x^2 + y^2 = u^2$, esto es, F es pitagórico, por lo tanto $\sum F^2 = F^2$, y por la proposición 3.1.7., F es pitagórico con un solo orden. Observar que existen cuerpos formalmente reales con un solo orden, pero que no son pitagóricos, por ejemplo Q.

3.2. EXTENSIÓN DE ÓRDENES Y CUERPOS ORDENADOS MAXIMALES

Sean F un cuerpo real (usaremos "real" por "formalmente real"), P un orden en F y $f = \langle a_1, \ldots, a_n \rangle$ una F-forma de grado n. Definimos:

$$\mathrm{Sig}_P(f) = n^+ - n^-$$

donde n^+ = número de $a_i \in P$ y n^- = número de $a_i \in -P$.

Proposición 3.2.1. $\mathrm{Sig}_P(f)$ es un invariante para la clase de equivalencia de $f = \langle a_1, \ldots, a_n \rangle$.

Demostración. Supongamos $f = \langle a_1, \ldots, a_n \rangle \simeq \langle b_1, \ldots, b_n \rangle = g$ sobre F. Elegimos un F-espacio cuadrático (V, B) con bases $u_1, \ldots, u_n$ y $v_1, \ldots, v_n$ tales que $B(u_i, u_i) = a_i$, $B(v_i v_i) = b_i$ y $B(u_i, u_j) = B(v_i, v_j) = 0$, si $i \neq j$. Afirmamos que si $a_1, \ldots, a_r$ son todos los $a_i \in P$ (esto puede suponerse reordenando, si es necesario, los a_i en la representación de f) y $b_1, \ldots, b_s$ todos los $b_i \in P$, entonces, $u_1, \ldots, u_r$, $v_{s+1}, \ldots, v_n$ son linealmente independientes. En caso contrario, existirán $a_1', \ldots, a_r'$, $b_{s+1}', \ldots, b_n'$ en F, no todos nulos, tales que $a_1'u_1 + \ldots + a_r'u_r = b_{s+1}'v_{s+1} + \ldots$

$\ldots + b_n'v_n$, de donde se tiene: $B(\sum_{i=1}^{r} a_i'u_i, \sum_{j=1}^{r} a_j'u_j) = B(\sum_{h=s+1}^{n} b_h'v_h, \sum_{k=s+1}^{n} b_k'v_k)$,

esto es $(a_1')^2 a_1 + \ldots + (a_r')^2 a_r = (b_{s+1}')^2 b_{s+1} + \ldots + (b_n')^2 b_n \in -P$, por lo tanto $(a_1')^2 a_1 + \ldots + (a_r')^2 a_r \in -P$, lo que no es posible, por lo tanto $r + (n-s) \leq \leq \dim(V) = n$, luego $r \leq s$, y por simetría podemos probar que $s \leq r$ y concluir que $r = s$, por lo tanto $\mathrm{Sig}_P(f) = \mathrm{Sig}_P(g)$.

Podemos definir entonces una aplicación $\mathrm{Sig}_P: WF \to Z$ tal que a cada elemento $f \in WF$ le hace corresponder el entero $\mathrm{Sig}_P(f)$. Esta aplicación se llama la aplicación de *signatura respecto de* P. Observamos que Sig_P está definida sobre WF debido a que $\mathrm{Sig}_P(\langle 1, -1 \rangle) = 0$. Además se prueba directamente que Sig_P es un homomorfismo de anillos. Si f es una F-forma de grado n, entonces decimos que "f es positiva definida" respecto de P, si $\mathrm{Sig}_P(f) = n$; que "f es negativa indefinida respecto de P, si $\mathrm{Sig}_P(f) = -n$, y que "f es indefinida, si $|\mathrm{Sig}_P(f)| < n$.

Sean K/F una extensión de cuerpos y P un orden en F, decimos que *un orden* P' en K, *extiende* P a K, si $P' \cap F = P$. También decimos que P es la restricción de P' a F.

Proposición 3.2.2. Sean K/F una extensión de cuerpos y P un orden en F. P se extiende a K si, y sólo si, toda forma cuadrática sobre F, positiva definida respecto de P, es anisótropa sobre K.

Demostración. Observamos que toda F-forma positiva definida respecto de P es anisótropa sobre K, puesto que $\dot{P} = P - \{0\}$ es un grupo multiplicativo cerrado aditivamente (recordar que las formas consideradas son regulares). Recíprocamente, supongamos que esta condición es satisfecha.

Definimos $P_0 = \{ \sum_{i=1}^{n} a_i x_i^2;\ a_i \in \dot{P},\ x_i \in K,\ n \in Z^+ \}$.

Es inmediato verificar que $P_0 + P_0 \subseteq P_0$ y $P_0 \cdot P_0 \subseteq P_0$.

Además $-1 \notin P_0$; en caso contrario, existen $x_1, \ldots, x_r \in K$, no todos nulos, tales que $-1 = a_1 x_1^2 + \ldots + a_r x_r^2$, $a_i \in \dot{P}$, esto es, la F-forma $\langle 1, a_1, \ldots, a_r \rangle$, que es positiva definida respecto de P, es isótropa sobre K, contrario a la hipótesis. También $K^2 \subseteq P_0$, por lo tanto, P_0 es un precono positivo en K y por la proposición 3.1.1. existe un cono P' en K

que contiene a P_0, como $P' \cap F$ es un cono positivo en F y $P \subseteq P' \cap F$, del lema 3.1.6. se tiene que $P' \cap F = P$, esto es, P' extiende a P.

Corolario 3.2.3. Sea K/F una extensión de grado impar, entonces todo orden de F se extiende a K.

Demostración. Por el teorema 2.3.1. toda forma cuadrática anisótropa sobre F permanece anisótropa sobre K, en particular las formas positivas definidas respecto de algún orden P de F, luego por la proposición anterior P se extiende a K.

Corolario 3.2.4. Sea $K = F(\sqrt{d})$, una extensión cuadrática de F. Todo orden P de F se extiende a K si, y sólo si, $d \in P$.

Demostración. Sea P' una extensión de P a K, luego $d = (\sqrt{d})^2 \in P'$, entonces $d \in P' \cap F = P$. Recíprocamente, supongamos que no exista extensión de P a K, luego existe una forma $f = \langle a_1, \ldots, a_n \rangle$ positiva definida respecto de P que es isótropa sobre K, por lo tanto podemos encontrar x_i e y_i en F, no todos nulos, tales que $\sum_{i=1}^{n} a_i(x_i + y_i\sqrt{d})^2 = 0$, de donde $\sum_{i=1}^{n} a_i x_i + d \sum_{i=1}^{n} a_i y_i^2 = 0$, esto es $d = -\dfrac{a_i x_i^2}{a_i y_i^2} \in -P$, y por consiguiente $d \notin P$.

Corolario 3.2.5. Si K/F es una extensión trascendente pura de grado finito, entonces todo orden de F se extiende a K.

Demostración. K tiene la forma $K = F(x_1, \ldots, x_n)$, con x_i elementos trascendentes sobre F. Por la observación d), pág. 32, sabemos que las formas anisótropas sobre F permanecen anisótropas sobre K, por lo tanto, todo orden se extiende de F a K.

Nota: En los corolarios 3.2.3 y 3.2.5 podemos observar que la condición que determina la extensión de los órdenes de F a K es que en ambos casos las formas anisótropas sobre F permanecen anisótropas sobre K. Más generalmente, si K/F es una extensión de un cuerpo real F, y sabemos que las formas anisótropas sobre F permanecen anisótropas sobre K, podemos concluir que todo orden de F se extiende a K.

Un cuerpo F se llama "cerrado-real" si es formalmente real y toda extensión algebraica propia de F es no formalmente real, esto es, F es formalmente real maximal.

Proposición 3.2.6. Sea K un cuerpo cerrado-real, entonces K es euclidiano y todo polinomio de grado impar en $K[X]$ tiene una raíz en K.

Demostración. Veamos que K tiene sólo dos clases módulo cuadrados. Sean P un cono positivo en K y $a \in P$. Si a no es cuadrado de algún elemento de K, entonces, en virtud del corolario 3.2.4., P se extiende a $K(\sqrt{a})$. Por consiguiente, K admite extensiones propias que son formalmente reales, lo que es contrario a que K es cerrado-real, luego

$K^2 = P$, y como $K = P \cup -P$, se concluye que K es euclidiano. Sea $f(X)$ un polinomio de grado impar con coeficientes en K. Podemos suponer que f es irreducible, pues, en caso contrario, se toma un factor irreducible de grado impar de f, que existe, precisamente, porque el grado de f es impar. Si $gr(f) > 1$, se considera $L = K[X]/(f)$, donde (f) denota el ideal principal generado por f en $K[X]$. L/K es una extensión tal que $[L:K] = gr(f) > 1$, y, como $[L:K]$ es impar, todo orden de K se extiende a L, y por lo tanto L es formalmente real, lo que contradice nuestra hipótesis sobre K. Luego, $f(X)$ es de grado 1 y, por lo tanto, tiene una raíz en K.

Proposición 3.2.7. Sea K cerrado-real, entonces:

a) $K(i)$ es algebraicamente cerrado, donde $i^2 = -1$.

b) Los polinomios irreducibles sobre $K[X]$ tienen grado ≤ 2.

Demostración. Veamos primero que $K(i)$ es cuadráticamente cerrado. Tomemos $x \in K(i)$, luego $x = a + bi$ con $a, b \in K$. Si $b = 0$, entonces $x = a$ y, como K es euclidiano, a es un cuadrado o el opuesto de un cuadrado, y en consecuencia x es un cuadrado en $K(i)$ en este caso. Supongamos $b \neq 0$; debemos encontrar $u, v \in K$ tales que sea $a + bi = (u + vi)^2$, esto es $a = u^2 - v^2$ y $b = 2uv$, de donde $u^4 - au^2 - b^2/4 = 0$. Si escribimos $k = u^2$, es $k^2 - ak - b^2/4 = 0$, y como $a^2 + b^2 > 0$, podemos considerar que $(a^2 + b^2)^{\frac{1}{2}}$ denote la raíz positiva de $a^2 + b^2$ en K y entonces obtenemos $k = \frac{a + (a^2 + b^2)^{\frac{1}{2}}}{2}$. Si fuese $a + (a^2 + b^2)^{\frac{1}{2}} \leq 0$, entonces

$a - (a^2 + b^2)^{\frac{1}{2}} \leq 0$ y, por consiguiente, $a^2 - (a^2 + b^2) \geq 0$, esto es $-b^2 \geq 0$, luego $b = 0$, contrario a la elección de b. Resulta que $k > 0$ y entonces $k = u^2$ tiene solución en K.

Probaremos ahora que $K(i)$ es algebraicamente cerrado. Para ello sea $L/K(i)$ una extensión algebraica finita de $K(i) = F$ y veamos que $L = F$. Sin pérdida de generalidad podemos suponer que L/K es de Galois con grupo G (tomando la "menor" extensión de Galois de K que contiene a L). Si escribimos $[L:K]$ en la forma $2^r m$, con m impar, entonces, aplicando el teorema fundamental de Galois, al subgrupo de Sylow de orden 2^r de G le corresponde una extensión L' de K de grado m, impar, lo que implica L' real, y, por lo tanto, $m = 1$. Resulta que L/K es Galois de grado 2^r, entonces L/F es Galois de grado 2^e. Por aplicación nuevamente de la correspondencia de Galois a la extensión L/F, teniendo en cuenta que su grupo de Galois es un 2-grupo, tenemos que, necesariamente $e = 0$, pues si $e \geq 1$, aplicando la correspondencia de Galois existiría una extensión cuadrática de F, lo que es contrario a que F es cuadráticamente cerrado. Luego $L = F$.

Ahora, como $K(i)$ es algebraicamente cerrado, se concluye inmediatamente que los polinomios irreducibles sobre K tienen grado ≤ 2.

Sea (K, P), donde K es un cuerpo y P un orden fijado en K. Una extensión algebraica L/K se llama una "clausura real" para (K, P), si L es cerrado-real y el orden P es la restricción a K del único orden de L.

Teorema 3.2.8. Para todo cuerpo ordenado (F, P) siempre existe una clausura real.

Demostración. Consideremos la familia (K', P') tales que K'/F es una extensión algebraica y P' un orden en K' que extiende P. Esta familia es inductiva respecto del orden por inclusión y, por el lema de Zorn, existen elementos maximales. Sea (K_1, P_1) un elemento maximal. Observemos que P_1 es el único orden en K_1, pues si se toma $a \in P_1$, entonces a debe ser un cuadrado de algún elemento de K_1. En caso contrario, por el corolario 3.2.4., P_1 podría extenderse a $K_1(\sqrt{a})$ lo que no es posible por la maximalidad de (K_1, P_1). Luego $P_1 = K_1^2$ y, por la proposición 3.1.7., P_1 es el único orden sobre K_1. Además, si (K_1, P_1) tuviese una extensión propia ordenada, ella induciría el orden P_1 sobre K_1 y, por lo tanto, P sobre F, lo que nuevamente es contrario a la maximalidad. Luego (K_1, P_1) es cerrado-real.

Nos proponemos ahora demostrar que la clausura real de un cuerpo ordenado (F, P) es única, salvo isomorfismo sobre F. Haremos antes algunas consideraciones.

Sea A una F-álgebra de dimensión finita. Sabemos que está definida la aplicación traza, $\mathrm{Tr}: A \to F$, aplicación F-lineal, que, a su vez, permite definir una forma cuadrática T sobre F por $T(x, y) = \mathrm{Tr}(x \cdot y)$. T se denomina la forma traza asociada a A (véase el apéndice A).

Supongamos que $f(X)$ es un polinomio sobre F y consideremos $A = F[X]/(f)$; A es un álgebra sobre F cuya dimensión es $\leq \mathrm{gr}(f)$. Sean P un orden en F y F_p un cuerpo cerrado-real que contiene a F y cuyo único orden induce P sobre F. Observemos que la forma traza asociada a la F_p-álgebra $F_p \otimes_F F[X]/(f)$ es precisamente la forma traza T_f, asociada a la F-álgebra $F[X]/(f)$, considerada sobre F_p; es decir, $F_p \otimes_F T_f = (T_f)_{F_p}$. Se desea calcular en primer término $\mathrm{Sig}_p(T_f)$. Supongamos que $f(X)$ no tiene raíces múltiples en F_p.

Teorema 3.2.9. Con las notaciones precedentes:

$$\mathrm{Sig}_p(T_f) = \text{número de raíces de } f \text{ en } F_p$$

Demostración. Como $\mathrm{Sig}_p(T_f) = \mathrm{Sig}_p(T_f)_{F_p}$ se calcula sobre F_p. Luego f se factoriza en polinomios irreducibles lineales y cuadráticos según la proposición 3.2.7. Escribamos $f = f_1 \ldots f_r g_1 \ldots g_s$ tales que $\mathrm{gr}(f_i) = 1$ y $\mathrm{gr}(g_i) = 2$, donde todos los factores son diferentes puesto que f tiene todas sus raíces simples. Como:

$$F_p \otimes_F A = F_p \otimes_F F[X]/(f) \simeq \frac{F_p \otimes F[X]}{F_p \otimes (f)} \simeq \frac{F_p[X]}{(f)}$$

por el "teorema chino del resto" (véase el apéndice B) se tiene:

$$F_p \otimes_F A \simeq F_p[X]/(f_1) \times \ldots \times F_p[X]/(f_r) \times F_p[X]/(g_1) \times \ldots \times F_p[X]/(g_s)$$

esto es $F_p \otimes_F A \simeq F_p \times \ldots \times F_p \times F_p' \times \ldots \times F_p'$, donde $F_p' = F_p(t)$ con $t^2 = -1$.

Pero, la forma traza asociada a $F_p \otimes_F A$, restringida a cada factor de la

forma F_p, es la forma $\langle 1 \rangle$ sobre F_p y sobre F_p' tiene por matriz en la base $\{1, t\}$ a $\begin{bmatrix} 2 & 0 \\ 0 & -2 \end{bmatrix}$. Luego F_p' como espacios cuadráticos son planos hiperbólicos sobre F_p. Observamos también que los subespacios son mutuamente otorgonales respecto a la forma traza de $F_p \otimes_F A$. En consecuencia, $\mathrm{Sig}_p(T_t)_{F_p} = r$.

Nota. Este resultado significa que el número de raíces de un polinomio en un cuerpo cerrado-real que contenga a F, depende únicamente del tipo de orden inducido por el cerrado real y no de la elección del mismo.

Recordamos que si K/F es una extensión de cuerpos, $b \in K$ es un elemento F-algebraico y $h: F \to L$ un morfismo de cuerpos, entonces h puede extenderse a $F(b)$ si el polinomio f^h, donde f es el F-polinomio minimal de b y f^h se obtiene aplicando h a los coeficientes de f, tiene una raíz en L.

Corolario 3.2.10. Sea K/F una extensión de grado finito con $K = F(x)$, entonces un orden P sobre F se extiende a K si, y sólo si, el F-polinomio minimal f_x de x tiene una raíz en toda clausura real de (F, P).

Demostración. Si f_x tiene una raíz x' en una clausura real K' de (F, P), entonces $F(x)$ es F-isomorfo con $F(x')$, luego el orden inducido por el único orden de K' sobre $F(x')$ proporciona un orden sobre $F(x) = K$ vía el isomorfismo. Recíprocamente, si P se extiende a K, se considera una clausura real (K', P') de (F, P) tal que $K \subseteq K'$, luego f_x tiene una raíz en K', y como el número de raíces en una clausura real es independiente de la clausura elegida, se sigue que f_x tendrá una raíz en cualquier otra clausura real de (F, P).

Teorema 3.2.11. Sean (K, P') una extensión de grado finito del cuerpo ordenado (F, P) (esto es, $F \subseteq K$ y $P' \cap F = P$), y $h: F \to L$ una inmersión de F en un cuerpo L cerrado-real, que preserva el orden, entonces existe una extensión h' de h a K, la cual preserva el orden.

Demostración. Podemos suponer $K = F(b)$ porque la característica de los cuerpos formalmente reales es cero (claramente, por la proposición 3.1.4.c. no puede ser $1 + \ldots + 1 = 0$). Sea $f(X)$ el F-polinomio minimal de b y consideremos una clausura real K' de K. Por el teorema anterior, al tener f una raíz en K' se deduce que $f^h(X)$ tendrá una raíz en L, desde que h identifica F como un subcuerpo de L y por la observación previa al corolario 3.2.10. existe una extensión h' de h a K, con lo que se garantiza la existencia de extensiones de h a K. Supongamos que ninguna de las posibles extensiones de h a K preserve el orden, entonces, denotando por $h_1, \ldots, h_n$ estas extensiones, existen $a_i \in K$ tales que $a_i \in P'$, pero $h_i(a_i) \notin L^2$ (L^2 es el único orden de L). En virtud del corolario 3.2.4., podemos extender P' a $K(\sqrt{a_1}, \ldots, \sqrt{a_n})$. Consideremos g una extensión de h_j a $K(\sqrt{a_1}, \ldots, \sqrt{a_n})$, que existe por lo demostrado ya, luego: $h_j(a_j) = g(a_j) = g((\sqrt{a_j})^2) = (g(\sqrt{a_j}))^2 \in L^2$, lo que es contrario a la elección de a_j.

Teorema 3.2.12. Sea K una clausura real del cuerpo ordenado (F, P) y K' un cuerpo cerrado-real. Si h es una inmersión de F en K' que preserva el orden, entonces h se extiende en forma única a K.

Demostración. Por aplicación del Lema de Zorn y del teorema 3.2.11. resulta inmediato que h puede extenderse a K. Veamos la unicidad, si g_1 y g_2 fuesen extensiones de h a K, consideremos $a \in K$ y sean $a_1 < a_2 \ldots < a_r$ todas las raíces del F-polinomio minimal de a que están en K; por lo tanto, $g_1(a_1) < \ldots < g_1(a_r)$ son todas las raíces de f^h en K' por el teorema 3.2.9. y lo mismo ocurre con $g_2(a_1) < \ldots < g_2(a_r)$, de donde resulta $g_1(a_i) = g_2(a_i)$, $i = 1, 2, \ldots, r$ y en particular $g_1(a) = g_2(a)$, y por consiguiente $g_1 = g_2$.

Corolario 3.2.13. (Unicidad de las clausuras reales). Sean (F, P) un cuerpo ordenado y K_1 y K_2 dos clausuras reales de (F, P), entonces existe $h: K_1 \to K_2$ un F-isomorfismo de K_1 con K_2 que preserva el orden.

Demostración. Sean $i: F \to K_1$ y $j: F \to K_2$ las inmersiones canónicas de F en K_1 y K_2. Por aplicación del teorema 3.2.12. obtenemos $h_1: K_2 \to K_1$ extensión de i, y $h_j: K_1 \to K_2$, extensión de j, entonces $h_1 h_j: K_1 \to K_1$ que extiende a i, por la unicidad en el teorema mencionado, es la identidad sobre K_1 y, análogamente, $h_j h_1$ sobre K_2. Luego h_1 y h_j son F-isomorfismos inversos que necesariamente preservan el orden.

Corolario 3.2.14. Sea K una clausura real de un cuerpo ordenado F, entonces todo endomorfismo sobre F de K es la identidad sobre K.

Demostración. Tal endomorfismo es una extensión de la inmersión $i: F \to K$, y como la identidad es otra extensión, por la unicidad se concluye que ambas coinciden.

Proposición 3.2.15. Sean K/F una extensión algebraica de grado finito y P un orden en F que se extiende a K, entonces:

a) El número de diferentes extensiones de P a K es igual al número de diferentes F-inmersiones de K en una clausura real (arbitraria) de (F, P).

b) Si K/F es de Galois, entonces el número de extensiones de P a K es $[K:F]$.

Demostración. Como caract$(F) = 0$, existe $a \in K$ tal que $K = F(a)$. Sea $f(X)$ el F-polinomio minimal de a, y sean $a_1, \ldots, a_r$ las diferentes raíces de $f(X)$ en una clausura real de (F, P) que contiene K, por lo tanto existen F-morfismos de cuerpos $h_j: K \to F(a_j)$. Definimos P_j como $P_j = \{x \in K / h_j(x) > 0 \text{ en } F(a_j)\}$, donde el orden considerado sobre $F(a_j)$ es el inducido por el único orden de la clausura real, L, considerada. Es inmediato verificar que P_j es un cono positivo en K. Supongamos que $P_i = P_j$, entonces $h_j h_i^{-1}: F(a_i) \to F(a_j)$ es una F-inmersión de $F(a_i)$ en L, real cerrado, que además preserva el orden. Como L es una clausura real de $F(a_i)$, aplicamos el teorema 3.2.12. y encontramos un endomorfismo de L. En virtud del corolario 3.2.14. tal endomorfismo es la identidad, esto es, sobre L es $h_j h_i^{-1}(x) = x$, y en particular, $a_i = h_j h_i^{-1}(a_i) = h_j(a) = a_j$, luego $i = j$. Sea ahora P' un orden sobre K, que

extiende el orden P de F. Consideremos L' una clausura real de (K, P'), L' es también una clausura real de (F, P), por lo tanto existe $h: L' \to L$, F-isomorfismo de cuerpos ordenados, luego $h(a) = a_j$ para algún $j = 1, \ldots$ $\ldots, r$ y entonces $h = h_j$ sobre K. Observamos que si $x \in P'$ es $h(x) > 0$ en L y luego $P' \subset P_j$, esto es $P' = P_j$.

b) Si K/F es de Galois, todas las raíces de $f(X)$ están en K y, por lo tanto, en la clausura L considerada.

3.3. ESPACIO DE ÓRDENES

Sean F un cuerpo formalmente real y $\dot{P}$ un cono de orden en F, es inmediato observar que $\dot{P} = P - \{0\}$ verifica $\dot{P} + \dot{P} \subseteq \dot{P}$, $\dot{P} \cdot \dot{P} \subseteq \dot{P}$, $\dot{P} \cup -\dot{P} = \dot{F}$ y $\dot{P} \cap -\dot{P} = \phi$, y recíprocamente, si $A \subseteq \dot{F}$ verifica $A + A \subseteq A$, $A \cdot A \subseteq A$ y $A \cup$ $\cup -A = \dot{F}$ y $A \cap -A = \phi$, entonces $A \cup \{0\}$ define un orden P' en F tal que $\dot{P}' = A$. Por este motivo, es equivalente considerar conos positivos, P, o "sus reducidos", $\dot{P}$. En la presente sección se conviene en considerar los conos reducidos y en consecuencia al referirnos a un cuerpo ordenado por el cono P, nos referimos al cono reducido (o sea, $0 \notin P$).

Denotemos por O_F la colección de todos los órdenes sobre F. Sea f una F-forma cuadrática. Definimos la "signatura total de f" como la aplicación $\hat{f}: O_F \to Z$ tal que $\hat{f}(P) = \mathrm{Sig}_P(f)$. También podemos definir $\sigma: f \to \hat{f}$, aplicación de WF en Z^{O_F} = anillo de las aplicaciones de O_F en Z, con las operaciones "coordenada a coordenada". En esta sección vamos a estudiar la conexión entre la signatura total de una forma cuadrática y su estructura, así como también las relaciones entre el espacio de órdenes y el anillo de Witt.

El primer paso en este estudio es dotar al espacio de órdenes O_F de una estructura topológica adecuada. Todo orden P define una aplicación, que denotamos también por P, $P: \dot{F} \to \{1, -1\}$, tal que $P(a) = 1$, si $a \in P$, y $P(a) = -1$, si $-a \in P$. Así, podemos sumergir O_F en el espacio $\{1, -1\}^{\dot{F}}$, provisto con la topología producto, donde $\{1, -1\}$ es considerado con la topología discreta. Luego O_F hereda la topología de $\{1, -1\}^{\dot{F}}$, que, por el teorema de Tychonoff, es un espacio topológico compacto. Los abiertos sub-básicos de $\{1, -1\}^{\dot{F}}$ son de la forma:

$$H_{a,t} = \{f: \dot{F} \to \{1, -1\} / f(a) = t;\ a \in \dot{F},\ t = \pm 1\}$$

Se observa que $H_{a,t}$ es abierto y cerrado desde que su complemento es $H_{a,-t}$; así, $\{1, -1\}^{\dot{F}}$ es totalmente disconexo.

Proposición 3.3.1. O_F, con la topología inducida por $\{1, -1\}^{\dot{F}}$, es compacto y totalmente disconexo.

Demostración. Es inmediato observar que la componente conexa de un $P \in O_F$ se reduce a $\{P\}$, pues si existiese $P' \neq P$ en la misma componente, entonces existe $a \in \dot{F}$ tal que $a \in P$ y $-a \in P'$, luego $P \in H_{a,1}$ y $P' \in H_{a,-1}$, lo que proporciona una disconexión de la componente conexa, lo que es absurdo. Para demostrar la compacidad de O_F basta mostrar que O_F es cerrado en $\{1, -1\}^{\dot{F}}$. Para ello se toma $f: \dot{F} \to \{1, -1\}$, pero tal que $f \in O_F$. Si $f(F) = 1$ se considera $H_{-1,1}$, y $f \in H_{-1,1}$, pero para todo

$P \in O_F$ $P \notin H_{-1,1}$, esto es $H_{-1,1}$ es una vecindad de f que no interseca a O_F. Si fuese $f(F) = -1$, se considera $H_{1,-1}$ y se concluye en forma análoga. Podemos por lo tanto suponer que f es suryectiva. Definimos en $\dot{F}$ elementos "positivos" si son aplicados por f en 1 y "negativos" si son aplicados en -1, pero, como $f \notin O_F$, entonces existirán $a, b \in \dot{F}$ "positivos" tales que $a + b$ o $a \cdot b$ no son "positivos". Si se denota por c cualquiera de estos dos elementos, consideremos el abierto básico $H_{a,1} \cap H_{b,1} \cap H_{c,-1}$. Vemos que él separa f de O_F. Por lo tanto, O_F es cerrado.

Los sub-básicos de O_F son de la forma $H_{a,1} \cap O_F = \{P \in O_F / a \in P\}$, con $a \in \dot{F}$, o $H_{a,-1} \cap O_F = \{P \in O_F / -a \in P\} = H_{-a,1} \cap O_F$, por lo que bastará considerar los sub-básicos de la forma $H_{a,1}$, $a \in \dot{F}$. Estos conjuntos se denotan por $H(a)$, $a \in \dot{F}$, y se llaman conjuntos de Harrison. Se llama $\{H(a)\}_{a \in \dot{F}}$ a la sub-base de Harrison de la topología de O_F.

Corolario 3.3.2. Si q es una forma F-cuadrática, entonces la "signatura total" $\hat{q}: O_F \to Z$ es continua.

Demostración. Como la suma de aplicaciones continuas es continua, basta considerar $q = \langle a \rangle$ y observar que:

$$\hat{q}^{-1}(t) = \{P \in O_F / \mathrm{Sig}_P(a) = t\} \text{ es } \emptyset, \text{ si } t \neq \pm 1;$$

$$H(a), \text{ si } t = 1 \text{ o } H(-a), \text{ si } t = -1.$$

Así, el homomorfismo de anillos c, definido por $c: q \to \hat{q}$, tiene su imagen en $C(O_F, Z)$ = anillo de las aplicaciones continuas de O_F en Z, donde se considera la topología discreta sobre Z.

Sea S un subconjunto de O_F, denotemos por h_S la función característica de S, esto es h_S es definida sobre O_F y tal que $h_S(P) = 1$, si $P \in S$, y $h_S(P) = 0$, si $P \notin S$. Es inmediato observar que $h_S \in C(O_F, Z)$, si S es un conjunto abierto y cerrado en O_F. Además, supongamos que $f \in C(O_F, Z)$, entonces $A_n = f^{-1}(n)$ es un abierto y cerrado en O_F, la familia de abiertos $\{A_n\}_{n \in Z}$ es un cubrimiento abierto de O_F y, por compacidad, existe un número finito de A_n's cuya unión es O_F, esto es $O_F = A_{n_1} \cup \ldots \cup A_{n_r}$, donde $f(A_{n_j}) = n_j$. Entonces tenemos que $f = \sum_{i=1}^{r} n_i h_{A_{n_i}}$ y, en consecuencia, la familia de aplicaciones $\{h_S\}$, cuando S recorre los conjuntos abiertos-cerrados de O_F genera aditivamente $C(O_F, Z)$.

Después de estas consideraciones generales nos concretaremos a establecer la correspondencia de Harrison-Lorenz-Leicht entre los ideales de WF y O_F.

Teorema 3.3.3. Sean F un cuerpo real y O_F su espacio de órdenes. Existe entonces una correspondencia biyectiva entre O_F y el conjunto de los ideales primos de WF que tienen característica cero.

Demostración. Consideremos un orden P sobre F y sea F_P una clausura real de (F, P). Es inmediato observar que $\mathrm{Sig}: WF_P \to Z$, aplicación

de signatura respecto al único orden de F_p, es un isomorfismo de anillos (véase el ejemplo 9, cap. 1). El núcleo de la aplicación:

$$WF \xrightarrow{r} WF_p \xrightarrow{\text{Sig}} Z$$

que denotaremos por φ_p es un ideal primo de WF de característica cero, desde que WF/φ_p es isomorfo a Z. Se tiene entonces una aplicación $P \to \varphi_p$. De otro lado, supongamos que φ es un ideal primo de WF cuya característica es cero, definimos:

$$P = \{a \in \dot{F} / \langle a, -1\rangle \in \varphi\}.$$

Observamos que:

a) Si $a \in \dot{F}$, entonces $\langle a\rangle = \langle 1\rangle$ o $\langle a\rangle = \langle -1\rangle$ mód φ, entonces $a \in P$ o $-a \in P$. Si $a, b \in P$, entonces $ab \in P$.

b) Sean $a, b \in P$, entonces como $\langle a, b\rangle = \langle a + b\rangle\ \langle 1, ab\rangle$ en WF, en WF/φ será $2\langle 1\rangle = 2\langle a + b\rangle$ y, como la característica de WF/φ es cero, entonces $\langle 1\rangle = \langle a + b\rangle$ en WF/φ, esto es, $a + b \in P$.

De lo observado en (a) y (b) tenemos que P es un orden en F y podemos considerar la aplicación $\varphi \to P$. Es fácil ver que estas aplicaciones son inversas y por consiguiente definen una biyección entre O_F y los ideales primos de WF de característica cero.

Observación: En la demostración del teorema, se puede ver a las claras que basta exigir que la característica de φ sea diferente de 2, para que P sea un orden.

Teorema 3.3.4. Sea F un cuerpo real, entonces los ideales primos de WF se clasifican de la siguiente forma:

a) Ideales primos de característica cero, los cuales son minimales.

b) IF, único ideal de característica 2.

c) Ideales primos de característica $\neq 2, 0$, los cuales son obtenidos como núcleo de la aplicación:

$$WF \xrightarrow{r} WF_p \approx Z \xrightarrow{h} Z_p,$$

donde F_p es la clausura real de (F, P), para P orden en F, $p \neq 2$ es un primo y h es la reducción módulo p. Estos ideales se denotan por $\varphi_{p,p}$.

Demostración. Por el teorema anterior, al ser F formalmente real, $O_F \neq \phi$ y existen entonces primos de característica cero en WF. Veamos que estos son minimales. Supongamos que φ_p sea ideal de característica cero, definido por el orden P de F, si φ es tal que $\varphi \subseteq \varphi_p$, φ primo; entonces si caract$(\varphi) = 2$, resulta $\varphi_p = IF$ ya que es el único primo de característica 2 (véase en la pág. 21, la observación después de la proposición 1.5.1.), entonces caract$(\varphi) \neq 2$ es 0 ó p. Si caract$(\varphi) = p$, entonces, suponiendo demostrado (c), es $\varphi = \varphi_{P',p}$, donde $P' \in O_F$, y como

$\mathcal{O}_{P'} \subseteq \mathcal{O}_{P'}$, $_{p} \subseteq \mathcal{O}_{P}$, obtenemos que $\mathcal{O}_{P'} \subseteq \mathcal{O}_{P}$, entonces $P' \subseteq P$ y por tanto $P' = P$, de donde $\mathcal{O} = \mathcal{O}_{P}$, esto es $\mathcal{O}_{P}$ es minimal.

b) Como se señaló ya, esto se demostró en el capítulo 1; por lo tanto, para completar la demostración queda por probar c). Observemos que los ideales $\mathcal{O}_{P,p}$ son maximales y de característica p, pues $WF/\mathcal{O}_{P,p}$ es isomorfo al cuerpo finito Z_p. Además, si considero $\mathcal{O}_{P}$, según ha sido definido en el teorema 3.3.3., tenemos $\mathcal{O}_{P} \subseteq \mathcal{O}_{P'}$, $_{p}$, y aún más, $\mathcal{O}_{P,p}$ es el único primo de característica p que contiene a $\mathcal{O}_{P}$, pues, si $\mathcal{O}$ fuese ideal primo tal que caract$(\mathcal{O}) = p$ y $\mathcal{O}_{P} \subseteq \mathcal{O}$, entonces el homomorfismo de cambio de clase $WF/\mathcal{O}_{P} \to WF/\mathcal{O}$, induce la reducción módulo p de Z en Z_p desde que $WF/\mathcal{O}_{P} \approx Z$ y $WF/\mathcal{O} \approx Z_p$. Luego, si $q \in \mathcal{O}_{P,p}$, es $\mathrm{Sig}_{P}(q) = mp$, esto es $q + \mathcal{O} = 0$ en $WF/\mathcal{O}$, de donde $\mathcal{O}_{P,p} \subseteq \mathcal{O}$.

Sea ahora $\mathcal{O}$ un ideal primo en WF, caract$(\mathcal{O}) = p \neq 2$, entonces según la observación hecha al finalizar el teorema 3.3.3., $P = \{a \in F / \langle a, -1\rangle \in \mathcal{O}\}$ es un orden sobre F. Se probará que $\mathcal{O}_{P} \subseteq \mathcal{O}$, con lo cual se concluye que $\mathcal{O} = \mathcal{O}_{P,p}$ de acuerdo con lo demostrado ya. Si $q \simeq \langle a_1, \ldots, a_n\rangle$ es una F-forma tal que $q \in \mathcal{O}_{P}$, entonces $\mathrm{Sig}_{P}(q) = 0$, de donde cabe suponer que $a_1, \ldots, a_r$ están en P y $-a_{r+1}, \ldots, -a_n \in P$ con $n = 2r$, es decir $\langle a_1, -1\rangle \in \mathcal{O}$ y $\langle -a_1, -1\rangle \in \mathcal{O}$, de donde $q \in \mathcal{O}$.

Corolario 3.3.5. Si F es un cuerpo no real, entonces WF es un anillo local con un único primo.

Demostración. Si existe un primo de característica $\neq 2$, éste define un orden sobre F.

Volvamos ahora a ocuparnos de la "signatura total" de una forma cuadrática. Más precisamente, vamos a demostrar que si $q \in WF$ es tal que $\hat{q} \equiv 0$ en $C(O_F, Z)$, entonces $q \in WF$ es un elemento de 2-torsión. Si F es un cuerpo no real se conviene en que $C(O_F, Z) = 0$.

Teorema 3.3.6. El núcleo de la aplicación $c: WF \to C(O_F, Z)$ tal que $c(q) = \hat{q}$ es de 2-torsión.

Demostración. Si F no es real, IF es el nilradical de WF por el corolario 3.3.5., luego existe un entero positivo r tal que $2^r\langle 1\rangle = 0$, de donde $2^r WF = 0$; en particular todo elemento de WF es de 2-torsión y $WF = WF_t$ = subgrupo de torsión del grupo aditivo WF. Luego el teorema se cumple si F no es formalmente real.

Supongamos que F es un cuerpo euclidiano. Entonces al existir un único orden sobre F, la signatura total es la signatura respecto del único orden de F y por lo tanto, c coincide con la aplicación de la signatura de WF en Z que es un isomorfismo de anillos. Luego el teorema es verdadero si F es euclidiano.

Procedemos ahora en el caso general. Sea $q \in WF$ y supongamos que q no es de 2-torsión. Veremos entonces que se puede construir un orden P sobre F tal que $\mathrm{Sig}_{P}(q) \neq 0$. Por la aplicación del Lema de Zorn, po-

demos encontrar un cuerpo K, tal que $F \subseteq K$, dentro de una clausura algebraica de F, tal que K es maximal respecto de la siguiente propiedad: "q_K no es de 2-torsión sobre K".

K resulta formalmente real por la primera parte de la demostración. Probaremos que K es euclidiano; en caso contrario, existe una clase módulo cuadrados $\neq \pm 1$. Sea a un representante de tal clase, esto es $a \notin \dot{K}^2$ y $-a \notin \dot{K}^2$, luego $K(\sqrt{a})$ y $K(\sqrt{-a})$ son extensiones de grado 2 de K. Denotemos por L cualquiera de estas dos extensiones; entonces q_L es de 2-torsión; existe luego un n, entero positivo, tal que $2^n q$ es hiperbólica sobre L, luego por el corolario 2.4.2. $\pm a$ es un factor de similaridad de $2^n q_K$, esto es $\pm a \in G_K(2^n q_K)$, y como $G_K(2^n q_K)$ es un grupo, se tiene entonces que $-1 \in G_K(2^n q_K)$. Ahora bien, por el ejercicio 22-e, cap. 1, tenemos que $2(2^n q_K) = 0$, lo que implica $2^{n+1} q_K = 0$, que es contrario a la elección de K. Por lo tanto debe ser K euclidiano. Si P' es su único orden, es $\mathrm{Sig}_P(q) \neq 0$, donde se denota por P el orden inducido por P' sobre F, con lo que queda demostrado el teorema.

Observación: Como $C(O_F, Z)$ es sin torsión, entonces WF_t está contenido en el núcleo de c, pero el teorema anterior establece la inclusión contraria, esto es $\mathrm{Nú}(c) = WF_t$. Esto se expresa en el llamado "Principio Local-Global de Pfister", como sigue:

Teorema 3.3.6'. Si F es formalmente real, la siguiente sucesión es exacta:

$$0 \rightarrowtail WF_t \rightarrow WF \xrightarrow{c} C(O_F, Z)$$

El siguiente teorema establece que el conúcleo de c es también de 2-torsión.

Teorema 3.3.7. Si F es un cuerpo formalmente real, entonces el conúcleo de $c: WF \rightarrow C(O_F, Z)$ es de 2-torsión.

Demostración. En la pág. 54 se observa que la familia $\{h_S\}$, cuando S recorre los conjuntos abiertos-cerrados de O_F, genera aditivamente $C(O_F, Z)$, donde h_S es la función característica de S. Luego $f \in C(O_F, Z)$ puede escribirse $f = \Sigma n_S h_S$ (nótese que la suma es finita), por lo tanto para demostrar que $f + \mathrm{Im}(c) \in$ conúcleo de $c = C(O_F, Z)/\mathrm{Im}(c)$ es de 2-torsión será suficiente demostrar que si C es un conjunto abierto-cerrado en O_F, existe un entero $n \geq 0$, tal que $2^n h_C \in \mathrm{Im}(c)$. Pero C, al ser cerrado, es compacto, luego puede expresarse como una unión finita de abiertos básicos $H(a_1) \cap H(a_2) \cap \ldots \cap H(a_n)$, y como las funciones características tienen la siguiente propiedad $h_{C_1 \cup C_2} = h_{C_1} + h_{C_2} - h_{C_1} \cdot h_{C_2}$, entonces basta verificar el teorema para un conjunto abierto-cerrado básico. Denotemos $H(a_1) \cap \ldots \cap H(a_n) = H(a_1, \ldots, a_n)$; este conjunto permite definir una n-forma de Pfister $\langle\langle a_1, \ldots, a_n \rangle\rangle$, luego $2^n h_{H(a_1, \ldots, a_n)} =$

$= 2^n h_{H(a_1) \cap \ldots \cap H(a_n)} = 2^n h_{H(a_1)} \ldots h_{H(a_n)} = \widehat{\langle\langle a_1 \rangle\rangle \ldots \langle\langle a_n \rangle\rangle} = \langle\langle a_1, \ldots, a_n \rangle\rangle \in$
$\in \mathrm{Im}(c)$. Por lo tanto, $2^n h_{H(a_1, \ldots, a_n)} = 0$, en $C(O_F, Z)/\mathrm{Im}(c)$.

En el capítulo 2 se ha definido cuándo un cuerpo es pitagórico. Estos cuerpos son particularmente importantes en el estudio de las

formas cuadráticas sobre cuerpos principalmente cuando además de pitagóricos son reales. En lo que sigue se hará la demostración de un teorema que permite advertir tal importancia. Concretamente, se caracterizan totalmente estos cuerpos por la condición de que el subgrupo de torsión de WF_t es cero.

Teorema 3.3.8. F es un cuerpo pitagórico y formalmente real si, y sólo si, $WF_t = 0$.

Demostración. Se probará suponiendo que F es real y pitagórico que, si q es F-forma anisótropa, entonces mq es anisótropa $\forall\ m > 0$, entero. Sea $q = \langle a_1, \ldots, a_n \rangle$, $a_i \in \dot{F}$. Si mq fuese isótropa sobre F, existirán $x_1, \ldots, x_n$, en F tales que $a_1x_1 + \ldots + a_nx_n = 0$, donde cada x_j es una suma de m cuadrados, y al ser F real, algún $x_j \neq 0$. Pero como F es pitagórico, cada $x_j = y_j^2$, entonces se obtiene $a_1y_1^2 + \ldots + a_ny_n^2 = 0$, con algún $y_j \neq 0$ en F, lo que contradice nuestra suposición de que q es anisótropa. Recíprocamente, supongamos que $WF_t = 0$, en particular no existe 2-torsión. Si $u, v \in \dot{F}$, sea $a = u^2 + v^2$. Como $\langle 1, 1 \rangle \simeq \langle a, a \rangle$, se tiene $2\langle 1 \rangle = 2\langle a \rangle$, lo que implica $\langle 1 \rangle \simeq \langle a \rangle$, esto es a es un cuadrado en $\dot{F}$, luego F es pitagórico. Si fuese no real, entonces F será cuadráticamente cerrado en virtud del lema 2.5.1. y $WF \approx Z_2$, lo que es una contradicción; por lo tanto, F debe ser formalmente real.

Un aspecto fundamental en la teoría de formas cuadráticas sobre cuerpos es clasificarlas mediante invariantes para las clases de equivalencia fijados de antemano; esto es, suponiendo conocido un conjunto de invariantes (como, por ejemplo, dimensión, determinante, "signatura total", etc.), poder decidir si dos formas cuadráticas dadas son equivalentes. Por ejemplo: Sea F pitagórico real y considérense los invariantes "dimensión" y "signatura total". Si q_1 y q_2 son F-formas de la misma dimensión y con $\hat{q}_1 = \hat{q}_2$, entonces $q_1 - q_2$ en WF es un elemento de torsión por el principio local-global de Pfister, pero, por el teorema 3.3.8., $q_1 = q_2$ en WF. Entonces, al tener la misma dimensión, se tiene que $q_1 \simeq q_2$. El hecho que la "dimensión" y la "signatura total" clasifiquen las formas cuadráticas sobre un cuerpo pitagórico real se conoce como la "Ley de Sylvester-Pfister".

Se continúa ahora examinando el espacio de órdenes O_F de un cuerpo formalmente real y algunas propiedades más sobre la extensión de órdenes.

Teorema 3.3.9. Sea K/F una extensión arbitraria de cuerpos, donde F es formalmente real. Si $w \in O_F$, se denota por P_w el correspondiente ideal primo minimal de WF, esto es $P_w = \{q \in WF / \mathrm{Sig}_w(q) = 0\}$. Las proposiciones siguientes son equivalentes:

1) w se extiende a K.

2) Toda F-forma q que es isótropa sobre K es indefinida respecto de w.

3) Toda F-forma q que es hiperbólica sobre K es tal que $\mathrm{Sig}_w(q) = 0$, esto es $W(K/F) \subseteq P_w$.

4) Si q es una forma de Pfister sobre F, que es hiperbólica sobre K, entonces $\mathrm{Sig}_w(q) = 0$.

Demostración. (1) → (2). Sea $q = \langle a_1, \ldots, a_n \rangle$, una F-forma tal que q_K es isótropa, entonces existen $x_1, \ldots, x_n \in K$, no todos nulos, tales que $a_1x_1^2 + \ldots + a_nx_n^2 = 0$, pero, por hipótesis, K es formalmente real, entonces no todos los a_i pueden ser positivos respecto a w en K, luego q es indefinida respecto a w.

(2) → (1) es inmediata de la proposición 3.2.2.

(1) → (3). Si q es F-forma tal que $q_K \simeq mH$, luego, como w se extiende a un orden w' sobre K, tenemos: $\mathrm{Sig}_w(q) = \mathrm{Sig}_{w'}(q_K) = \mathrm{Sig}_{w'}(mH) = 0$, luego $q \in P_w$, y por lo tanto, $W(K/F) \subseteq P_w$.

(3) → (4) es inmediata.

(4) → (2). Sea $q = \langle a_1, \ldots, a_n \rangle$, F-forma que es isótropa sobre K; por consiguiente lo es también la F-forma $\langle 1, a_1a_2, \ldots, a_1a_n \rangle$ que es subforma de la forma de Pfister $\ll a_1a_2, \ldots, a_1a_n \gg$, luego $\ll a_1a_2, \ldots, a_1a_n \gg$ es hiperbólica sobre K y por lo tanto $\mathrm{Sig}_w(\ll a_1a_2, \ldots, a_1a_n \gg) = 0$, de donde existe i tal que $a_1a_i \notin w$, luego q es indefinida sobre F respecto de w.

Corolario 3.3.10. Sea K/F una extensión arbitraria de F formalmente real, entonces todo orden de F se extiende a K si, y sólo si, $W(K/F)$ es un nilideal de WF.

Demostración. Para todo $w \in O_F$ es $W(K/F) \subseteq P_w$, luego $W(K/F) \subseteq \bigcap_{w \in O_F} P_w$ nilradical de WF por el teorema 3.3.4.

Observamos lo siguiente: Sea q una F-forma en WF. Es $\hat{q} \equiv 0$ si, y sólo si, $\hat{q}(w) = \mathrm{Sig}_w(q) = 0$, $\forall\, w \in O_F$, si, y sólo si, $q \in \bigcap_{w \in O_F} P_w = \mathrm{nilrad}(WF)$. Pero, por el principio local-global de Pfister, $\hat{q} \equiv 0$ si, y sólo si, $q \in WF_t$. En consecuencia, para un cuerpo real F, es $WF_t = \mathrm{nilrad}(WF)$.

Corolario 3.3.11. Sean F un cuerpo pitagórico real y K/F una extensión de cuerpos. Entonces todo orden de F se extiende a K si, y sólo si, $W(K/F) = 0$.

Demostración. Al ser F pitagórico real por 3.3.8 resulta $WF_t = 0$ y recíprocamente. Todo orden se extiende a K si, y sólo si, $W(K/F) \subseteq \mathrm{nilrad}(WF) = WF_t = 0$.

El teorema de Springer (Teorema 2.3.1.) establece que si la dimensión de una extensión K/F es impar, entonces las formas anisótropas sobre F se preservan a K, en particular $W(K/F) = 0$. A continuación se demostrará un caso particular de recíproco del teorema de Springer, el cual se debe a Roger Ware.[15] Este resultado establece que si L/F es una extensión de Galois de grado n, donde L es pitagórico, tal que $W(L/F) = 0$, entonces n es impar. (Véase el ejercicio 26 correspondiente a este capítulo.) Para ello se demostrará antes el lema siguiente:

Lema 3.3.12. Sean E un cuerpo pitagórico y F un subcuerpo de E tal que $[E:F]$ es finito, entonces F es también pitagórico.

Demostración. Por inducción sobre $[E:F] = n$. Si $n = 1$, no hay qué demostrar. Supongamos $n > 1$. Si F no es pitagórico, existe $x \in \dot{F}$ tal

que $K = F(\sqrt{w})$, $w = 1 + x^2$ es una extensión de grado 2 y por la hipótesis inductiva K es pitagórico. Como: $2(w + \sqrt{w}) = (w + 2\sqrt{w} + 1) + (w - 1) = (\sqrt{w} + 1)^2 + x^2 = u^2 \in \dot{K}^2$ y $2 = 1 + 1$ es un cuadrado en K, resulta que $w + \sqrt{w} \in \dot{K}^2$, y tomando norma N en la extensión cuadrática K/F se tiene:

$$N(w + \sqrt{w}) = (w + \sqrt{w})(w - \sqrt{w}) = w(w - 1) = wx^2,$$

luego wx^2 es un cuadrado en F y, por lo tanto, también w, lo que es contrario a nuestra suposición sobre w. Esta contradicción demuestra el lema.

Proposición 3.3.13. Sea L/F una extensión de Galois de grado finito, con L pitagórico. Si $W(L/F) = 0$, entonces el grado de la extensión L/F es impar.

Demostración. Si $G = G(L/F)$ tiene orden par, se considera un 2-subgrupo de Sylow H del grupo G, no trivial. Luego $o(H) = 2^e$, y si se denota por $K = L^H$ (subcuerpo de L formado por los H-invariantes) y se aplica la correspondencia de Galois, se obtiene que existe una extensión cuadrática de K en L. Si F es un cuerpo no real, K es no real y por el lema también es pitagórico, entonces por el lema 2.5.1. K es cuadráticamente cerrado, por lo tanto K no tiene extensiones cuadráticas, lo que es una contradicción. Luego, si F es no real, $G(L/F)$ tiene orden impar. Supongamos que F es formalmente real, por el lema anterior F es pitagórico, y por el corolario 3.3.11. todo orden de F se extiende a L. Si w es un orden sobre F, por la proposición 3.2.15., w tiene exactamente $[L:F]$ extensiones diferentes a L y r extensiones a K, donde $r \leq [K:F]$. Consideremos $w_1, \ldots, w_s$ todas las extensiones de w a K que se extienden a L ($s \leq r$), cada w_j tiene exactamente $[L:K]$ diferentes extensiones a L por ser L/K de Galois, en consecuencia $[L:F] = s[L:K]$ y entonces $s = [K:F]$, esto es $r = s$, lo que significa que toda extensión de w a K se extiende a L. Pero, todo orden sobre K es una extensión de algún orden en F, por lo tanto, todo orden de K se extiende a L y por el corolario 3.3.11. es $W(L/K) = 0$. Sea K'/K de grado 2 dentro de L, luego $K' = K(\sqrt{a})$. Observamos que $\langle 1, -a \rangle$ es anisótropa sobre K y por la inyectividad es $\langle 1, -a \rangle_K$ diferente de cero en WL. Pero esto es absurdo, pues $\langle 1, -a \rangle_K$ es un plano hiperbólico en L. Luego $o(G)$ debe ser impar.

Consideremos A un anillo conmutativo con unidad. Se denomina "espectro de A" al conjunto de los ideales primos de A, provisto de la topología de Zariski (llamada también topología espectral), esto es la topología sobre el conjunto de ideales primos de A, para la cual los cerrados son los conjuntos de la forma $V(M)$, $M \subseteq A$, definidos por $V(M) = \{J \text{ ideal primo} / J \supseteq M\}$. Es fácil demostrar que la colección de estos conjuntos, cuando M recorre el conjunto de partes de A, cumple los axiomas de "cerrados" de una topología (véase (7), ejemplo 1.7, pág. 103). Se denota por $\mathrm{Spec}(A)$ el conjunto de ideales primos de A provisto de la topología de Zariski. Si se identifica O_F, espacio de órdenes de F, con el subconjunto de $\mathrm{Spec}(WF)$, formado por los primos minimales de WF, se puede considerar la topología inducida por la topología de Zariski sobre O_F. Entonces los cerrados de O_F en esta topología serán de la forma:

$$V(U) = \{P_w / P_w \supseteq U,\ w \in O_F\} = \{w \in O_F / \mathrm{Sig}_w(q) = 0\ \forall\ q \in U\},$$

donde U es ideal de WF.

Recordemos que sobre O_F se ha definido también la topología de Harrison, cuyos abiertos sub-básicos son de la forma $H(a) = \{\omega \in O_F / a \in \omega\}$. Observamos inmediatamente que $H(a) = V(\langle 1, -a \rangle)$, $\forall\, a \in \dot{F}$, luego $H(a)$ es abierto en la topología espectral sobre O_F y por lo tanto todo abierto en la topología de Harrison lo es en la espectral. Supongamos que O es abierto en la topología espectral, luego $O = O_F - V(U)$ para algún ideal U de WF. Sea $\omega_0 \in O$, entonces existe una F-forma $q \in U$ tal que $\mathrm{Sig}_{\omega_0}(q) \neq 0$. Escribamos $q = \langle a_1, \ldots, a_n \rangle$. Podemos suponer que $a_1, \ldots, a_r \in \omega_0$, con $n/2 < r \leq n$, y considerar el abierto básico $H(a_1, \ldots, a_r, -a_{r+1}, \ldots, -a_n) = H$. Entonces, si $\omega \in H$, es $\mathrm{Sig}_\omega(q) \neq 0$, y entonces $\omega \in O$. Luego $\omega_0 \in H(a_1, \ldots, a_r, a_{r+1}, \ldots, a_n) \subset O$, esto es O es abierto en la topología de Harrison. Se ha demostrado así que la topología de Harrison coincide con la inducida por la topología espectral.

Proposición 3.3.14. La topología de Harrison sobre O_F es la topología inducida por la topología de $\mathrm{Spec}(WF)$ sobre O_F.

EJERCICIOS

1. Sea F un cuerpo. Demostrar que:

a) Si $o(\dot{F}/\dot{F}^2)$ es finito, es una potencia de 2.

b) Si $o(\dot{F}/\dot{F}^2)$ es finito, entonces F posee a lo más 2^{n-1} órdenes, donde $o(\dot{F}/\dot{F}^2) = 2^n$.

c) Se cumplen las desigualdades $m \leq \mathrm{card}(O_F) \leq 2^{n-1}$, donde $(\dot{F} : S) = 2^n$ $S = \Sigma F^2 - \{0\}$. (Sug: véase el ejercicio 7.) Construir ejemplos que realicen las igualdades.

2. En la clausura algebraica de un cuerpo dado, demostrar que la intersección de cualquier familia de cuerpos pitagóricos es un cuerpo pitagórico. Se define: Dados un cuerpo F y F' una clausura algebraica de F, se llamará "cápsula pitagórica de F' al cuerpo intersección de todos los subcuerpos pitagóricos de F' que contienen a F y se denotará por F_{pit}.

3. Sea F un cuerpo. Demostrar que:

a) Si F no es pitagórico, entonces F_{pit}/F es una extensión de grado infinito.

b) F_{pit}/F es una extensión normal.

4. Si Q denota el cuerpo racional, demostrar que $\dot{Q}_{\mathrm{pit}}/\dot{Q}^2_{\mathrm{pit}}$ tiene orden infinito. (Sug.: usar el teorema enunciado en el capítulo 2, ejercicio 19.)

5. Sea F un cuerpo formalmente real. Para $a, b \in \dot{F}$, demostrar que $H(-ab) = H(-a) \,\Delta\, H(-b)$. Deducir de ello que los conjuntos de Harrison, con la diferencia simétrica, forman un subgrupo del grupo de partes de O_F con la diferencia simétrica.

6. Demostrar que la correspondencia entre $\dot{F}/S$, donde $S = (\Sigma F^2) - \{0\}$ subgrupo multiplicativo de $\dot{F}$ (véase proposición 3.1.3.), y el grupo de los conjuntos de Harrison con "Δ", que asocia; $aS \to H(-a)$, es un isomorfismo de grupos.

7. Para F formalmente real demostrar que F es pitagórico con infinitas clases módulo cuadrados si, y sólo si, F es pitagórico con infinitos órdenes. (Sug.: aplicar el ejercicio 6.)

8. Si K/F es una extensión de grado finito y K es euclidiano, demostrar que F es euclidiano. (Sug.: demostrar primero que $[K:F]$ es impar. Para ello tomar a tal que $K = F(a)$ y sea $f(X)$ su F-polinomio minimal. Ver que en una clausura real K' de K, $f(X)$ se factoriza con un solo factor lineal y el resto cuadráticos. Usando que $[K:F]$ es impar, deducir que $o(\dot{F}/\dot{F}^2) \leq o(\dot{K}/\dot{K}^2) = 2$. Observar que puede afirmarse de inmediato que F es pitagórico, pero no euclidiano.

9. Sea F un cuerpo tal que -1 no es un cuadrado, entonces demostrar que F es pitagórico si, y sólo si, F no tiene extensiones cíclicas de grado 4.

10. Sea F' una clausura algebraica de F. Una extensión K/F se llama "admisible" si existe una "torre" de cuerpos $F = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n = K$ tal que $K_{i+1} = K_i(\sqrt{1 + a_i^2})$, donde $a_i \in K_i$. Demostrar que la composición de todas las extensiones admisibles de F en F' es la cápsula pitagórica de F.

11. Considerar el conjunto de "series de Laurent" sobre F, esto es series formales de la forma $\sum_{n=k}^{\infty} a_n t^n$, m, $k \in Z$, y t una letra. Demostrar que, con las operaciones de suma y multiplicación ordinarias para series, este conjunto es un cuerpo que denotaremos por $F((t))$; repitiendo el proceso se puede considerar $F((t_1))((t_2)) \ldots ((t_n))$.

12. Dado un cuerpo F, demostrar que:

a) Si F es formalmente real, todo orden de F se extiende de dos únicas formas a $F((t))$, una en la que t es positivo y la otra en la que es negativo.

b) F es pitagórico real si, y sólo si, $F((t))$ es pitagórico real.

c) Si F es cerrado-real, $F((t_1)) \ldots ((t_n))$ tiene 2^{n+1} clases módulo cuadrados y 2^n órdenes.

13. Si K/F es una extensión de cuerpos con K pitagórico, demostrar que la clausura algebraica de F en K es también pitagórica.

14. Si F es formalmente real y pitagórico, demostrar que una F-forma cuadrática es universal si, y sólo si, es isótropa. (Sug.: la hipótesis de universal es excesiva, basta considerar que f, una F-forma representa u y $-u \in \dot{F}$. Luego se puede escribir $f = \langle u, a_2, \ldots, a_n \rangle$ y, en-

tonces, $\langle u, u, a_2, \ldots, a_n\rangle$ es isótropa. A partir de esto, deducir que f no puede ser anisótropa.)

15. Son equivalentes los siguientes enunciados para F cuerpo formalmente real.

a) Si a y b representan diferentes clases módulo cuadrados en $\dot{F}$, entonces existe $w \in O_F$ tal que $-ab \in w$.

b) Si $q = \ll a, b\gg$ con $a \neq b$ en $\dot{F}/\dot{F}^2$, entonces $\hat{q}$ tiene un cero en O_F (es decir, existe $w \in O_F$ tal que $\hat{q}(w) = 0$).

c) Cualquier n-forma de Pfister, no isométrica a $2_n\langle 1\rangle$, tiene un cero en O_F.

d) Si $a \neq -1$ en $\dot{F}/\dot{F}^2$, entonces existe un $w \in O_F$ tal que $a \in w$.

e) F es pitagórico.

16. Sean F pitagórico real (bastará suponer que I^nF es sin torsión) y f y g n-formas de Pfister sobre F. Demostrar que son equivalentes los siguientes enunciados:

a) $f \simeq g$. b) $D_F(f') = D_F(g')$. c) $D_F(f) = D_F(g)$.

(Sug.: $b) \rightarrow a)$ probar que $\hat{f} = \hat{g}$ y aplicar el principio local-global de Pfister.)

17. Supongamos que F es pitagórico real, demostrar que:

a) Si f y g son F-formas binarias, entonces $f \simeq g$ si, y sólo si, $D_F(f) = D_F(g)$.

b) Si f y g son formas ternarias sobre F, entonces $f \simeq g$ si, y sólo si, $D_F(f) = D_F(g)$ y $d(f') = d(g)$.

(Sug.: aplicar el ejercicio 16.)

18. Sea F un cuerpo real. Demostrar que los siguientes enunciados son equivalentes:

1) Para todo C subgrupo finito de $\dot{F}/\dot{F}^2$ tal que $-1 \notin C$, existe $w \in O_F$ tal que $C \subseteq w$.

2) Para cualquier subgrupo C de $\dot{F}/\dot{F}^2$ tal que $-1 \notin C$, existe un $w \in O_F$ tal que $C \subseteq w$.

3) Para cualquier Z_2-base de F/F^2, $\{-1, u_t/t \in T\}$, siendo T un conjunto de índices, si T_1, $T_2 \subseteq T$, $T_1 \cap T_2 = \phi$, entonces existe $w \in O_F$ tal que $u_{t_1} \in w$, $\forall\, t_1 \in T_1$ y $-u_{t_2} \in w$, $\forall\, t_2 \in T_2$.

4) Para cualquier Z_2-base de $\dot{F}/\dot{F}^2$, $\{-1, x_t/t \in I\}$, si $i_1, \ldots, i_m$, $i_{m+1}, \ldots, i_n$ son índices distintos en I, entonces existe $w \in O_F$ tal que $x_{i_1}, \ldots, x_{i_m} \in w$ y $x_{i_{m+1}}, \ldots, x_{i_n} \in -w$.

5) Existe una Z_2-base de $\dot{F}/\dot{F}^2$, $\{-1, y_j/j \in J\}$, que verifica el enunciado 4). Sug. : 1) → 2). Tomar una familia de clases módulo cuadrados $\{w_j\}$ $j \in J$ que genera a C sobre Z_2, como Z_2-espacio vectorial. Si $w_{j_1}, \ldots, w_{j_n}$ es una subfamilia, observar que 1) implica que existe un $w \in O_F$ tal que $w \in H(w_{j_1}, \ldots, w_{j_n})$, deducir de aquí que por la compacidad de O_F existe un $v \in O_F$ y $v \in \bigcup_{j \in J} H(-w_j)$, luego v es tal que $C \subseteq v$.

2) → 3). Considerar $\{-1, u_{t_1}/t_1 \in T_1\} \cup \{u_{t_2}/t_2 \in T_2\}$. Observar que el subespacio generado por $\{u_{t_1}, -u_{t_2}\}$ no contiene a "-1" y aplicar 2).

3) → 4) → 5) son inmediatas.

5) → 1). - Supongamos que existe una base $\{-1, y_j\}$ $j \in J$ que verifica 4); si C es un subgrupo finito de $\dot{F}/\dot{F}^2$, $-1 \notin C$, existen $y_1, \ldots, y_n$ tales que C está contenido en el subespacio generado por $\{-1, y_1, \ldots, y_n\}$, que se denota por S.

Considerar C_1 de codimensión 1 en S tal que $C_1 \supseteq C$ y $-1 \notin C_1$ y observar que y_j o $-y_j$ pertenecen a C_1, $1 \leq j \leq n$; considerar luego $y_1, \ldots, y_r \in C_1$ y $y_{r+1}, \ldots, y_n \notin C_1$ (reescribiendo convenientemente los índices). El conjunto $\{y_1, \ldots, y_r, -y_{r+1}, \ldots, -y_n\}$ es Z_2-linealmente independiente y genera C_1. Aplicar 5).

19. Si F es un cuerpo formalmente real que satisface cualesquiera de los cinco enunciados anteriores (ejercicio 19), se dice que F es un cuerpo *superpitagórico*. Estos cuerpos aparecen por vez primera en "Zur Galoistheorie pythagoreischer Körper" *Arch. der Math.*, 16, 1965, de J. Diller y A. Dress, y posteriormente en 1972, fueron redescubiertos por Elman y Lam,[1] quienes los han caracterizado en la forma en que se presentan en esta monografía. En los últimos años estos cuerpos han sido objeto de profundo estudio por su conexión con la teoría algebraica de formas cuadráticas.

Demostrar para un cuerpo F, real, que:

a) Todo superpitagórico es pitagórico.

b) Todo euclidiano es superpitagórico. Entonces tenemos numerosos ejemplos de superpitagóricos, como toda clausura real, y en particular, el cuerpo de los números reales R.

20. Si F es pitagórico real con 2^n clases módulo cuadrados, demostrar que F es superpitagórico si, y sólo si, F tiene 2^{n+1} órdenes.

21. Si F es cerrado-real, demostrar que $F((t_1)) \ldots ((t_n))$ es superpitagórico. (Sug. : usar el ejercicio 20.)

22. Si F es superpitagórico, demostrar que $F((t_1)) \ldots ((t_n))$ es superpitagórico. (Sug. : observar que si $\{-1, y_j, t/j \in J\}$ es una Z_2-base de $\dot{F}/\dot{F}^2$, entonces $\{-1, y_j, t/j \in J\}$ es una Z_2-base para $F((t))/F((t))^2$.

23. Si F es pitagórico real con a lo más cuatro clases módulo cuadrados, demostrar que F es superpitagórico y $I^2F = 2IF$.

24. Demostrar que sobre un cuerpo F el enunciado "WF es tal que $I^3F = 2I^2F$" es equivalente con los enunciados del ejercicio 7, cap. 1.

25. Supongamos que F es pitagórico real, f una n-forma de Pfister y g una m-forma de Pfister con $n \geq m$ sobre F. Supongamos que $f \neq 2^{n-m}g$, demostrar que existe un $w \in \dot{O}_F$ tal que w es un cero de $\hat{f}$ o de $\hat{g}$ en $\dot{O}_F$, pero no de los dos simultáneamente. (Sug.: suponer que $\forall\, w \in \dot{O}_F$ fuese $\hat{f}(w) \neq 0 \rightarrow \hat{g}(w) \neq 0$, implicación verdadera, así como que $\hat{f}(w) = 0 \rightarrow \hat{g}(w) = 0$, demostrar que entonces $\hat{f}$ y $2^{n-m}\hat{g}$ coinciden en $\dot{O}_F$, aplicar luego el principio local-global de Pfister y que f es pitagórico real.)

26. El siguiente ejemplo demuestra que en la proposición 3.3.13., la hipótesis de pitagórico exigida a L es necesaria.

(Knebusch-Ware) Una extensión L/F de Galois de cuerpos formalmente reales con F pitagórico $W(L/F) = 0$ y de dimensión par: Considerar un cuerpo K formalmente real sobre el cual actúa el grupo alternado A_n, $n \geq 5$, como grupo de automorfismos; por ejemplo, se puede tomar $K = R(X_1, \ldots, X_n)$ (justificar porqué es formalmente real). Sea $E = K^{A_n}$ y considerar la clausura cuadrática de E, que se denota por E_c. E_c se obtiene de la composición de todas las extensiones de Galois de E cuyo grado es una potencia de 2. Observar que:

a) E_c/E es una extensión de Galois.

b) K no es un subcuerpo de E_c y $E_c \cap K$ es una extensión de Galois de E, de lo que se obtiene $E_c \cap K = E$.

c) Considerar K_w es una clausura real de (K, w), donde $w \in \dot{O}_K$, y sea $F = K_w \cap E_c$. Ver que $F \cap K = E$ y que F es euclidiano, y luego pitagórico con un solo orden.

d) Sea $L = FK$ (composición de F y K en K_w), entonces L es formalmente real y L/F es de Galois con grupo A_n, de dimensión par.

e) Usar que $WF \approx Z$ para establecer que $W(L/F) = 0$.

27. Un orden P sobre un cuerpo F se dice arquimediano si para todo $a \in F$ existe un n (suma de n veces el 1 de F) tal que $n - a \in P$. En caso contrario, se dice que es no-arquimediano.

a) Sean F un cuerpo ordenado y P un cono positivo. Se define en $F[X]$: $a_0 + a_1X + \ldots + a_nX^n \in P_1$ si, y sólo si, $a_n \in P$. Entonces, en $F(X)$ existe un orden, definido por $w \in F(X)$ y $w = f/g$ es positivo si, y sólo si, $f \cdot g \in P_1$, $f, g \in F[X]$. Demostrar que el orden definido en $F(X)$ es *no arquimediano* y extiende el orden P.

29. Probar que un cuerpo ordenado por un orden arquimediano es isomorfo (isomorfismo preservando el orden) a un subcuerpo del cuerpo R de los números reales.

4

FORMAS CUADRÁTICAS SOBRE EXTENSIONES TRASCENDENTES Y CUERPO DE FUNCIONES DE UNA FORMA CUÁDRATICA

4.1. TEOREMAS DE CASSELS-PFISTER

Si K/F es una extensión algebraica, se ha visto en los capítulos 2 y 3 que el estudio del núcleo $W(K/F)$ de la aplicación canónica $WF \to WK$ es interesante, en particular con relación a la propiedad de preservación de formas anisótropas sobre F a la extensión K y al problema de extender los órdenes de F a K. Bajo este punto de vista, el caso en que K/F es trascendente pura carece de interés pues, como se sabe: $W(K/F) = 0$, las formas anisótropas sobre F se preservan a K y todo orden sobre F puede ser extendido a K. Sin embargo, las extensiones trascendentes puras tienen interés desde otros puntos de vista, principalmente con relación al problema de determinar los elementos representados sobre el cuerpo de base por una forma cuadrática sobre él. La solución de este problema se facilita cuando se dispone de la información correspondiente en el caso de ciertas extensiones trascendentes puras. La información básica pertinente está dada por los llamados teoremas de representación de Cassels-Pfister, a cuya exposición se dedica esta sección.

Teorema 4.1.1. Sea f una F-forma cuadrática, supongamos que f representa sobre $F(X)$ un polinomio $p(X)$ no nulo, entonces f representa a $p(X)$ sobre el anillo $F[X]$.

Demostración. Sea $f = \langle a_1, \ldots, a_n \rangle$, si f es isótropa sobre F, entonces $f = \langle 1, -1 \rangle \perp f_0$ y como $p(X) = (\frac{p(X)+1}{2})^2 - (\frac{p(X)-1}{2})^2$, tenemos que f representa a $p(X)$ sobre $F[X]$. Supongamos, por lo tanto, que f es anisótropa sobre F. Como $p(X)$ es representado por f sobre $F(X)$ se puede encontrar

$$a_1(\frac{f_1(X)}{f_0(X)})^2 + \ldots + a_n(\frac{f_n(X)}{f_0(X)})^2 = p(X) \qquad (*)$$

donde $f_0, f_1, \ldots, f_n \in F[X]$, $f_0(X) \neq 0$ y f_0 es elegido con el menor grado para una representación como (*) de $p(X)$. El teorema queda demostrado si se demuestra que $\mathrm{gr}(f_0) = 0$. Supongamos que es grado de $f_0 > 0$. Se considera sobre $F(X)$ la forma cuadrática $q = \langle -p(X), a_1, \ldots, a_n \rangle$ de dimensión $n+1$; a q podemos asociar el espacio cuadrático (K^{n+1}, B_q), donde $K = F(X)$ y $B_q(e_i, e_j) = 0$, si $i \neq j$; $B_q(e_0, e_0) = -p(X)$, $B_q(e_i, e_i) = a_i$. Consideremos $I \subseteq K^{n+1}$ el conjunto de vectores isótropos de (K^{n+1}, B_q), inmediatamente observamos que $w = (f_0, f_1, \ldots, f_n) \in I$, por (*). Por la división euclidiana, cada f_i puede escribirse $f_i(X) = f_0(X)g_i(X) + r_i(X)$, con $0 \leq \mathrm{gr}(r_i) < \mathrm{gr}(f_0)$ para $i = 1, \ldots, n$. Para $i = 0$, se define $g_0(X) = 1$ y $r_0(X) = 0$ y como $\mathrm{gr}(0) = -\infty$ se obtiene que $\mathrm{gr}(r_i) < \mathrm{gr}(f_0)$ para $i =$

$= 0, 1, \ldots, n$. Escribiendo $u = (g_0, \ldots, g_n)$, construimos $v = B_q(u,u)w - 2B_q(w,u)u \in K^{n+1}$.

Observamos, por cálculo directo, que $B_q(v,v) = -4B_q(u,u)B_q(w,u)^2 + 4B_q(w,u)^2B_q(u,u) = 0$, esto es v es un vector isótropo para q, y:

$$B_q(u,u) = q(u) = -pg_0^2 + a_1g_1^2 + \ldots + a_ng_n^2,$$

$$B_q(w,u) = -pf_0g_0 + a_1f_1g_1 + \ldots + a_nf_ng_n,$$

demuestran que las coordenadas de v están en $F[X]$. Examinemos ahora v_0, donde $v = (v_0, v_1, \ldots, v_n)$:

$$\begin{aligned} v_0 &= (-pg_0^2 + \sum_{i=1}^{n} a_ig_i^2)f_0 - 2(-pf_0g_0 + \sum_{i=1}^{n} a_if_ig_i)g_0 \\ &= pf_0 + \sum_{i=1}^{n} a_i(g_i^2f_0 - 2f_ig_i) \\ &= \frac{1}{f_0}(pf_0^2 + \sum_{i=1}^{n} a_i((g_if_0)^2 - 2f_ig_if_0)) \\ &= \frac{1}{f_0}(pf_0^2 + \sum_{i=1}^{n} a_i(f_i - g_if_0)^2 - \sum_{i=1}^{n} a_if_i^2) \\ &= \frac{1}{f_0}(\sum_{i=1}^{n} a_ir_i^2). \end{aligned} \qquad (**)$$

Luego, $gr(v_0) \leq 2 \max_{1\leq i\leq n}(gr(r_i) - gr(f_0)) < gr(f_0)$, lo que, junto con el hecho que v es isótropo para q, implica que podemos obtener una representación para $p(X)$ como la representación(') , pero con denominador con menor grado. Esto no es posible, pues $gr(f_0)$ se tomó el menor posible para una representación de la forma (') . Observar que $v_0 \neq 0$, pues por la elección del grado de f_0, f_0 no divide a todos los f_i, luego existe $r_i(X) \neq 0$ y como f es anisótropa sobre F, lo es sobre $F(X)$ y entonces de (") resulta $v_0 \neq 0$.

Sea F un cuerpo, denotamos por $F[X]$ el anillo de polinomios en las indeterminadas $X_1, \ldots X_n$, esto es $F[X] = F[X_1, \ldots, X_n]$, en los dos corolarios siguientes:

Corolario 4.1.2. Sea q una forma cuadrática sobre F, $p(X) \in F[X]$ y $a = (a_1, \ldots, a_n) \in F^n$ tal que $p(a) \neq 0$, entonces si $p(X) \in D_{F(X)}(q)$ es $p(a) \in D_F(q)$.

Demostración. Por hipótesis es $p(X) \in D_{F(X)}(q)$, donde $F(X) = F(X_1, \ldots, X_n) = F(X_1, \ldots, X_{n-1})(X_n)$, en consecuencia, por el teorema 4.1.1., q representa a $p(X)$ sobre $F(X_1, \ldots, X_{n-1})[X_n]$. Si se escribe tal representación y se sustituye X_n por a_n en la misma, se obtiene que q representa a $p(X_1, \ldots, X_{n-1}, a_n)$ sobre $F(X_1, \ldots, X_{n-1})$ y el argumento se puede repetir hasta obtener que q representa a $p(a)$ sobre F.

Teorema 4.1.3. Sea $q \perp \langle a \rangle$ una F-forma anisótropa sobre F, $a \in F$, entonces $d \in D_F(q)$ si, y sólo si, $d + aX^2 \in D_{F(X)}(q \perp \langle a \rangle)$.

Demostración. Si $d \in D_F(q)$, luego $q = \langle d, \ldots \rangle$ y por consiguiente $q \perp \langle a \rangle$ representa $d + aX^2$ sobre $F(X)$. Recíprocamente, por el teorema 4. 1. 1., podemos escribir:

$$d + aX^2 = a_1 f_1^2 + \ldots + a_n f_n^2 + a g^2,$$

donde $q = \langle a_1, \ldots, a_n \rangle$ es una representación diagonal de q, $f_1, \ldots, f_n$, $g \in F[X]$. Si existe algún f_i de grado ≥ 2 ó $\mathrm{gr}(g) \geq 2$, entonces para que tenga sentido la ecuación polinómica anterior los términos de mayor grado que 2 deben eliminarse, lo que implica que la forma $q \perp \langle a \rangle$ contiene un plano hiperbólico, lo que es una contradicción, pues al ser $q \perp \langle a \rangle$ anisótropa sobre F, lo es también sobre $F(X)$. Entonces $\mathrm{gr}(f_i) \leq 1$ y $\mathrm{gr}(g) \leq 1$. Sea $g(X) = bX + c$, elegimos en $\dot{F}$ un e que sea solución de alguna de las ecuaciones $bX + c = \pm X$, y reemplazando $e = X$ en la ecuación polinómica obtenemos $d = a_1 f_1(e)^2 + \ldots + a_n f_n(e)^2 \in D_F(q)$.

Observación. Si fuese $q \perp \langle a \rangle$ isótropa sobre F, lo sería también sobre $F(X)$ y en consecuencia $D_{F(X)}(q \perp \langle a \rangle) = F(X) - [0]$. Pero si $d \notin D_F(q)$, la hipótesis $d + aX^2 \in D_{F(X)}(q \perp \langle a \rangle)$ se cumple. Esto demuestra que no se puede prescindir de la hipótesis sobre $q \perp \langle a \rangle$ de anisotropía.

Aplicación. Sea F, $a \in \dot{F}$, definimos:

$$\mathrm{long}_F(a) = \text{mínimo } \{n / a = x_1^2 + \ldots + x_n^2;\ x_i \in F\}.$$

Si a no es suma de cuadrados en F, se dice que tiene "longitud" infinita. $\mathrm{long}_F(a)$ se llama "la longitud de a sobre F". Supongamos que F es un cuerpo formalmente real.

1) Si $u \in \dot{F}$, entonces $\mathrm{long}_{F(X)}(u + X^2) = 1 + \mathrm{long}_F(u)$.

Sea $\mathrm{long}_F(u) = n$ finita, luego $u + X^2$ se expresa en $F(X)$ como la suma de $n + 1$ cuadrados, en consecuencia $\mathrm{long}_{F(X)}(u + X^2) \leq n + 1$. Si $\mathrm{long}_{F(X)}(u + X^2) = m$, tenemos $u + X^2 \in D_{F(X)}(m\langle 1 \rangle)$, o también $u + X^2 \in D_{F(X)}((m - 1)\langle 1 \rangle \perp \langle 1 \rangle)$. Si se aplica el teorema 4. 1. 3., con $a = 1$, $q = (m - 1)\langle 1 \rangle$, se deduce que $u \in D_F(m - 1)$, de donde $\mathrm{long}_F(u) \leq m - 1$, esto es $1 + \mathrm{long}_F(u) \leq m$.

2) $\mathrm{long}_K(X_1^2 + \ldots + X_n^2) = n$, donde $K = F(X_1, \ldots, X_n)$. Basta observar que:

$$\mathrm{long}_K(X_1^2 + \ldots + X_n^2) = 1 + \mathrm{long}_{F(x_1, \ldots, x_{n-1})}(X_1^2 + \ldots + X_{n-1}^2)$$

y aplicar inducción.

3) $\mathrm{long}_K(1 + X_1^2 + \ldots + X_n^2) = n + 1$, $K = F(X_1, \ldots, X_n)$.

Teorema 4. 1. 4. (de la subforma). Sean f y g formas cuadráticas sobre F y f anisótropa. Son equivalentes:

a) g es isométrica a una subforma de f.

b) Para cualquier extensión K/F, se cumple $D_K(g) \subseteq D_K(f)$.

c) $g(X_1, \ldots, X_n) \in D_{F(x_1, \ldots, x_n)}(f)$, $n = \dim(g)$.

Demostración. a) → b) es inmediata.

b) → c). Tomar $K = F(X_1, \ldots, X_n)$.

c) → a). Sea $g = \langle a_1, \ldots, a_n \rangle$ y procedamos por inducción sobre la dimensión de f.

Si $\dim(f) = 0$, es $D_{F(X)}(f) = \phi$, donde $F(X) = F(X_1, \ldots X_n)$, luego g es la forma cero.

Sea $\dim(f) > 0$. Como $a_1X_1^2 + \ldots + a_nX_n^2 \in D_{F(X)}(f)$, aplicando el corolario 4. 1. 2. con $a = (1, 0, 0, \ldots, 0)$, obtenemos que $a_1 \in D_F(f)$. Podemos escribir $f \simeq \langle a_1 \rangle \perp f_1$ sobre F y si se denota por $X' = (X_2, \ldots, X_n)$, observamos que f es anisótropa sobre $F(X')$ y g puede escribirse $g = \langle a_1 \rangle \perp h$, $h = \langle a_2, \ldots, a_n \rangle$, entonces:

$$a_1X_1^2 + h(X') = g(X) \in D_{F(X)}(f) = D_{K(X_1)}(\langle a_1 \rangle \perp f_1),$$

donde $K = F(X')$. Por el teorema 4. 1. 3. tenemos que $h(X') \in D_{F(X')}(f_1)$. Aplicando la hipótesis inductiva a f_1 se tiene $f_1 \simeq h \perp q$ para alguna F-forma q, de donde, sumando $\langle a_1 \rangle$, obtenemos $f \simeq g \perp q$.

Observación. Sean f y g como en el teorema, entonces $g(X_1, \ldots, X_n) \in D_{F(X_1, \ldots, X_n)}(f)$ implica que la dimensión de g es $\leq$ que $\dim(f)$.

Teorema 4. 1. 5. Sea f una F-forma de dimensión n. Los siguientes enunciados son equivalentes:

a) f es una forma de Pfister.

b) $\forall\ K/F$ es $D_K(f)$ un grupo.

c) Si $X = (X_1, \ldots, X_n)$ e $Y = (Y_1, \ldots, Y_n)$, entonces $f(X)\, f(Y) \in D_{F(X, Y)}(f)$.

d) $f(X) \cdot f \simeq f$ sobre $F(X)$.

Demostración. a) → d). f como forma de Pfister sobre $F(X)$ representa a $f(X)$, luego $f(X) \cdot f \simeq f$.

d) → c). También $f(X) \cdot f \simeq f$ sobre $F(X, Y)$ y como f representa $f(Y)$ sobre $F(Y)$, entonces $f(X) \cdot f$ representa $f(X)\, f(Y)$ sobre $F(X, Y)$.

c) → b). Sean K/F una extensión y $f(u)$ y $f(v)$ valores representados por f sobre K. Por hipótesis, f representa $f(X)\, f(Y)$ sobre $F(X, Y)$, y entonces, sobre $K(X, Y)$, por el corolario 4. 1. 2, tenemos que $f(u)\, f(v) \in D_K(f)$.

b) → a). Al ser $D_F(f)$ un grupo, entonces f representa 1, luego f contiene a la 0-forma de Pfister $\langle 1 \rangle$. Supongamos que 2^r es la dimensión máxima de una subforma de f que es r-forma de Pfister, es claro que $r \geq 1$ a menos que $n = 1$, en cuyo caso está demostrado ya. Si fuese $n > 2^r$, podemos escribir $f = g \perp f_0$, donde g es r-Pfister sobre F. Afirmamos que si $a \in D_F(f_0)$, $g \perp \langle a \rangle \cdot g$ es una subforma de f sobre F. Para ello consideramos $X' = \{X_1, \ldots, X_{2^r}\}$, $Y' = \{Y_1, \ldots, Y_{2^r}\}$ conjuntos disjuntos de indeterminadas sobre F, y observamos que $g(X') + ag(Y') = g(Y')\,(g(X')\, g(Y')^{-1} + a)$. Como g es Pfister, se tiene $g(X')\, g(Y')^{-1} \in D_K(g)$, donde $K = F(X', Y')$, luego $g(X')/g(Y') + a$ está representado por f sobre K desde que $f \simeq g \perp \langle a, \ldots \rangle$ sobre F.

En consecuencia, por la hipótesis, se tiene que $\varphi(X') + a\varphi(Y')$ está representado por f sobre K y entonces por el teorema 4.1.4. es $\varphi \perp \langle a \rangle \varphi$ una subforma de f sobre F, pero $\varphi \perp \langle a \rangle \varphi = \varphi \langle 1, a \rangle$ es una $r+1$-forma de Pfister, lo que es contrario a la maximalidad de φ, entonces $n = 2^r$.

4.2. CUERPO DE FUNCIONES DE UNA FORMA CUADRÁTICA

Sea f una F-forma de grado n, $f \neq \langle 1, -1 \rangle$, $n \geq 2$. En estas condiciones es inmediato observar que el polinomio f es irreducible y por lo tanto genera un ideal primo en el dominio de factorización $F[X_1, \ldots, X_n]$. Consideremos el dominio de integridad $F[X_1, \ldots, X_n]/(f)$ y denotemos por $F(f)$ su cuerpo de fracciones. Con las observaciones precedentes, $F(f)$ se llama *el cuerpo de funciones de la forma cuadrática* f (o también un cuerpo de ceros genérico de la forma f).

Si $\pi: F[X_1, \ldots, X_n] \to F[X_1, \ldots, X_n]/(f)$ es la aplicación canónica al cociente y se denota $\pi(X_i) = x_i$. Se observa que $F(f) = F(x_1, \ldots, x_n)$ es el cuerpo de fracciones de $F[x_1, \ldots, x_n]$. Aún más:

a) Como F se identifica con un subcuerpo de $F(f)$, entonces f puede considerarse como $F(f)$-forma. Sea, por ejemplo, $f = \langle a_1, \ldots, a_n \rangle$, $a_i \in \dot{F}$, entonces en $F(f)$ se tiene $a_1x_1^2 + \ldots + a_nx_n^2 = 0$, esto es, f es isótropa sobre $F(f)$ y el vector isótropo $(x_1, \ldots, x_n)$ se llama un "cero genérico de f".

b) Supongamos que $f_1 \simeq f_2$, F-formas, entonces $F(f_1)$ es isomorfo a $F(f_2)$, pues bastará considerar el automorfismo del anillo $F[X_1, \ldots, X_n]$ que asocia a cada polinomio $p(X_1 \ldots, X_n)$ el polinomio $p(A \cdot X)$, donde X se toma como vector columna de componentes X_i y A es la $n \times n$ matriz inversible tal que $f_2(A \cdot X) = f_1(X)$. También, si $f_2 = af_1$, $a \in \dot{F}$, entonces $F(f_1) = F(f_2)$ desde que f_1 y f_2 generan el mismo ideal en $F[X_1, \ldots, X_n]$.

c) $F(f) = F(x_1, \ldots, x_n)$ tiene grado de trascendencia $n-1$, pues cualquier subconjunto de $n-1$ elementos de $\{x_1, \ldots, x_n\}$ es algebraicamente independiente sobre F.

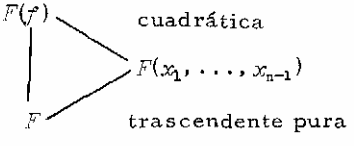
d) Sea $f = \langle a_1, \ldots, a_n \rangle$. De lo observado en a) tenemos:

$$x_n^2 = -a_n^{-1}(a_1x_1^2 + \ldots + a_{n-1}x_{n-1}^2),$$

esto es $x_n^2 \in F(x_1, \ldots, x_{n-1})$, por lo tanto:

$$F(f) = F(x_1, \ldots, x_{n-1})(x_n) = F(x_1, \ldots, x_{n-1})(\sqrt{-d})$$

donde $d = a_n^{-1}(a_1x_1^2 + \ldots + a_{n-1}x_{n-1}^2)$. Por tanto tenemos el siguiente diagrama de estructura para $F(f)$.



Observemos también que al ser, por ejemplo, $x_1, \ldots, x_{n-1}$, algebraicamente independientes sobre F, podemos también identificar $F(X_1, \ldots, X_{n-1})$ con $F(x_1, \ldots, x_{n-1})$ dentro de $F(f)$ y entonces $a = a_n^{-1}(a_1X_1^2 + \ldots + a_{n-1}X_{n-1}^2)$.

Después de estas consideraciones generales haremos la demostración de un reciente y famoso resultado (1971) conocido como el "Hauptsatz" de Arason y Pfister.

Lema 4.2.1. Sean $K = F(\sqrt{d})$ una extensión cuadrática y q una F-forma anisótropa sobre F e hiperbólica sobre K, entonces $X^2 - d$ verifica $(X^2 - d) \cdot q \simeq q$ sobre $F(X)$ para cualquier indeterminada X sobre F.

Demostración. Por 2.4.1.b) al ser q_K hiperbólica, existe una F-forma h tal que $q \simeq \langle 1, -d\rangle \otimes h$ sobre F. Como $X^2 - d$ es representado por $\langle 1, -d\rangle$ sobre $F(X)$ y $D_{F(X)}(\langle 1, -d\rangle) = G_{F(X)}(\langle 1, -d\rangle)$, por 1.5.5.b) tenemos $(X^2 - d)\langle 1, -d\rangle \simeq \langle 1, -d\rangle$ sobre $F(X)$, de donde $(X^2 - d)\langle 1, -d\rangle \otimes h \simeq \langle 1, -d\rangle \otimes h \simeq q$, esto es $(X^2 - d)\, q \simeq q$ sobre $F(X)$.

Teorema (Arason y Pfister) 4.2.2. Sea $q \neq 0$ una F-forma anisótropa sobre F tal que $q \in I^nF$, entonces $\dim(q) \geq 2^n$.

Demostración. Sabemos que I^nF es generado aditivamente en WF por las n-formas de Pfister, por lo tanto $q = c_1f_1 + \ldots + c_rf_r$, donde $c_j = \pm 1$, f_j son F-formas de Pfister de dimensión 2^n. Procedemos por
72 inducción sobre r.

Si $r = 1$, es $q = c_1f_1$. Por ser f_1 anisótropa (pues, en caso contrario, será hiperbólica y $q = 0$ en WF, lo que no es), se tiene que q y c_1f_1 son dos formas anisótropas que representan el mismo elemento en WF. Entonces $\dim(q) = \dim(c_1f_1) = 2^n$. Sea $r > 1$. Consideremos $K = F(f_1) = F(c_1f_1)$ por lo observado en b). Luego en K es $q = c_2f_2 + \ldots + c_rf_r$, si fuese q no hiperbólica sobre K, entonces en WK se tiene que:

$$(q_K)_a = q_K = c_2f_2 + \ldots + c_rf_r,$$

donde $(q_K)_a$ denota la parte anisótropa de q_K. Por aplicación de la hipótesis inductiva es $\dim((q_K)_a) \geq 2^n$ y luego $\dim(q) \geq 2^n$. Si q es hiperbólica sobre K, denotemos por $L = F(X_1, \ldots, X_{2^n-1})$, y por la observación d), tenemos que $K = L(\sqrt{-d})$, una extensión cuadrática de L, donde, en este caso, $d = a_{2^n}^{-1}(a_1X_1^2 + \ldots + a_{2^n-1}X_{2^n-1}^2)$ para una representación de $f_1 = \langle a_1, \ldots, a_{2^n}\rangle$. En la extensión cuadrática K/L aplicamos el lema 4.2.1. puesto que q es anisótropa sobre L y considerando la indeterminada X_{2^n} sobre L, obtenemos $(X_{2^n}^2 - d) \cdot q \simeq q$, esto es, de la anterior expresión de d, $f_1(X_1, \ldots, X_{2^n}) \cdot q \simeq q$ sobre $F(X_1, \ldots, X_{2^n})$. Luego, si $a \in D_F(q)$, entonces para $q_1 = aq$ es $1 \in D_F(q_1)$, q_1 anisótropa, $f_1(X_1, \ldots, X_{2^n})\, q_1 \simeq q_1$, de donde $f_1(X_1, \ldots, X_{2^n}) \in D_{F(x_1, \ldots, x_{2^n})}(q_1)$ y por el teorema de la subforma es $\dim(q) = \dim(q_1) \geq \dim(f_1) = 2^n$.

Corolario 4.2.3. $\bigcap_{n=1}^{\infty} I^nF = 0$.

Demostración. Del teorema anterior es claro que no puede existir una forma anisótropa de dimensión finita y positiva en $I^n F$ para todo n.

Veamos algunas propiedades del cuerpo de funciones de una forma cuadrática.

Proposición 4.2.4. Sea f una F-forma, entonces $F(f)/F$ es trascendente pura si, y sólo si, f es isótropa sobre F.

Demostración. Si $F(f)/F$ es trascendente pura, entonces es inmediato que f debe ser isótropa sobre F, pues en caso contrario será anisótropa sobre $F(f)$.

Recíprocamente, si f es isótropa, entonces $f \simeq f_0 \perp \langle 1, -1\rangle$, pero $\langle 1, -1\rangle \simeq X_{n-1}X_n$, por lo tanto podemos escribir en $F(f)$, $f_0(x_1, \ldots, x_{n-2}) + x_{n-1}x_n = 0$, de donde, $x_n = -f_0(x_1, \ldots, x_{n-2})\, x_{n-1}^{-1}$, de lo que obtenemos $F(f) = F(x_1, \ldots, x_n) = F(x_1, \ldots, x_{n-1})$ que es trascendente pura sobre F.

Teorema 4.2.5. Sean f y g F-formas, $\dim(f) = n$. Si g es hiperbólica sobre $F(f)$ y $1 \in D_F(f)$, entonces $f(X) \in G_{F(X)}(g)$, donde $X = (X_1, \ldots, X_n)$.

Demostración. Como $1 \in D_F(f)$, escribamos $f = \langle 1\rangle \perp f_1$, luego $F(f) = F(X_2, \ldots, X_n)(\sqrt{-f_1(X')})$, donde $X' = (X_2, \ldots, X_n)$, esto es, $F(f) = K(\sqrt{-f_1(X')})$, donde $K = F(X_2, \ldots, X_n)$. Supongamos primero que g es anisótropa sobre F. En este este caso, g es anisótropa sobre K y, al ser hiperbólica sobre $F(f)$, por 2.4.1. existe una K-forma h tal que $g \simeq \langle 1, f_1(X')\rangle \otimes h$. Sobre $F(X)$ la 1-forma de Pfister $\langle 1, f_1(X')\rangle$ representa $X_1^2 + f_1(X') = f(X)$, luego $\langle 1, f_1(X')\rangle$ tiene a $f(X)$ como factor de similaridad sobre $F(X)$, de donde $g_{F(X)} \simeq \langle 1, f_1(X')\rangle_{F(X)} \otimes h_{F(X)} \simeq f(X) \otimes \langle 1, f_1(X')\rangle_{F(X)} \otimes h_{F(X)} \simeq f(X) \cdot g_{F(X)}$ demuestra el teorema en este caso. Ahora si g es isótropa, entonces $g \simeq g_a \perp mH$, con g_a = parte anisótropa de g sobre F. Sobre $F(X)$: $f(X) \cdot g \simeq f(X) \cdot g_a \perp f(X) \cdot mH \simeq g$.

Corolario 4.2.6. Para cualquier F-forma f, f es hiperbólica sobre $F(f)$ si, y sólo si, f es hiperbólica o múltiplo escalar de una forma de Pfister.

Demostración. Si $f \simeq ag$, donde g es una forma de Pfister sobre F, entonces $F(f) = F(g)$, y como g es hiperbólica sobre $F(g)$, resulta f hiperbólica sobre $F(f)$. Recíprocamente, si f es isótropa sobre F, es $F(f)/F$ trascendente pura por 4.2.4., luego debe ser f hiperbólica sobre F, pues, en caso contrario, su parte anisótropa es $\neq 0$ y se preserva al "levantar" la forma a $F(f)$, lo que es contrario a nuestra hipótesis. Supongamos que f es anisótropa sobre F, podemos suponer que f representa al 1 (multiplicando si es necesario f por un elemento por ella representado sobre F), luego por el teorema 4.2.5. es $f(X)f \simeq f$, sobre $F(X)$, y entonces por el teorema 4.1.5. es f una forma de Pfister sobre F.

Corolario 4.2.7. Sean f y g F-formas tales que $1 \in D_F(f)$, g hiperbólica sobre $F(f)$ y g anisótropa sobre F, entonces $\forall\, a \in D_F(g)$, g contiene una subforma isométrica a af sobre F.

Demostración. Por el teorema 4.2.5. al ser, por hipótesis, g hiperbólica sobre $F(f)$ es $f(X) \cdot g \simeq g$ sobre $F(X)$, donde $X = (X_1, \ldots, X_n)$,

$n = \dim(f)$. $af(X)$ se representa por $g(X)$ sobre $F(X)$, luego por el teorema de la subforma g contiene una subforma isométrica a af sobre F.

Finalizamos con el siguiente resultado importante, el cual caracteriza el núcleo $W(F(f)/F)$ cuando f es una forma de Pfister; el caso particular en que f es una 1-forma de Pfister se estudió ya y corresponde a 2. 4. 1. c).

Teorema 4.2.8. Sea f una forma de Pfister sobre F y g una forma sobre F, anisótropa sobre F. g es hiperbólica sobre $F(f)$ si, y sólo si, $g \simeq f \otimes h$ para alguna F-forma h.

Demostración. Si $g \simeq f \otimes h$, es inmediato que g es hiperbólica sobre $F(f)$ puesto que f es una forma de Pfister. Ahora bien, si g es hiperbólica sobre $F(f)$, por el corolario 4. 2. 7. es $g \simeq \langle a \rangle f \perp g_1$, $a \in D_F(g)$. En $F(f)$ tenemos que g_1 es hiperbólica sobre $F(f)$ y aplicando la hipótesis inductiva a g_1 encontramos que $g_1 \simeq \langle a_2, \ldots, a_s \rangle \otimes f$, de donde $g \simeq \langle a_1, \ldots, a_s \rangle \otimes f$, donde $a = a_1$.

Corolario 4.2.9. $W(F(f)/F) = WF \cdot f$ para cualquier F-forma de Pfister f sobre F.

Un problema actual es el siguiente: Si f es F-forma, ¿cómo son los elementos de $W(F(f)/F)$? Un caso particular es el demostrado ya.

EJERCICIOS

1. Probar que F es algebraicamente cerrado en $F(f)$ para cualquier f, F-forma.

2. (Wadsworth). Si $F(f) = F(g)$ son F-isomorfos, donde f es una forma de Pfister anisótropa, entonces g es múltiplo escalar de f sobre F.

3. Demostrar que un orden w sobre F se extiende a $F(f)$ si, y sólo si, f es indefinida respecto de w.

4. Dado un cuerpo F, se denomina el "nivel de F" al número $s(F) = \log_F(-1)$, luego si F es formalmente real $s(F)$ es infinito y si $s(F)$ es finito F es no real.

(Pfister). Si F es no real, demostrar que $s(F)$ es una potencia de 2. (Sug. : existe k tal que $2^k \leq s(F) < 2^{k+1}$, luego $-1 = u + v$, donde $u \in D_F(2^k \langle 1 \rangle)$ y $v \in D_F((2^k - 1)\langle 1 \rangle)$. Observar que $-u \in D_F(2^k \langle 1 \rangle)$ y aplicar que $D_F(2^k \langle 1 \rangle)$ es un grupo para concluir que $-1 \in D_F(2^k \langle 1 \rangle)$.

5. Demostrar que $s(F) = s(F(X))$.

6. Sean f y g formas sobre F de dimensión 2^n, las cuales representan un elemento en común $c \in \dot{F}$. Demostrar que $f \equiv g$ mód $I^{n+1}F$ implica que $f \simeq g$. (Sug. : observar que $f \simeq \langle c \rangle \perp f_0$ y $g \simeq \langle c \rangle \perp g_0$. Poner $q = f_0 \perp \langle -1 \rangle \cdot g_0$ y $f \perp \langle -1 \rangle g \simeq H \perp q$, luego, por hipótesis, $q \in I^{n+1}F$ y como $\dim(q_a) \leq \dim(q) < 2^{n+1}$ por el "Hauptsatz" es $q = 0$ en WF.

APÉNDICE AL CAPÍTULO 1

FORMAS CUADRÁTICAS SOBRE CUERPOS p-ÁDICOS

Este apéndice es una breve exposición de la teoría de formas cuadráticas sobre cuerpos p-ádicos. Con este fin se han introducido inicialmente los conceptos de valuación, anillo de valuación, cuerpo residual y completación de un cuerpo valuado. Se definen los cuerpos p-ádicos y se demuestra que su cuerpo residual es finito. Para cuerpos locales cuyo cuerpo residual tiene característica distinta de 2 se enuncia el teorema de Springer sobre el anillo de Witt, y a continuación se aplica a los cuerpos p-ádicos con $p \neq 2$. La demostración de este importante teorema puede consultarse en la cita (9). No se trata el caso $p = 2$ y sólo se enuncian los principales resultados. Finalmente se considera el teorema de Hasse-Minkowski, el cual clasifica las formas cuadráticas sobre cuerpos de números algebraicos. La demostración de este teorema puede verse en (17), § 66; nuestro interés es su aplicación al cuerpo racional.

A. 1. VALUACIONES Y VALORES ABSOLUTOS

Definición. 1. Sea K un cuerpo; una valuación discreta sobre K es un homomorfismo $v: \dot{K} \to Z$ del grupo multiplicativo $\dot{K}$ sobre el grupo aditivo de los enteros Z tal que:

$$v(x + y) \geq \text{mínimo } \{v(x),\ v(y)\}.$$

Se conviene en definir $v(0) = \infty$.

Ejemplo 1. Sea p un número primo positivo en Z y Q el cuerpo de los racionales. Todo $x \in \dot{Q}$ se puede escribir $x = p^r \cdot m/n$, donde $r \in Z$, $m, n \in \dot{Z}$ y $(m, p) = (n, p) = 1$. Se define $v: \dot{Q} \to Z$ tal que $v(x) = r$, $v(0) = \infty$. Es inmediato verificar que v es una valuación sobre Q conocida como *valuación p-ádica de Q*.

Sea v una valuación sobre K. El conjunto $A = \{x \in K / v(x) \geq 0\}$ es un subanillo de K cuyo cuerpo de fracciones es K. *A es llamado el anillo de valuación de v.* $\mathfrak{M} = \{x \in K / v(x) > 0\}$ es un ideal de A. Aún más, $\mathfrak{M}$ es el único ideal maximal de A, pues si $x \notin \mathfrak{M}$, entonces $v(x) = 0$, luego $0 = v(1) = v(x \cdot x^{-1}) = v(x) + v(x^{-1})$ implica $v(x^{-1}) = 0$ y, por lo tanto, $x^{-1} \in A$. Así todo elemento del complemento de $\mathfrak{M}$ en A es una unidad en A, de lo que se obtiene que A es un anillo local con ideal maximal $\mathfrak{M}$ y grupo de unidades $U = \{x \in A / v(x) = 0\}$. Si $J \neq 0$ es un ideal en A, sea k = mínimo entero tal que existe $x \in J$ con $v(x) = k$, luego $J = \{y \in A / v(y) \geq k\}$ (puesto que si y es tal que $v(y) \geq k = v(x)$ para algún $x \in J$, $v(y \cdot x^{-1}) \geq 0$, de donde $yx^{-1} \in A$). Se obtiene así que los ideales no nulos de A tienen la forma $\mathfrak{M}_k = \{y \in A / v(y) \geq k\}$, $k \in Z$. Además, como v es suryección,

existe un x tal que $v(x) = 1$, de donde $\mathcal{M} = Ax$ y $\mathcal{M}_k = Ax^k$. Uno de tales elementos se llama el *normalizador de* v y se denota por π. Por $\bar{K}$ se denota el cuerpo $A/\mathcal{M}$, el cual se llama el *cuerpo de clases residuales* de K (o más simplemente, el cuerpo residual de K). Todo $x \in A$ se escribe $x = u\pi^r$, $r \geq 0$, $u \in U$. En consecuencia, todo $x \in \dot{K}$ puede escribirse en forma única como $x = u\pi^r$, donde $r \in Z$ y $u \in U$.

A. 2. TOPOLOGÍA DEFINIDA POR UNA VALUACIÓN

Sea (K, v) un cuerpo valuado, $\rho > 1$ y $\rho \in R$. La aplicación $\varphi: K \to R$ definida por $\varphi(x) = \rho^{-v(x)}$ cumple las siguientes propiedades:

a) $\varphi(x) \geq 0$; $\varphi(x) = 0$ si, y sólo si, $x = 0$.

b) $\varphi(xy) = \varphi(x)\varphi(y)$.

c) $\varphi(x + y) \leq \text{máx}\ \{\varphi(x), \varphi(y)\}$.

φ se denomina el *valor absoluto* (no arquimediano) asociado a la valuación discreta v. Es claro que φ está definida unícamente por v y que la relación $v(x) = -\log_\rho \varphi(x)$ permite recuperar v a partir de φ. También obtenemos que: $A = \{x \in K / \varphi(x) \leq 1\}$; $\mathcal{M} = \{x \in K / \varphi(x) < 1\}$.

En este apéndice consideraremos un cuerpo valuado (K, v) fijo y por φ denotaremos el valor absoluto correspondiente.

Se define sobre K una métrica $d: K \times K \to R$ por $d(x, y) = \varphi(x-y) = \rho^{-v(x-y)}$.

Definición 2. Un cuerpo valuado (K, v) se denomina un *cuerpo local*, si K es un espacio métrico completo con la topología definida por φ.

Ejemplo 2. Sean p un primo positivo en Z y v la valuación p-ádica sobre Q; elegimos $\rho = p$, entonces la métrica definida sobre Q es $d(x, y) = p^{-v(x-y)}$. Es sabido que todo espacio métrico puede ser completado, esto es, puede ser sumergido homeomórficamente en un espacio métrico completo. Denotando por Q_p la completación de Q con la valuación p-ádica, Q_p es un cuerpo local, llamado el *cuerpo de los números p-ádicos*.

Teorema 1. Sea E un espacio métrico. Existe un espacio métrico completo $\hat{E}$ y una inyección $j: E \to \hat{E}$ tal que j es una isometría (métrica) de E sobre $j(E)$ y $j(E)$ es denso en $\hat{E}$.

Demostración. Véase la monografía no. 9 de esta misma serie.

En la demostración del teorema 1 se considera X = conjunto de todas las sucesiones de Cauchy en E y se define $(x_n) \sim (y_n)$, si $(d(x_n, y_n))$, es una sucesión de números reales convergente a cero. "$\sim$" es una relación de equivalencia. Se define $\hat{E} = X/\sim$, $\hat{d}(\dot{x}, \dot{y}) = \lim_{n\to\infty} d(x_n, y_n)$, donde $(x_n) \in \dot{x}$ e $(y_n) \in \dot{y}$. Se demuestra que $(\hat{E}, \hat{d})$ es un espacio métrico completo y que $j: E \to \hat{E}$ tal que $j(x) = \dot{x}$, donde $\dot{x}$ es la clase de la sucesión (x_n) y $x_n = x\ \forall\ n$ es la isometría buscada. Identificado E con $j(E)$ se demuestra luego que todo punto $\dot{x}$ de $\hat{E}$ es límite de una sucesión (x_n) tal que $x_n \in E\ \forall\ n$.

Teorema 2. Sea (K, v) un cuerpo valuado, el completado métrico $\hat{K}$ de K puede ser provisto de una estructura de cuerpo valuado $(\hat{K}, \hat{v})$, donde $\hat{v}$ es la valuación que extiende a $\hat{K}$ la valuación v de K.

Demostración. En X = colección de todas las sucesiones de Cauchy en K se define: (x_n) es *sucesión nula* si $\lim_{n\to\infty} \varphi(x_n) = 0$. X tiene estructura de anillo conmutativo con unidad con las operaciones ordinarias de sucesiones. Además, el conjunto $I = \{(x_n) \in X / (x_n)$ es nula$\}$ es un ideal de X. Es fácil observar que $\hat{K} = X/\sim$ es justamente X/I. Demostramos ahora que I es maximal. Si $(x_n) \notin I$, entonces existe $\varepsilon > 0$ y $n_0 > 0$ tal que $\forall\ n \geq n_0$ es $\varphi(x_n) \geq \varepsilon$ (demostrarlo como ejercicio); se define (y_n) por $y_n = 0$, si $n \leq n_0$ e $y_n = x_n^{-1}$, si $n > n_0$. Es un ejercicio fácil probar que (y_n) es de Cauchy. Se observa que $(x_n)(y_n) = \dot{1} - (1, \ldots, 1, 0, 0, \ldots)$. Por lo tanto, si J es un ideal conteniendo propiamente a I, se toma $(x_n) \in J - I$ y es $(x_n)(y_n) \in J$, de donde $\dot{1} \in J$. Luego $\hat{K}$ es una extensión del cuerpo K. Se define $\hat{\varphi}$ por $\hat{\varphi}(\dot{x}) = \hat{a}(\dot{x}, 0)$. $\hat{\varphi}$ es una aplicación de K en R que verifica las propiedades a), b) y c) de un valor absoluto no arquimediano, pero $\hat{\varphi}(\hat{K}) = \varphi(K)$ (demostrarlo), entonces se define $\hat{v}(\dot{x}) = -\log_\rho \hat{\varphi}(\dot{x}) \cdot v(x) \in Z$, pues existe $y \in K$ tal que $\hat{\varphi}(\dot{x}) = \varphi(y)$, luego $-\log_\rho \hat{\varphi}(\dot{x}) = -\log_\rho \varphi(y) = v(y) \in Z$.

A. 3. CUERPO RESIDUAL DE UN CUERPO p-ÁDICO.

Lema 1. Sea (L, w) una extensión del cuerpo valuado (K, v) (w restringida a K coincide con v). Existe un isomorfismo de $\bar{K}$ sobre un subcuerpo de $\bar{L}$.

Demostración. $A_v \subseteq A_w$ y $\mathcal{M}_v \subseteq \mathcal{M}_w$, por lo tanto se puede definir $f: A_v/\mathcal{M}_v \to A_w/\mathcal{M}_w$ por $f(x + \mathcal{M}_v) = x + \mathcal{M}_w$. Si $x \notin \mathcal{M}_v$ es $\varphi_v(x) = 1$ y luego $\varphi_w(x) = 1$, esto es $x \notin \mathcal{M}_w$.

Proposición 1. Sea L la completación del cuerpo valuado (K, v), entonces $\bar{L} = \bar{K}$.

Demostración. Basta ver que f definida en el lema es suryectiva. Sea $\bar{a} \in A_w$, luego $a = \lim_{n\to\infty}(a_n)$, donde $a_n \in K\ \forall\ n$, (a_n) sucesión de Cauchy. Entonces existe n_0 tal que $\forall\ n \geq n_0$ es $\varphi_w(a_n - a) < 1$. Luego si $n \geq n_0$, es $\varphi_w(a_n - a) < 1$. Luego si $n \geq n_0$, es $\varphi_v(a_n) = \varphi_w(a_n) = \varphi_w((a_n - a) + a) \leq$ máx $\{\varphi_w(a_n - a), \varphi_w(a)\} \leq 1$. Se toma $x = a_n$, donde $n > n_0$, y $f(\bar{x}) = \bar{a}$.

Aplicación 1. El cuerpo residual del cuerpo p-ádico Q_p es Z_p.

Sea v la valuación p-ádica sobre Q definida por el primo p. Se observa fácilmente que:

$$A = \{m/n \in Q / (m, n) = (n, p) = 1\}$$

$$\mathcal{M} = \{m/n \in Q / (m, n) = (n, p) = 1,\ p \text{ divide a } m\}.$$

Como $Z \subset A$ se tiene el siguiente homomorfismo de anillos:

$$\varrho: Z \to A \to A/\mathcal{M} = \bar{Q}.$$

Se afirma que es suryectivo. Si $x = m/n + \mathcal{M}$, $(n, p) = 1$, entonces existen $a, b \in Z$ tales que $an + bp = 1$, luego $m/n = ma + pb(m/n)$, esto es $m/n - ma = pbm/n \in \mathcal{M}$, de donde $\varrho(ma) = x$.

Además, si m es entero, $m \in \mathrm{Nu}(\varphi)$ implica $m \in \mathfrak{M}$, luego p divide a m, esto es $\mathrm{Nu}(\varphi) = pZ$. Concluimos así que $A/\mathfrak{M} \approx Z/pZ = Z_p$ y como $\bar{Q}_p = \bar{Q}$ es $\bar{Q}_p \approx Z_p$.

A. 4. CLASES MÓDULO CUADRADOS EN UN CUERPO LOCAL

Se mantiene la notación establecida en A. 1. Si $x \in A$, se utiliza $\bar{x}$ para denotar su imagen en el residual.

Proposición 2. Sea (K, v) un cuerpo local cuyo cuerpo residual tiene característica distinta de 2. u unidad en A es cuadrado en K y si, sólo si, $\bar{u}$ es cuadrado en $\bar{K}$.

Demostración. Si $u = a^2$, $a \in K$, se tiene $0 = v(u) = 2v(a)$, entonces $v(a) = 0$ y $\bar{u} = \bar{a}^2$ en $\bar{K}$. Recíprocamente si $\bar{u}$ es cuadrado en $\bar{K}$ se puede construir una sucesión (x_i) en U tal que $x_1^2 \equiv u$ mód $\mathfrak{M}^1$ y $x_{i+1} \equiv x_i$ mód $\mathfrak{M}^i$ $\forall\, i \geq 1$. Así, si x denota el límite de tal sucesión se tiene $x^2 - u = \lim_{i\to\infty} (x_i^2 - u) = 0$ (pues $x_i^2 - u \in \mathfrak{M}^i$ implica $d(x_i^2, u) = \rho^{-v(x_i^2-u)} = \rho^{-j}$, donde $j \geq i$), y se concluye que $u = x^2$. Para la construcción de la sucesión se procede recursivamente. Como $u = x_1^2 + \mathfrak{M}$, es $x_1^2 \equiv u$ mód$\mathfrak{M}^1$. Se supone definido el término x_i y se procede a determinar un z en A tal que si definimos $x_{i+1} = x_i + \pi^i z$, el término x_{i+1} satisface las condiciones pedidas. Escribamos $x_1^2 - u = \pi^i c$, $c \in A$, entonces $x_{i+1}^2 - u = \pi^i(c + 2x_i z)$ mód$\mathfrak{M}^{i+1}$ (aquí nos planteamos la ecuación $c + 2x_i z = \pi$ y podemos "despejar" z puesto que la caract$(\bar{K}) \neq 2$). Tomando z tal que $c + 2x_i z = \pi$, se obtiene $x_{i+1}^2 \equiv u$ mód$\mathfrak{M}^{i+1}$.

Consideremos los grupos de clases módulo cuadrados $\dot{K}/\dot{K}^2$ y $\dot{\bar{K}}/\dot{\bar{K}}^2$ del cuerpo local (K, v) y su residual, respectivamente (caract$(\bar{K}) \neq 2$). De la proposición anterior se desprende que:

$$j : \dot{\bar{K}}/\dot{\bar{K}}^2 \to \dot{K}/\dot{K}^2,\ j(\bar{u}\dot{\bar{K}}^2) = u\dot{K}^2$$

es un homomorfismo de grupos bien definido (si u y u_1 son tales que $\bar{u} = \bar{u}_1$, entonces $uu_1^{-1} = 1$ en $\bar{K}$, luego $uu_1^{-1} = a^2$ en $\dot{K}$).

Proposición 3. Sea (K, v) un cuerpo local cuyo cuerpo residual tiene característica distinta de 2. La siguiente sucesión de grupos es exacta y se "parte":

$$1 \to \dot{\bar{K}}/\dot{\bar{K}}^2 \xrightarrow{j} \dot{K}/\dot{K}^2 \xrightarrow{v} Z_2 \to 0$$

donde v designa la aplicación inducida por $v : \dot{K} \to Z$.

Demostración. La inyectividad es inmediata de la definición de j. Además la sucesión se parte pues, si se define $s : Z_2 \to \dot{K}/\dot{K}^2$ por $1 \to \pi\dot{K}^2$ se tiene que $VS = id_{Z_2}$.

Exactitud en $\dot{K}/\dot{K}^2$: $\mathrm{Im}(j) \subseteq \mathrm{Nu}(v)$ puesto que $v \cdot j = 0$. Si $x \in \mathrm{Nu}(v)$ y $x = a\dot{K}^2$, como $v(x) = 2Z$, resulta $v(a) \in 2Z$, esto es $a = u\pi^{2n}$, con $u \in U$, de donde $x = u(\pi^n)^2\,\dot{K}^2 = u\dot{K}^2$, y considerando $\bar{u}\dot{\bar{K}}^2$ se obtiene $j(\bar{u}\dot{\bar{K}}^2) = x$.

Corolario 1. Sea (K, v) un cuerpo local, caract$(\bar{K}) \neq 2$. Entonces:

$$o(\dot{K}/\dot{K}^2) = 2\, o(\dot{\bar{K}}/\dot{\bar{K}}^2).$$

Aplicación 2. El cuerpo p-ádico Q_p, $p \neq 2$, tiene exactamente cuatro clases módulo cuadrados.

Ello es una consecuencia inmediata del corolario 1 y del hecho que todo cuerpo finito tiene exactamente dos clases módulo cuadrados. Aún más, si u es unidad en Q_p tal que $\bar{u} \notin \bar{Z}_p^2$, entonces $\{1, u, \pi = p, up\}$ es un conjunto de representantes de las clases módulo cuadrados de Q_p.

Nota. En el caso $p = 2$ se demuestra:

a) Q_2 tiene exactamente 8 clases módulo cuadrados.

b) Sea $x \in Q_2$, x unidad. x es un cuadrado en Q_2 si, y sólo si, $x \equiv 1$ mód 8[1].

Ejemplo 3. $\sqrt{33}$ es un elemento de Q_2, pues basta observar que 33 es una unidad en Q_2 (al no ser dividido por 2 su valuación es cero), $33 - 1 = 8 \cdot 4 \in 8\Lambda$ (pues $v(4) = 2$), y en consecuencia, 33 es un cuadrado en Q_2 de acuerdo con b).

A. 5. TEOREMA DE SPRINGER PARA CUERPOS LOCALES

Teorema 3 (T.A. Springer). Sea K un cuerpo local cuyo cuerpo residual tiene característica distinta de 2. Se tiene el siguiente isomorfismo de grupos aditivos:

$$WK \approx W\bar{K} \times W\bar{K}$$

Aplicación 3.

1) Existen exactamente 16 formas anisótropas sobre un cuerpo p-ádico Q_p, $p \neq 2$.

En el ejemplo 7-e del capítulo 1 se ha establecido que:

a) Si p es de la forma $4n + 1$, $WZ_p \approx Z_2 \times Z_2$.

b) Si p es de la forma $4n + 3$, $WZ_p \approx Z_4$.

En consecuencia aplicando el teorema 3 se tiene en el caso a) $WQ_p \approx \approx Z_2^4$ y en el caso b) $WQ_p \approx Z_4^2$. En ambos, por cardinalidad, se concluye la existencia de exactamente 16 elementos en el anillo de Witt de Q_p, lo que significa que sólo existen 16 formas anisótropas (salvo isometría) sobre un cuerpo p-ádico Q_p, donde $p \neq 2$.

Nota. En el caso $p = 2$ se demuestra que $WQ_2 \approx Z_8 \times Z_2^2$ (como grupos aditivos), de lo que se concluye que existen exactamente 32 formas anisótropas sobre Q_2.

2) Anillo de Witt de un cuerpo de series de Laurent.

Sea K un cuerpo cuya característica es distinta de 2. Se considera el conjunto de series de potencia, formales, en una "indeterminada"

t, de la forma $\sum_{n=m}^{\infty} a_n t^n$, $n \in Z$, $a_n \in K$. Se denota este conjunto por $K((t))$ y se define sobre él la suma y producto de series de la forma usual. De esta manera $K((t))$ es un cuerpo llamado el *cuerpo de series de Laurent* sobre K (para demostrar que $K((t))$ es cuerpo, demostrar primero que un elemento de la forma $\sum_{i=0}^{\infty} a_i t^i$ es inversible si, y sólo si, a_0 es distinto de cero).

Se define una valuación sobre $K((t))$ definiendo $v(\sum_{i=m}^{\infty} a_i t^i) = m$, si $a_m \neq 0$. Se observa de inmediato que v es una valuación cuyo anillo de valuación es el anillo de series $K[[t]]$ y que tiene cuerpo residual K. Demostremos que $K((t))$ es completo respecto de la topología definida por v. Si $x = \sum_{i=m}^{\infty} a_i t^i$ podemos identificar x a la aplicación $x: Z \to K$ tal que $x(j) = 0$, si $j < m$, y $x(j) = a_j$, $j \geq m$. Sea (x_n) una sucesión de Cauchy en $K((t))$, luego si se elige $\varepsilon = \rho^{-i} > 0$ existe $N_1 > 0$ tal que si $k, s > N_1$ es $d(x_k, x_s) < \varepsilon$, esto es:

$$\text{si } k, s > N_1 \text{ es } \rho^{-v(x_k - x_s)} < \rho^{-i} \quad (\rho > 1).$$

80 Luego $v(x_k - x_s) > i$, en consecuencia si $j \leq i$ es $x_k(j) = x_s(j)$; $\forall\, k, s > N_1$. Definimos $b_j = x_k(j)$, donde $k > N_1$, para todo $j \leq i$. Se afirma que $x = \sum_{i=1}^{\infty} b_i t^i$ es límite de la sucesión (x_n), pues dado un $\varepsilon > 0$ existe un i tal que $\rho^{-i} < \varepsilon$, entonces existe $N = N_1$ tal que si $k > N$ es $x_k(j) = x(j)$ $\forall$ $j \leq i$, esto es $v(x_k - x) > i$, lo que significa que si $k > N$, es $d(x_k, x) < \rho^{-i} < \varepsilon$.

Se tiene así que $K((t))$ es un cuerpo local cuya característica del residual es distinta de 2, por lo tanto podemos aplicar el teorema de Springer y obtener el isomorfismo de grupos $WK((t)) \approx WK \times WK$. Por ejemplo, si $K = R$ (cuerpo de los números reales) es $WR((t)) \approx Z \times Z$. También si $p \neq 2$, se tiene $WZ_p((t)) \approx WQ_p$, de lo que se deduce que existen exactamente 16 formas anisótropas sobre el cuerpo local $Z_p((t))$.

Sea K un cuerpo local tal que $\text{caract}(\bar{K}) \neq 2$. Toda forma cuadrática de dimensión 1 puede ser escrita $\langle u \rangle$ o $\langle \pi u \rangle$. De aquí resulta que toda forma diagonal q sobre K puede escribirse $q = \langle u_1, \ldots, u_m \rangle \perp \pi \cdot \langle u_{m+1}, \ldots, u_n \rangle$, donde u_i son unidades en A, sean $\bar{q}_1 = \langle \bar{u}_1, \ldots, \bar{u}_m \rangle$, $\bar{q}_2 = \langle \bar{u}_{m+1}, \ldots, \bar{u}_n \rangle$, $\bar{q}_1$ y $\bar{q}_2$ son llamadas la primera y segunda formas residuales de q. El teorema de Springer establece que las formas residuales son únicamente determinadas por q cuando se consideran q, $\bar{q}_1$ y $\bar{q}_2$ como elementos del anillo de Witt respectivo; más precisamente, existe un isomorfismo:

$$(d_1, d_2): WK \to W\bar{K} \times W\bar{K}$$

de los grupos aditivos tal que si $q \in WK$ es $d_1(q) = \bar{q}_1$ y $d_2(q) = \bar{q}_2$. A con-

tinuación se presentan algunas otras consecuencias importantes del teorema de Springer.

Proposición 4. Sea K un cuerpo local, caract$(\bar{K}) \neq 2$.

a) Si $q = \langle u_1, \ldots, u_n \rangle$, $u_i \in U$ es K-forma. q es anisótropa sobre K si, y sólo si, $\bar{q}$ es anisótropa sobre $\bar{K}$.

b) Si $q = q_1 \perp \langle \pi \rangle q_2$, donde $q_1 = \langle u_1, \ldots, u_m \rangle$ y $q_2 = \langle u_{m+1}, \ldots, u_n \rangle$, $u_i \in U$. q es anisótropa sobre K si, q_1, q_2 son anisótropas sobre $\bar{K}$.

c) Si toda forma cuadrática de dimensión $n+1$ sobre $\bar{K}$ es isótropa, entonces toda forma cuadrática de dimensión $2n+1$ sobre K es isótropa.

d) Si existe sobre $\bar{K}$ una forma anisótropa de dimensión n, entonces K tiene una forma cuadrática anisótropa de dimensión $2n$.

Demostración. Probaremos a). b), c) y d) son consecuencia inmediata de a) y del teorema 3 (se dejan como ejercicio para el lector). Supongamos que $\bar{q}$ es anisótropa, si fuese q isótropa, existiría un vector $(x_1, \ldots, x_n)$ en K^n isótropo para q. Como $x_i = a_i b_i^{-1}$, $b_i \neq 0$ a_i en A, se pueden elegir los x_i en A, y aún más, prescindiendo de la potencia común de π contenida en los x_i se puede suponer que algún $x_i \in$ $\in U$, de donde $(x_1, \ldots, x_n)$ es un vector isótropo para $\bar{q}$ en K, lo que es contrario a lo supuesto. Recíprocamente, sea q anisótropa. Si $\bar{q}$ fuese isótropa, entonces sobre $\bar{K}$ sería $\bar{q} = (\bar{q})_a \perp (\bar{q})_h$, donde $\dim(\bar{q})_a <$ $< \dim(\bar{q})$. Tomando una diagonalización de $(\bar{q})_a$ sobre K y aplicando el isomorfismo inverso a $(\hat{a}_1, \hat{a}_2)$, se obtiene $q = \langle v_1, \ldots, v_r \rangle$ en WK, pero, por lo ya demostrado, $\langle v_1, \ldots, v_r \rangle$ es anisótropa, entonces $\dim(q) = r =$ $= \dim(\bar{q})_a$, lo que es absurdo. 81

Aplicación 4. Sea p un número primo, $p \neq 2$, Q_p el cuerpo de los números p-ádicos. Entonces:

a) Toda forma cuadrática sobre Q_p de dimensión mayor o igual que 5 es isótropa.

b) Existe una única forma cuadrática anisótropa sobre Q_p de dimensión 4.

b') Existe una única álgebra de cuaterniones sobre Q_p, no trivial, el álgebra (u, p), donde $u \in U$ y $\bar{u} \notin \dot{\bar{Q}}_p^2$.

Demostración.

a) Como toda forma ternaria sobre Z_p es isótropa, basta aplicar c) de la proposición 4.

b) La única forma binaria anisótropa sobre Z_p es $\langle 1, -\bar{u} \rangle$, donde 1 y $\bar{u}$ son los representantes de las dos clases módulo cuadrados de Z_p (véase el ejemplo 7 e, capítulo 1). Resulta que $\langle 1, -u \rangle \perp \pi \langle 1, -u \rangle$ es anisótropa sobre Q_p, esto es $\langle 1, -u, -p, pu \rangle$ es la única forma anisótropa de dimensión 4 sobre Q_p por aplicación de la proposición 4 d.

b') La forma de Pfister $\langle\langle -u, -p\rangle\rangle$ como espacio cuadrático es justamente el álgebra de cuaterniones (u, p).

Nota.

a) Como 0, $\langle 1\rangle$, $\langle \bar{u}\rangle$ y $\langle 1, \bar{u}\rangle$ son todas las formas anisótropas sobre Z_p (si p es de la forma $4n + 1$), y 0, $\langle 1\rangle$, $\langle -1\rangle$ y $\langle 1, \bar{u}\rangle$ en el caso $p = 4n + 3$, donde 1 y $\bar{u}$ representan las dos clases módulo cuadrados de Z_p, entonces de la proposición 4 b se pueden escribir las 16 formas anisótropas sobre Q_p.

b) Los enunciados a) y b) (respectivamente b') son también válidos en el caso $p = 2$.

Ejemplo 4. Sea Q_3 el cuerpo de los 3-ádicos. El normalizador es 3, Z_3 es el cuerpo residual y 1 y 2 los representantes de las clases módulo cuadrados en Z_3. Todas las formas anisótropas sobre Z_3 son 0, $\langle 1\rangle$, $\langle 2\rangle$ y $\langle 1, -2\rangle$, luego a partir de la proposición b) se tiene que las formas anisótropas sobre Q_3 (salvo isometría) son 0, $\langle 1\rangle$, $\langle 2\rangle$, $\langle 1, -2\rangle$, $\langle 3\rangle$, $\langle 6\rangle$, $\langle 3, -6\rangle$, $\langle 1, 3\rangle$, $\langle 1, 6\rangle$, $\langle 1, 3, -6\rangle$, $\langle 2, 3\rangle$, $\langle 2, 6\rangle$, $\langle 2, 3, -6\rangle$, $\langle 1, -2, 3\rangle$, $\langle 1, -2, 6\rangle$ y $\langle 1, -2, 3, -6\rangle$.

Ejemplo 5. La forma $q = \langle 3, -1, 14\rangle$ es isótropa sobre Q_2, pues $(1, \sqrt{17}, 1)$ es un vector isótropo para q (observar que $17 \equiv 1$ mód 8A). Si $\langle a, b, c\rangle$ es una forma ternaria sobre Q_p, donde $p \neq 2$, $a, b, c \in U$,
82 entonces es isótropa en virtud de la proposición 4 a). Luego $q = \langle 3, -1, 14\rangle$ es isótropa sobre todo Q_p, si $p \neq 3, 7$. Veamos sobre Q_3: $q = \langle 14, -1\rangle \perp 3\langle 1\rangle$, luego $\bar{q}_1 = \langle 2, -1\rangle$ y $\bar{q}_2 = \langle 1\rangle$ en WZ_3. Observamos directamente que $\bar{q}_1 \cdot \bar{q}_2$ son anisótropas sobre Z_3, por lo tanto de la proposición 4 b) resulta q anisótropa sobre Q_3 (véase el caso $p = 7$ como ejercicio).

A. 6 EL TEOREMA DE HASSE-MINKOWSKI PARA Q

En las secciones precedentes hemos podido observar que la clasificación de las formas cuadráticas sobre un cuerpo p-ádico, $p \neq 2$, está completa por la aplicación del teorema de Springer. El caso $p = 2$ es más complejo y aunque no lo tratamos, en este caso la clasificación también está completa. Para el caso del cuerpo Q de los racionales (o de extensiones finitas de Q) el problema de clasificación es más difícil y abarca resultados profundos de la teoría de los números. El principal resultado es el famoso teorema de Hasse-Minkowski, cuyos alcances son mayores a los que vamos a tratar.

Sea Q el cuerpo racional, una valuación discreta sobre Q determina un valor absoluto no arquimediano de la forma vista ya. Un teorema clásico de la teoría de valuaciones afirma que todo valor absoluto sobre Q es, salvo equivalencia, un valor absoluto p-ádico o el valor absoluto ordinario de Q. Así, podemos denotar por Q_p las completaciones de Q para todos los valores absolutos no arquimedianos, y $Q_p = R$ cuando se trata del valor absoluto ordinario, en este caso se dice que p es el primo infinito o el primo arquimediano de Q y se escribe $p = \infty$.

Teorema 4 (Hasse-Minkowski). Una forma cuadrática sobre Q es isótropa si, y sólo si, es isótropa sobre todas las completaciones Q_p de Q.

Se tienen de inmediato los siguientes corolarios:

Corolario 1. Sea q una forma cuadrática sobre Q, $a \in \dot{Q}$, q representa a a si, y sólo si, q representa a a en todo Q_p.

Demostración. Si q representa a a, entonces $Q \subset Q_p$ implica que q representa a a en todo Q_p. Recíprocamente, $q \perp \langle -a \rangle$ es isótropa en todo Q_p implica, por el teorema de Hasse-Minkowski, que $q \perp \langle -a \rangle$ es isótropa sobre Q y, por lo tanto, representa a a.

Corolario 2. Existe un homomorfismo de anillos

$$r: WK \to \prod_p WQ_p$$

que identifica WQ con un subanillo del anillo producto.

Demostración. La inclusión $Q \subset Q_p$ induce un homomorfismo de anillo $r_p: WQ \to WQ_p$, luego $r = (r_p): WQ \to \prod WQ_p$ es un homomorfismo de anillos. Sea $q \in WQ$ tal que q es hiperbólica sobre todo Q_p. Se procede por inducción en $n = \dim(q)$. Por el teorema de Hasse-Minkowski q es isótropa sobre Q, luego si $n = 2$, q es un plano hiperbólico. Sea $n > 2$, entonces $q = q_1 \perp H$ sobre Q. Se observa que q_1 es hiperbólica sobre todo Q_p desde que q lo es (aplicando el teorema de cancelación de Witt), como $\dim(q_1)$ es menor que n, por la hipótesis inductiva, es q_1 hiperbólica sobre Q, por lo tanto q es hiperbólica sobre Q, lo que demuestra que r es inyectiva.

Se observa que la inyección r no proporciona una imagen explícita de WQ. Puede demostrarse independientemente del teorema de Hasse-Minkowski que $WQ \approx Z \oplus Z_2 \oplus \bigoplus_{p \neq 2} WZ_p$ como grupo aditivo.

Corolario 3. Sea q una forma cuadrática sobre Q, $\dim(q) \geq 5$. Si q es isótropa sobre R, entonces q es isótropa sobre Q.

Demostración. Aplicar el teorema de Hasse-Minkowski y la aplicación 4 a).

Ejemplos:

6) Todo racional positivo puede expresarse como la suma de 4 cuadrados en Q.

Sea $a \in Q^+$, la forma $q = \langle 1, 1, 1, 1, -a \rangle$ sobre Q es isótropa sobre R, puesto que $-a \equiv -1$ mód $\dot{R}^2$, luego existen x_1, x_2, x_3, x_4 y x_5 no todos nulos, $x_i \in Q$ tales que:

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = a\, x_5^2$$

si $x_5 = 0$, tendríamos necesariamente que $x_1 = x_2 = x_3 = x_4 = 0$ desde que Q es formalmente real, luego es $x_5 \neq 0$ y a puede expresarse como la suma de 4 cuadrados en Q.

Nota. Este resultado es una aproximación al clásico teorema de Lagrange que establece que todo entero positivo es suma de 4 cuadrados en Z.

Ejemplo 7. La forma $q = \langle 1, 2, 5, -10\rangle$ es anisótropa y universal sobre Q. Por el teorema de Hasse-Minkowski basta ver que existe una completación Q_p de Q en la cual q es anisótropa. Se observa que $\langle 1, 2, 5\rangle$ es isótropa sobre todo Q_p tal que $p \neq 2, 5$ (en el primo infinito, como $-10 \equiv -1 \bmod \dot{R}^2$ se tiene que q es isótropa). En Q_5 se tiene que $q = \langle 1, 2\rangle \perp 5 \cdot \langle 1, -2\rangle$, luego $\bar{q}_1 = \langle 1, 2\rangle$ y $\bar{q}_2 = \langle 1, -2\rangle$ son las formas residuales en WZ_5. Es fácil verificar en forma directa que $\bar{q}_1$ y $\bar{q}_2$ son anisótropas sobre Z_5, por lo tanto, aplicando la proposición 4 b) se tiene que q es anisótropa sobre Q_5. Si $d \in \dot{Q}$, la forma $\langle 1, 2, 5, -10, -d\rangle$ es isótropa sobre Q desde que lo es sobre R (corolario 3), en consecuencia existen x_i, $i = 1, \ldots, 5$, en Q, no todos nulos tales que:

$$x_1^2 + 2x_2^2 + 5x_3^2 - 10x_4^2 = d x_5^2.$$

Si $x_5 = 0$ resultaría q isótropa sobre Q, contrario a lo demostrado ya, por lo tanto $x_5 \neq 0$ y q representa d, esto es q es universal.

Ejemplo 8. La forma $q = \langle 3, 5, -7, 11\rangle$ es isótropa sobre Q. Sobre R es inmediato ver que q es isótropa. También, como la forma $\langle 3, 5, -7\rangle$ es isótropa sobre Q_p, si $p \neq 3, 5, 7$ se tiene que q es isótropa sobre Q_p, $p \neq 3, 5, 7$. En el caso $p = 3$ se observa que $q = \langle 5, -7, 11\rangle \perp 3 \cdot \langle 1\rangle$ tiene su primera forma residual isótropa (desde que 5, -7 y 11 son unidades en Q_3), por lo tanto q es isótropa sobre Q_3. De modo análogo, q es isótropa sobre Q_5 y Q_∞, por lo tanto, aplicando el teorema de Hasse-Minkowski tenemos que q es isótropa sobre Q.

APÉNDICE A. LA APLICACIÓN TRAZA

En el capítulo 2 se ha hecho uso de algunas propiedades de la *traza* en extensiones separables de grado finito. En este Apéndice, para facilitar la lectura, se desarrollará en forma breve y restringida los conceptos necesarios para la comprensión de los temas expuestos relacionados con la aplicación traza.

Sean A una F-álgebra de dimensión finita y $x \in A$ un elemento arbitrario. Sabemos que $T_x: A \to A$, definido por $T_x(a) = x \cdot a \ \forall\, a \in A$, es un F-endomorfismo del espacio vectorial A. Se define la traza de T_x como la traza de la matriz de T_x en una base cualquiera de A. Definimos entonces $T: A \to F$ por $T(x) = \text{traza}(T_x)$. T se denota usualmente por $T_{A/F}$ y se denomina la *aplicación traza de* A.

Supongamos que K/F es una extensión de cuerpos de grado finito, separable. Existe un $x \in K$ tal que $K = F(x)$. Puede verse de inmediato que si $X^n - a_1X^{n-1} + \ldots + (-1)^n a_n$ es el F-polinomio minimal de x, entonces $T_{K/F}(x) = a_1 = \varphi_1(x) + \ldots + \varphi_n(x)$, donde $\varphi_1, \ldots, \varphi_n$ son las diferentes F-inmersiones de K en su clausura algebraica. Más generalmente, supongamos que deseamos calcular la traza $T_{K/F}(y)$ para $y \in K$. Sea $X^m - b_1X^{m-1} + \ldots + (-1)^m b_m$ su F-polinomio minimal. Sea $w \in K$ tal que $K = F(y)(w)$, entonces una F-base del espacio K es:

$$\{1, y, \ldots, y^{m-1}, w, \ldots, w^{r-1}, yw, \ldots, yw^{r-1}, \ldots, y^{m-1}w^{r-1}\},$$

donde $r \cdot m = [K:F]$. Calculando directamente en relación con la base la matriz de T_y se encuentra que $T_{K/F}(y) = rb_1$. Se observa que rb_1 es $\varphi_1(y) + \ldots + \varphi_n(y)$ (porque las inmersiones φ_j se obtienen como composición de las m inmersiones distintas de $F(y)$ sobre F, en la clausura algebraica, con las r inmersiones de K sobre $F(y)$). Tenemos luego que si K/F es una extensión separable de grado finito la aplicación traza $T_{K/F}: K \to F$ es tal que $T_{K/F}(x) = \varphi_1(x) + \ldots + \varphi_n(x) \ \forall\, x \in K$.

Se define la aplicación *norma* de K sobre F, denotada por $N_{K/F}: K \to F$, por $N_{K/F}(x) = \varphi_1(x) \ldots \varphi_n(x) \ \forall\, x \in K$, donde $\varphi_1, \ldots, \varphi_n$ denotan todas las distintas inmersiones de K sobre F en una clausura algebraica.

Observaciones: Denotemos por Ω una clausura algebraica de F fija.

a) $T_{K/F}: K \to F$ es una aplicación F-lineal y $N_{K/F}: \dot{K} \to \dot{F}$ es un homomorfismo de grupos multiplicativos, donde $a \to T_{K/F}(a)$ y $a \to N_{K/F}(a)$ son las aplicaciones definidas.

b) Si $K = F(\sqrt{d})$ es una extensión cuadrática y como las F-inmersiones de K en Ω son la identidad sobre K y $x + y\sqrt{d} \to x - y\sqrt{d}$, se tiene:

$$T_{K/F}(x + y\sqrt{d}) = (x + y\sqrt{d}) + (x - y\sqrt{d}) = 2x$$

$$N_{K/F}(x + y\sqrt{d}) = x^2 - dy^2.$$

Proposición A.1. Sean $f_1, \ldots, f_n \neq$ a morfismo de cuerpo de K en L. Entonces $a_1 f_1(x) + \ldots + a_n f_n(x) = 0$, $\forall\, x \in K$, $a_i \in L$, implica, $a_1 = \ldots = a_n = 0$, es decir $f_1, \ldots, f_n$ son L-linealmente independientes.

Demostración. Por inducción sobre n. Si $n = 1$, es $a_1 f_1(x) = 0$, $\forall\, x$, luego $a_1 f_1(1) = 0$, entonces $a_1 = 0$. Supongamos $n > 1$ y que la proposición es válida para $n - 1$ morfismos. En $a_1 f_1(x) + \ldots + a_n f_n(x) = 0$ podemos suponer todos los $a_j \neq 0$, ya que en caso contrario concluimos por la hipótesis inductiva. Luego existe un $c \in K$ tal que $f_1(c) \neq f_n(c)$ y entonces de $\sum_{i=1}^{n} a_i f_i(x) = 0$ se sigue que $\sum_{i=1}^{n} a_n^{-1} f_n(c^{-1}) a_i f_i(c) f_i(x) = 0$ y también $\sum_{i=1}^{n} a_n^{-1} a_i f_i(x) = 0$. Restando esta expresión de la anterior se observa que el n-ésimo término de la sumatoria es cero y obtenemos:

$$\sum_{i=1}^{n} a_n^{-1} a_i (f_i(c) f_n(c^{-1}) - 1) f_i(x) = 0.$$

Entonces, por la hipótesis inductiva, es $f_i(c) f_n(c)^{-1} = 1$, en particular $f_1(c) f_n(c)^{-1} = 1$, luego $f_1(c) = f_n(c)$, lo que es contrario a la elección de c, en consecuencia todos los a_i son cero.

Corolario A.2. Sea K/F una extensión algebraica, separable de grado finito n, entonces $T_{K/F}: K \to F$ es una aplicación F-lineal no nula.

Demostración. Sean $f_1, \ldots, f_n$ las $\neq$ a F-inmersiones de K en la clausura algebraica de F, entonces $T_{K/F} = f_1 + \ldots + f_n$, y por la proposición anterior, no puede ser $T_{K/F}$ idénticamente nula.

Corolario A.3. Sea K/F una extensión separable de grado finito, $T_r: K \times K \to F$, aplicación definida por $T_r(x, y) = T_{K/F}(x \cdot y)$, entonces (K, T_r) es un F-espacio cuadrático regular.

Demostración. Por el corolario A.2, existe un x_0 tal que $T_{K/F}(x_0) \neq 0$. Sea $y \in K$ tal que $T_r(x, y) = 0$, si $y \neq 0$ sea $x = x_0 y^{-1}$, entonces $0 = T_r(x_0 y^{-1}, y) = T_{K/F}(x_0)$ es una contradicción.

APÉNDICE B. TEOREMA CHINO DEL RESTO

Sea A un anillo conmutativo con unidad $1 \neq 0$. Si I y J son ideales de A se dicen comaximales, si $I + J = A$. Sabemos que si $J_1, \ldots, J_n$ es una familia finita de ideales, entonces $J_1 \ldots J_n \subset J_1 \cap J_2 \cap \ldots \cap J_n$. Aún más si los ideales J_i son comaximales dos a dos, entonces se cumple la otra inclusión, esto es la igualdad.

Teorema "Chino" del Resto. Sean A un anillo conmutativo con unidad, y $J_1, \ldots, J_n$ ideales comaximales dos a dos. Dados $x_1, \ldots, x_n \in A$, entonces existe $x \in A$ tal que $x_i \equiv x$ mód(J_i) para $i = 1, \ldots, n$.

Demostración. Se hace por inducción. Si $n = 2$, como $J_1 + J_2 = A$, entonces $1 = a_1 + a_2$, con $a_i \in J_i$. Tomemos entonces $x = a_1x_2 + a_2x_1$ y se verifica lo pedido. Sean $n \geq 2$ y el teorema válido para $n - 1$ ideales comaximales dos a dos. Dado J_1 y J_i con $i \neq 1$, podemos encontrar $b_i \in J_i$ y $a_i \in J_1$ tales que $1 = a_i + b_i$ para $i = 2, \ldots, n$, luego $b_i = 1 - a_i$, entonces $\pi b_i = \pi(1 - a_i)$, lo que implica que J_1 y $J_2 \ldots J_n$ son comaximales, y considerando 1, 0 en A, aplicamos el caso $n = 2$ ya demostrado y encontramos un $z_1 \in A$ tal que $z_1 \equiv 1$ mód J_1 y $z_1 \equiv 0$ mód $J_2 \ldots J_n$. Repitiendo el proceso encontramos $z_2, \ldots z_r$ tales que $z_j \equiv$ mód J_j y $z_j \equiv 0$ mód(J_i), si $i \neq j$. Ahora bastará definir el elemento $x = x_1z_1 + \ldots + x_nz_n$ para tener el elemento buscado.

Corolario B.2.2. Con las mismas hipótesis que el teorema anterior, se tiene el siguiente isomorfismo:

$$\frac{A}{J_1 \ldots J_n} \approx \frac{A}{J_1 \cap J_2 \cap \ldots \cap J_n} \approx \prod_{i=1}^{n} A/J_i$$

Demostración. Es inmediata.

BIBLIOGRAFÍA

(1) ELMAN, R. y LAM, T.Y. "Quadratic Forms Over Formally Real Fields and Pythagoreans Fields", *Amer. J. Math.*, **94**, 1155-1194 (1972).

(2) ELMAN, R., LAM, T.Y. y WADSWORTH, A. Amenables Fields and Pfister Extension, Conference of Quadratic Forms, 1976, Queen's University, Canada, 445-481 (1977).

(3) ELMAN, R., LAM, T.Y. y WADSWORTH, A. "Orderings Under Field Extensions", *J. Reine Angew. Math.*, **7**, 27-306 (1979).

(4) GENTILE, E.R. Estructuras Algebraicas I, monografía no. 3, Serie de Matemática, OEA, Washington, D.C., 131 págs. (1977).

(5) GENTILE, E.R. Estructuras Algebraicas II, monografía no. 12, Serie de Matemática, OEA, Washington, D.C., 160 págs. (1971).

(6) GENTILE, E.R. y SHAPIRO, D.B. Conservative Quadratic Forms, *Math. Zeit.*, Springer-Verlag, 163, 15-23 (1978).

(7) HORVÁTH, J. Introducción a la Topología General, monografía no. 9, Serie de Matemática, OEA, Washington, D.C., 147 págs. (1969).

(8) KNEBUSCH, M. a) Generic Splitting of Quadratic Forms, I, II, *Proc. London Math. Soc., Ser. 3*, **33**, 65-93, (1976). b) *Ser. 4*, 1-31 (1977).

(9) LAM, T.Y. The Algebraic Theory of Quadratic Forms, Benjamin, Nueva York, N.Y., 343 págs. (1973).

(10) LAM, T.Y. Ten Lectures on Quadratic Forms Over Fields, Conference of Quadratic Forms, 1976, Queen's University, Canadá, 1-102 (1977).

(11) MERKLEN, H.A. Estructuras Algebraicas V (Teoría de Cuerpos), monografía no. 22, Serie de Matemática, OEA, Washington, D.C., 104 págs. (1979).

(12) MICALI, A. y VILLAMAYOR, O.E. Estructuras Algebraicas IV, monografía no. 16, Serie de Matemática, OEA, Washington, D.C., 78 págs. (1976).

(13) PFISTER, A. Quadratische Formen in beliebigen Körpern, *Invent. Math.*, 1, 116-132 (1966).

(14) PRESTEL, A. Lectures on Formally Real Fields, IMPA, Río de Janeiro, Brasil, 22, 181 págs. (1975).

(15) WARE, R. A Note on Quadratic Forms Over Pythagorean Fields, *J. Math.*, 58, 651-654 (1975).

(16) WARE, R. Some Remarks on the Map Between Witt Rings of an Algebraic Extension, Conference on Quadratic Forms, 1976, Queen's University, Canada, 634-649 (1977).

(17) O'MEARA, O. T. Introduction to Quadratics Forms, Academic, Nueva York, N. Y., 341 págs. (1963).

(18) CASSELS, J. W. S. Rational Quadratic Forms, Academic, Nueva York, N. Y. (1980).

(19) GENTILE, E. R. Aspectos Históricos de la Teoría Algebraica de Formas Cuadráticas y Cuerpos Ordenados. Trabajos de Matemática, 1981. Instituto Argentino de Matemática, Buenos Aires, Argentina.

(20) KNEBUSCH, M. y SCHARLAU, W. Algebraic Theory of Quadratic Forms, Generic Methods and Pfister Forms, Birkhäuser, Boston (1980).

(21) LAM, T. Y. The Theory of Real Fields, Proceedings of the Algebra and Ring Theory Conference, University of Oklahoma, Dekker, Nueva York, N. Y. (1980).

ÍNDICE DE NOTACIONES

Notación		Página
F	Cuerpo de característica $\neq 2$	
$\simeq$	Equivalencia de formas	5
(V, B)	Espacio cuadrático	7
$D_F(f)$	Elemento representado por f	10
$d(f)$, $\det(f)$	Determinante de f	11
$f = \langle d_1, \ldots, d_n \rangle$	Representación diagonal de f	11
$V_1 \perp V_2$	Suma ortogonal de espacios cuadrados	14
$H = \langle 1, -1 \rangle$	Plano hiperbólico	15
WF	Anillo de Witt	17
$f \otimes g$	Producto tensorial de formas	17
f_a	Parte anisótropa de f	17
$n\langle 1 \rangle$	Suma ortogonal $\langle 1 \rangle \perp \ldots \perp \langle 1 \rangle$ (n-sum.)	20
IF	Ideal de WF de las formas pares	21
$\ll a_1, \ldots, a_n \gg$	n-forma de Pfister	21
f'	Parte pura de la forma de Pfister f	22
$G_F(f)$	Grupo de isotropía de f	23
f_K	f como K-forma	31
$W(K/F)$	Núcleo de $r: WF \to WK$	32
(V, SB)	"Transferencia" de (V, B) por S	32
$\mathrm{Sig}_P(f)$	Signatura de f respecto de P	46
O_F	Espacio de órdenes de F	53
$\hat{f}$	Signatura total de f	54

Notación		Página
$H(a_1, \ldots, a_n)$	Abierto básico en la topología de O_F	57
$\mathcal{F}(\mathcal{J})$	Cuerpo de funciones de $\mathcal{J}$	71
$o(G)$	Orden del grupo G	
$\approx$	Isomorfismo	
$Nu(\varphi)$	Núcleo del homomorfismo φ	

ÍNDICE DE TÉRMINOS

	Página
Álgebra de cuaterniones	24
Anillo de Witt	17
Arason-Pfister (Hauptsatz)	72
Cápsula pitagórica	61
Clausura real	49
Cono positivo	44
Correspondencia Harrison-Lorentz-Leicht	54
Cuerpo cerrado real	48
Cuerpo euclidiano	46
Cuerpo pitagórico	38
Cuerpo superpitagórico	64
Cuerpo de funciones	71
Equivalencia en cadena	29
Espacio cuadrático	7
Espacios isométricos	8
Espacio de órdenes	53
Extensión de órdenes	47
Extensiones excelentes	39
Formas de Pfister	21
Forma definida positiva	47
Formas isótropas, anisótropas	9
Grupo de isotropía	23

	Página
Ley de Sylvester-Pfister	58
Longitud de un elemento	69
Nivel de un cuerpo	74
Principio local-global de Pfister	57
Signatura	46
Signatura total	54
Suma ortogonal	14
Teorema de cancelación	17
Teorema de descomposición	17
Teoremas de Cassels-Pfister	67
Teorema de Springer	34
Teorema de Springer para cuerpos locales	79
Teorema "Chino del resto"	87
Teorema de la subforma	69
Teorema de la subforma pura	22
Topología de Harrison	54
Topología de Zariski	60
Teorema de Hasse-Minkowski	82
Transferencia de Scharlau	32
Traza (aplicación de)	85

COLECCIÓN DE MONOGRAFÍAS CIENTÍFICAS

Publicadas

Serie de matemática

N° 1. La Revolución en las Matemáticas Escolares, por el Consejo Nacional de Maestros de Matemáticas de los Estados Unidos de América.
N° 2. Espacios Vectoriales y Geometría Analítica, por Luis A. Santaló.
N° 3. Estructuras Algebraicas I, por Enzo R. Gentile.
N° 4. Historia de las Ideas Modernas en la Matemática, por José Babini.
N° 5. Álgebra Lineal, por Orlando E. Villamayor.
N° 6. Algebra Linear e Geometria Euclidiana, por Alexandre Augusto Martins Rodrigues.
N° 7. El Concepto de Número, por César A. Trejo.
N° 8. Funciones de Variable Compleja, por José I. Nieto.
N° 9. Introducción a la Topología General, por Juan Horváth.
N° 10. Funções Reais, por Djairo G. de Figueiredo.
N° 11. Probabilidad e Inferencia Estadística, por Luis A. Santaló.
N° 12. Estructuras Algebraicas II (Álgebra Lineal), por Enzo R. Gentile.
N° 13. La Revolución en las Matemáticas Escolares (Segunda Fase), por Howard F. Fehr, John Camp y Howard Kellog.
N° 14. Estructuras Algebraicas III (Grupos Finitos), por Horacio H. O'Brien.
N° 15. Introducción a la Teoría de Grafos, por Fausto A. Toranzos.
N° 16. Estructuras Algebraicas IV (Álgebra Multilineal), por Artibano Micali y Orlando E. Villamayor.
N° 17. Introdução a Análise Funcional: Espaços de Banach e Cálculo Diferencial, por Leopoldo Nachbin.
N° 18. Introducción a la Integral de Lebesgue en la Recta, por Juan Antonio Gatica.
N° 19. Introducción a los Espacios de Hilbert, por José I. Nieto.
N° 20. Elementos de Biomatemática, por Alejandro B. Engel.
N° 21. Introducción a la Computación, por Jaime Michelow.
N° 22. Estructuras Algebraicas V (Teoría de Cuerpos), por Héctor A. Merklen.
N° 23. Estructuras Algebraicas VI (Formas Cuadráticas), por Francisco M. Piscoya.

Serie de física

N° 1. Concepto Moderno del Núcleo, por D. Allan Bromley.
N° 2. Panorama de la Astronomía Moderna, por Félix Cernuschi y Sayd Codina.
N° 3. La Estructura Electrónica de los Sólidos, por Leopoldo M. Falicov.
N° 4. Física de Partículas, por Igor Saavedra.
N° 5. Experimento, Razonamiento y Creación en Física, por Félix Cernuschi.

N° 6. Semiconductores, por George Bemski.
N° 7. Aceleradores de Partículas, por Fernando Alva Andrade.
N° 8. Física Cuántica, por Onofre Rojo y Harold V. McIntosh.
N° 9. La Radiación Cósmica, por Gastón R. Mejía y Carlos Aguirre.
N° 10. Astrofísica, por Carlos Jaschek y Mercedes C. de Jaschek.
N° 11. Ondas, por Oscar J. Bressan y Enrique Gaviola.
N° 12. El Láser, por Mario Garavaglia.
N° 13. Teoría Estadística de la Materia, por Antonio E. Rodríguez y Roberto E. Caligaris.
N° 14. Aplicações da Teoria de Grupos na Espectroscopia Raman e do Infra-Vermelho, por Jorge Humberto Nicola y Anildo Bristoti.

Serie de química

N° 1. Cinética Química Elemental, por Harold Behrens LeBas.
N° 2. Bioenergética, por Isaias Raw y Walter Colli.
N° 3. Macromoléculas, por Alejandro Paladini y Moises Burachik.
N° 4. Mecanismo de las Reacciones Orgánicas, por Jorge A. Brieux.
N° 5. Elementos Encadenados, por Jacobo Gómez Lara.
N° 6. Enseñanza de la Química Experimental, por Francisco Giral.
N° 7. Fotoquímica de Gases, por Ralf-Dieter Penzhorn.
N° 8. Introducción a la Geoquímica, por Félix González-Bonorino.
N° 9. Resonancia Magnética Nuclear de Hidrógeno, por Pedro Joseph-Nathan.
N° 10. Cromatografía Líquida de Alta Presión, por Harold M. McNair y Benjamín Esquivel H.
N° 11. Actividad Óptica, Dispersión Rotatoria Óptica y Dicroísmo Circular en Química Orgánica, por Pierre Crabbé.
N° 12. Espectroscopia Infrarroja, por Jesús Morcillo Rubio.
N° 13. Polarografía, por Alejandro J. Arvía y Jorge A. Bolzan.
N° 14. Paramagnetismo Electrónico, por Juan A. McMillan.
N° 15. Introducción a la Estereoquímica, por Juan A. Garbarino.
N° 16. Cromatografía en Papel y en Capa Delgada, por Xorge A. Domínguez.
N° 17. Introducción a la Espectrometría de Masa de Sustancias Orgánicas, por Otto R. Gottlieb y Raimundo Braz Filho.
N° 18. Cinética Química, por Rodolfo V. Caneda.
N° 19. Fuerzas Intermoleculares, por Mateo Díaz Peña.
N° 20. Físico-Química de Superficies, por Tibor Rabockai.
N° 21. Corrosión, por José R. Galvele.
N° 22. Introducción a la Electroquímica, por Dionisio Posadas.

Serie de biología

N° 1. La Genética y la Revolución en las Ciencias Biológicas, por José Luis Reissig.
N° 2. Bases Ecológicas de la Explotación Agropecuaria en la América Latina, por Guillermo Mann F.
N° 3. La Taxonomía y la Revolución en las Ciencias Biológicas, por Elías R. de la Sota.

N° 4. Principios Básicos para la Enseñanza de la Biología, por Oswaldo Frota-Pessoa.
N° 5. A Vida da Célula, por Renato Basile.
N° 6. Microorganismos, por J. M. Gutiérrez-Vázquez.
N° 7. Principios Generales de Microbiología, por Norberto J. Palleroni.
N° 8. Los Virus, por Enriqueta Pizarro-Suárez y Gamba.
N° 9. Introducción a la Ecología del Bentos Marino, por Manuel Vegas Vélez.
N° 10. Biosíntesis de Proteínas y el Código Genético, por Jorge E. Allende.
N° 11. Fundamentos de Inmunología e Inmunoquímica, por Félix Córdoba Alva y Sergio Estrada-Parra.
N° 12. Bacteriófagos, por Romilio Espejo T.
N° 13. Biogeografía de América Latina, por Angel L. Cabrera y Abraham Willink.
N° 14. Relación Hospedante-Parásito. Mecanismo de Patogenicidad de los Microorganismos, por Manuel Rodríguez-Leiva.
N° 15. Genética de Poblaciones Humanas, por Francisco Rothhammer.
N° 16. Introducción a la Ecofisiología Vegetal, por Ernesto Medina.
N° 17. Aspectos de Biología Celular y la Transformación Maligna, por Manuel Rieber.
N° 18. Transporte a Través de la Membrana Celular, por P. J. Garrahan y A. F. Rega.
N° 19. Duplicación Cromosómica y Heterocromatina a Nivel Molecular y Citológico, por Néstor O. Bianchi.
N° 20. Citogenética Básica y Biología de los Cromosomas, por Francisco A. Sáez y Horacio Cardoso.
N° 21. Ecología de Poblaciones Animales, por Jorge E. Rabinovich.

En preparación

Serie de matemática

Estructuras Algebraicas VII (Estructuras de Álgebras), por Artibano Micali.

Serie de física

Teoría de Fluidos en Equilibrio, por Antonio E. Rodríguez y Roberto E. Caligaris.
Geofísica, por Alvaro F. Espinosa.
Superconductividad, por Miguel Kiwi.
Efecto Mössbauer, por Jacques A. Dannon
Elementos de Cristalografía Física, por Jaime Rodríguez Lara.
Introducción a la Espectroscopia Atómica por Mario Garavaglia y Athos Giacchetti.
Aplicaciones Metrológicas del Láser, por Mario Garavaglia.

Serie de química

Síntesis Orgánica, por Eduardo Sánchez.
Catálisis Homogénea, por Eduardo Humeres A.

Catálisis Heterogénea, por Sergio Droguett.
Cromatografía de Gases, por Harold M. McNair.
Fisicoquímica de Interfases, por Francisco Javier Garfias.
Química de Suelos, por Elemer u. Bornemisza
Introducción a la Metalurgia Física, por Joaquín Hernández Marín.
Cinética de Disolución de Medicamentos, por Edison Cid Cárcamo.
Introducción a la Electrocatálisis, por Alejandro J. Arvía y María Cristina Giordano.

Serie de biología

Etología: El Estudio del Comportamiento Animal, por Raúl Vaz-Ferreira.
Análisis de Sistemas en Ecología, por Gilberto C. Gallopín.
Comportamiento y Aprendizaje, por Héctor Maldonado y Josué A. Núñez.
Principios Básicos de la Contracción Muscular, por Carlos Caputo.
Germinación, por Luiz Gouvêa Laboriau.
Clastogénesis y Contaminación Ambiental, por Fernando Noel Dolout.
Fotosíntesis, por Rubén H. Vallejos.
Introducción a la Teoría y Práctica de la Taxonomía Numérica, por Jorge V. Crisci.
Cromosomas Humanos y de Primates, por Máximo E. Drets y Héctor Seuanez.
Metodología para la Descripción y el Análisis de la Vegetación, por Silvia D. Matteucci y Aída Colma.
Diferenciación Celular, por Roberto B. García y Susana Pereyra-Alfonso.

Nota: Las personas interesadas en adquirir estas obras deben dirigirse a la Unidad de Ventas y Promoción, Organización de los Estados Americanos, Washington, D.C., 20006 o a las Oficinas de la OEA en el país respectivo.