TEOREMA DE WITT

JUAN HERMO ÁLVAREZ Y MARÍA JESÚS VALE GONSALVES

1. Introducción

En este trabajo se introducen los conceptos fundamentales de la teoría de espacios ortogonales sobre un cuerpo K de característica distinta de 2. Se prueba el teorema de Witt que afirma que toda isometría entre dos subespacios de un espacio ortogonal V se puede extender a una isometría de V y a partir de este teorema se prueban la ley de cancelacion y el teorema de descomposición de Witt. Se definen invariantes que permiten clasificar los espacios ortogonales sobre un cuerpo K, si K es cuadráticamente cerrado o bien es euclidiano o pitagórico o si se trata de un cuerpo finito. Se calcula el grupo de Witt de K en estos casos.

2. Preliminares

2.1. Espacios vectoriales ortogonales

Sea V un espacio vectorial de dimensión $n \geq 0$ sobre el cuerpo K.

Definición 2.1. Se dice que una aplicación $\sigma\colon V \times V \to K$ es una *aplicación bilineal simétrica* o una *forma bilineal simétrica* en V si verifica las siguientes condiciones:

(1) $\sigma(\lambda_1 v_1 + \lambda_2 v_2, w) = \lambda_1 \sigma(v_1, w) + \lambda_2 \sigma(v_2, w),\ v_1, v_2, w \in V,\ \lambda_1, \lambda_2 \in \mathbb{R}$.

(2) $\sigma(v, \lambda_1 w_1 + \lambda_2 w_2) = \lambda_1 \sigma(v, w_1) + \lambda_2 \sigma(v, w_2),\ v, w_1, w_2 \in V,\ \lambda_1, \lambda_2 \in \mathbb{R}$.

(3) $\sigma(v, w) = \sigma(w, v),\ v, w \in V$

Si σ es una aplicación bilineal, denotaremos con frecuencia $\sigma(u, v)$ por $u \cdot v$ y $v \cdot v$ por v^2.

Un espacio ortogonal es un par (V, σ), donde V es un espacio vectorial sobre K y $\sigma\colon V \times V \to K$ es una forma bilineal simétrica. Lo denotaremos por (V, σ) o simplemente por V.

Denotaremos por $M_n(K)$ el conjunto de matrices $n \times n$ sobre K.

Definición 2.2. Sea $\sigma\colon V \times V \to K$ una forma bilineal simétrica en V y sea $B = \{v_1, \ldots, v_n\}$ una base de V. Se llama *matriz de Gram* de σ respecto a la base B a la matriz simétrica

$$G_\sigma^B = \begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ \vdots & \vdots & & \vdots \\ g_{n1} & g_{n2} & \cdots & g_{nn} \end{pmatrix} = (g_{ij}) \in M_n(K)$$

donde $g_{ij} = v_i \cdot v_j\,,\ i, j = 1, \ldots, n$.

Proposición 2.3. *Sea $\sigma\colon V \times V \to K$ una forma bilineal simétrica en V y sea $B = \{v_1, \dots v_n\}$ una base de V. Sean $v = x_1v_1 + \dots + x_nv_v$, $w = y_1v_1 + \dots + y_nv_n$ vectores de V y $G_\sigma^B = (g_{ij})$ la matriz de Gram de σ respecto a B. Se tiene:*

$$\sigma(v,w) = \sum_{i,j=1}^{n} g_{ij}\, x_i\, y_j = \begin{pmatrix} x_1 & \dots & x_n \end{pmatrix} G_\sigma^B \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

Proposición 2.4. *Sean $B = \{v_1, \dots, v_n\}$ una base de V y $v = x_1v_1 + \dots + x_nv_n$, $w = y_1v_1 + \dots + y_nv_n$ vectores de V. Sea $A = (a_{ij}) \in M_n(K)$ una matriz simétrica. La aplicación $\sigma_A\colon V \times V \to K$ dada por :*

$$\sigma_A(v,w) = \sum_{i,j=1}^{n} a_{ij}x_iy_i = \begin{pmatrix} x_1 & \dots & x_n \end{pmatrix} A \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

es una forma bilineal simétrica en V cuya matriz de Gram respecto a la base B es la matriz A.

Proposición 2.5. *Sean $B = \{v_1, \dots v_n\}$ y $B' = \{v_1', \dots v_n'\}$ bases de V y sea $\sigma\colon V \times V \to K$ una forma bilineal simétrica. Sea $P = 1_{B'B} = (p_{ij})$ la matriz de cambio de base de B' a de B,*

$$v_i' = \sum_{j=1}^{n} p_{j\,i}\, v_j,\ i = 1, \dots, n.$$

Entonces se tiene

$$G_\sigma^{B'} = P^t\, G_\sigma^B\, P$$

siendo P^t la matriz traspuesta de la matriz P.

Sea K^* el grupo multiplicativo de los elementos de no cero de K. Puesto que K^* es un grupo abeliano con el producto, el conjunto de sus cuadrados

$$K^{*2} = \{x^2 \mid x \in K^*\}$$

es un subgrupo de K^* y podemos formar el grupo cociente K^*/K^{*2}. La igualdad

$$\det G_\sigma^{B'} = (\det G_\sigma^B)(\det P)^2$$

demuestra que la clase $(\det G_\sigma^B)\, K^{*2}$ no depende de la base considerada, es decir

$$(\det G_\sigma^{B'})\, K^{*2} = (\det G_\sigma^B)\, K^{*2}$$

Definición 2.6. Si (V, σ) es un espacio ortogonal no singular se llama *discriminante* de (V, σ) y se denota por $\operatorname{disc}(V, \sigma)$ o $\operatorname{disc}(V)$ a la clase $(\det G_\sigma^B)\, K^{*2}$, donde B es una base cualquiera de V.

Definición 2.7. Sean $A, B \in M_n(K)$. Se dice que las matrices A y B son *congruentes* si existe una matriz regular $P \in M_n(K)$ tal que

$$P^t\, A\, P = B$$

***Observación* 2.8.** La relación "ser congruentes" es una relación de equivalencia en el conjunto de matrices $M_n(K)$.

Proposición 2.9. *Si $A, B \in M_n(K)$ son matrices congruentes entonces tienen igual rango.*

Demostración. Dos matrices congruentes son equivalentes y por lo tanto, tienen el mismo rango. □

Definición 2.10. Se llama *rango* de una forma bilineal simétrica $\sigma\colon V \times V \to K$ al rango de la matriz de Gram G_σ^B de σ respecto a una base B cualquiera de V,

$$\operatorname{rango} \sigma := \operatorname{rango} G_\sigma^B$$

***Observación* 2.11.** De las proposiciones 2.5 y 2.9 se sigue que el rango de σ no depende de la base considerada en V.

Definición 2.12. Se dice que un espacio ortogonal (V, σ) es *no singular* si el rango de σ coincide con la dimensión de V.

2.2. Isometrías

Definición 2.13. Sean (V,σ) y (V', σ') espacios ortogonales sobre K. Se dice que una aplicación $f\colon V \to V'$ es una *isometría* si verifica

(1) f es un isomorfismo de espacios vectoriales sobre K.

(2) $v \cdot w = f(v) \cdot f(w)$, $v, w \in V$.

Si existe una isometría $f\colon V \to V'$ entonces se dice que (V, σ) y (V', σ') son espacios vectoriales ortogonales *isométricos*.

Propiedades 2.14. (1) *Si (V, σ) es un espacio ortogonal sobre K, entonces la aplicación $1_V\colon V \to V$ es una isometría.*

(2) *Si (V_1, σ_1), (V_2, σ_2) y (V_3, σ_3) son espacios ortogonales sobre K y $f_1\colon V_1 \to V_2$ y $f_2\colon V_2 \to V_3$ son isometrías, entonces $f_1 \circ f_2\colon V_1 \to V_3$ es una isometría.*

(3) *Si (V, σ) y (V', σ') son espacios ortogonales sobre K y $f\colon V \to V'$ es una isometría, entonces $f^{-1} : V' \to V$ es una isometría.*

Proposición 2.15. *Sean (V, σ) y (V', σ') espacios ortogonales sobre K de dimensión n, $B = \{v_1, \dots v_n\}$ una base de V y $f\colon V \to V'$ un isomorfismo de espacios vectoriales. Se tiene que f es una isometría si y sólo si $v_i \cdot v_j = f(v_i) \cdot f(v_j)$, $i, j = 1, \dots, n$.*

Demostración. Si f es una isometría, entonces $v_i \cdot v_j = f(v_i) \cdot f(v_j)$, $i, j = 1, \dots, n$.

Recíprocamente, supongamos que $v_i \cdot v_j = f(v_i) \cdot f(v_j)$, $i, j = 1, \dots, n$. Sean $v = x_1 v_1 + \ldots + x_n v_n$ y $w = y_1 v_1 + \ldots + y_n v_n$ vectores de V. Se tiene

$$f(v) \cdot f(w) = (\sum_{i=1}^{n} x_i v_i) \cdot (\sum_{i=1}^{n} y_i v_i) = \sum_{i,j=1}^{n} x_i y_j f(v_i) \cdot f(v_j) = \sum_{i,j=1}^{n} x_i y_j v_i \cdot v_j = v \cdot w$$

□

Teorema 2.16. *Sean (V, σ) y (V', σ') espacios ortogonales sobre K de dimensión n. Son equivalentes*

(1) *(V, σ) y (V', σ') son isométricos.*

(2) *Existen bases B de V y B' de V' tales que las matrices de Gram de σ respecto a B y de σ' respecto a B' coinciden, es decir, tales que $G_\sigma^B = G_{\sigma'}^{B'}$*

Demostración. (1) $\Rightarrow$ (2) Sea $f\colon V \to V'$ una isometría. Si B es una base de V, entonces $G_\sigma^B = G_{\sigma'}^{f(B)}$.

(2) $\Rightarrow$ (1) Sean $B = \{v_1, \ldots, v_n\}$ y $B' = \{v_1', \ldots, v_n'\}$ bases de V y V', respectivamente, y tales que $G_\sigma^B = G_{\sigma'}^{B'}$. Sea $f\colon V \to V'$ el isomorfismo de espacios vectoriales dado por $f(v_i) = v_i'$, $i = 1, \ldots, n$. De la igualdad $G_\sigma^B = G_{\sigma'}^{f(B)}$ se sigue que $f(v_i) \cdot f(v_j) = v_i \cdot v_j$, para $i, j = 1, \ldots, n$. Por la proposición 2.15, f es una isometría. □

Corolario 2.17. *Sean (V, σ) y (V', σ') espacios ortogonales sobre K de dimensión n. Sea B una base de V y sea B' una base de V'. Se verifica que (V, σ) y (V', σ') son isométricos si, y solo si, las matrices de Gram G_σ^B y $G_{\sigma'}^{B'}$ son congruentes.*

Demostración. Si $f\colon V \to V'$ es una isometría, entonces $G_\sigma^B = G_{\sigma'}^{f(B)}$. Por la proposición 2.5, las matrices $G_{\sigma'}^{f(B)}$ y $G_{\sigma'}^{B'}$ son congruentes. Así, las matrices G_σ^B y $G_{\sigma'}^{B'}$ son congruentes.

Recíprocamente, dado que G_σ^B y $G_{\sigma'}^{B'}$ son congruentes, existe una matriz regular P tal que

$$G_{\sigma'}^{B'} = P^t\, G_\sigma^B\, P.$$

Sea $\bar{B}$ la base de V tal que $P = 1_{\bar{B}B}$. Por la proposición 2.5, $P^t\, G_\sigma^B\, P = G_\sigma^{\bar{B}}$. Por tanto $G_\sigma^{\bar{B}} = G_{\sigma'}^{B'}$ y utilizando el teorema 2.16 se tiene que (V, σ) y (V', σ') son isométricos. □

Proposición 2.18. *Si dos espacios ortogonales no singulares son isométricos, entonces tienen igual discriminante.*

Demostración. Se sigue del corolario anterior. □

***Observación* 2.19.** Dos espacios ortogonales de igual discriminante no son, en general, isométricos ni siquiera en el caso de tener igual dimensión. Por ejemplo, consideremos en $\mathbb{R}^2$ las formas bilineales σ y σ' cuyas matrices de Gram en la base canónica C son

$$G_\sigma^C = \operatorname{diag}(1, 1), \quad G_{\sigma'}^C = \operatorname{diag}(-1, -1),$$

Se tiene que $\operatorname{disc}(\mathbb{R}^2, \sigma) = \operatorname{disc}(\mathbb{R}^2, \sigma') = \mathbb{R}^{*2}$ pero $(\mathbb{R}^2, \sigma)$ y $(\mathbb{R}^2, \sigma')$ no son isométricos, puesto que σ y σ' tienen distinta signatura (teorema 5.13).

3. Ortogonalidad

Sea (V, σ) un espacio ortogonal sobre el cuerpo K.

Definición 3.1. Se dice que los vectores v y w son *ortogonales* si $v \cdot w = 0$.

Definición 3.2. Sea $S \subset V$. Se llama *subespacio ortogonal* a S al siguiente subespacio de V :

$$S^\perp = \{w \in V \mid v \cdot w = 0,\ v \in S\}$$

Definición 3.3. Sea (V, σ) un espacio ortogonal. Se llama *radical* de (V, σ), y se denota por $\operatorname{rad}(V)$, al subespacio

$$\operatorname{rad}(V) = \{v \in V \mid v \cdot w = 0,\ w \in V\}$$

Proposición 3.4. *Si (V,σ) es un espacio ortogonal de dimensión n. Se tiene*

$$\dim_K \operatorname{rad}(V) = n - \operatorname{rango}\sigma$$

Demostración. Sea $B = \{v_1, \ldots, v_n\}$ una base de V. Se tiene

$$\operatorname{rad}(V) = \{ \sum_{i=1}^{n} x_i v_i \in V \mid G_\sigma^B \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \}.$$

□

Corolario 3.5. *Sea (V,σ) un espacio ortogonal. Se tiene que (V,σ) es no singular si y sólo si* $\operatorname{rad}(V) = 0$.

Proposición 3.6. *Sea (V,σ) un espacio ortogonal sobre K. El espacio vectorial cociente $V/\operatorname{rad}(V)$ es un espacio ortogonal sobre K no singular con la forma bilineal*

$$\bar{\sigma}\colon V/\operatorname{rad}(V) \times V/\operatorname{rad}(V) \to K$$

dada por $\bar{\sigma}(u+\operatorname{rad}(V), v+\operatorname{rad}(V)) = \sigma(u,v)$ para cada $u, v \in V$.

Demostración. Vamos a probar que $\bar{\sigma}$ está bien definida. Si $u+\operatorname{rad}(V) = u'+\operatorname{rad}(V)$, $v+\operatorname{rad}(V) = v'+\operatorname{rad}(V)$ y $n_1, n_2 \in \operatorname{rad}(V)$ son tales que $u' = u+n_1$ y $v' = v+n_2$, entonces

$$\sigma(u',v') = \sigma(u,v) + \sigma(u,n_2) + \sigma(n_1,v) + \sigma(n_1,n_2) = \sigma(u,v),$$

y por tanto la aplicación $\bar{\sigma}$ está bien definida. Es fácil ver que $\bar{\sigma}$ cumple las propiedades de la definición 2.1 con lo cual $\bar{\sigma}$ es una forma bilineal simétrica. Veamos que $V/\operatorname{rad}(V)$ es no singular. En efecto, si $v+\operatorname{rad}(V) \in \operatorname{rad}(V/\operatorname{rad}(V))$, entonces

$$\sigma(v,v') = \bar{\sigma}(v+\operatorname{rad}(V), v'+\operatorname{rad}(V)) = 0,\ v' \in V.$$

Así, $v \in \operatorname{rad}(V)$ y $v+\operatorname{rad}(V) = \operatorname{rad}(V)$. □

Proposición 3.7. *Sea (V,σ) un espacio ortogonal sobre K y sea U un subespacio de V. El espacio vectorial U es un espacio ortogonal sobre K con la forma bilineal simétrica $\sigma_U\colon U \times U \to K$, dada por*

$$\sigma_U(u,u') = \sigma(u,u')$$

Proposición 3.8. *Sea (V,σ) un espacio ortogonal sobre K y sea U un subespacio de V. Se tiene*

$$\operatorname{rad}(U) = U \cap U^\perp$$

Definición 3.9. Sean $U_1, \ldots, U_s$ subespacios de un espacio vectorial V. Se dice que la suma $U_1+\ldots+U_s$ es *directa* y se denota por $U_1 \oplus \ldots \oplus U_s$ si se verifica la condición

$$u_1 \in U_1, \ldots, u_s \in U_s\,, \quad u_1+\ldots+u_s = 0 \quad \Longrightarrow \quad u_1 = \ldots = u_s = 0$$

***Observación* 3.10.** Si $U_1, \ldots, U_s$ son subespacios de V, entonces $U_1 + \ldots + U_s = U_1 \oplus \ldots \oplus U_s$, sí y sólo sí,

$$U_i \cap (\sum_{j \neq i} U_j) = 0,\ i = 1, \ldots, s.$$

Si la suma $U_1 + \ldots + U_s$ es directa, entonces $\dim_K(U_1 + \ldots + U_s) = \dim_K U_1 + \ldots + \dim_K U_s$.

Definición 3.11. Sea (V, σ) un espacio ortogonal. Se dice que el subespacio U es ortogonal al subespacio W si $u \cdot w = 0$, para cada $u \in U$, $w \in W$.

Definición 3.12. Sea (V, σ) un espacio ortogonal y sean $U_1, \ldots, U_r$ subespacios de V. Se dice que la suma $U_1 + \ldots + U_r$ es una *suma ortogonal* y se denota por $U_1 \perp \ldots \perp U_r$ si

(1) $U_1 + \ldots + U_r = U_1 \oplus \ldots \oplus U_r$.

(2) U_i es ortogonal a U_j para todo $i \neq j$.

Proposición 3.13. *Sea (V, σ) un espacio ortogonal.*

(1) *Sean $U_1, \ldots, U_r$ subespacios de V tales que U_i es ortogonal a U_j para $i \neq j$.*

(a) *Si $V = U_1 + \ldots + U_r$ entonces*

$$\operatorname{rad}(V) = \operatorname{rad}(U_1) + \ldots + \operatorname{rad}(U_r).$$

Si además $V = U_1 \perp \ldots \perp U_r$, entonces $\operatorname{rad}(V) = \operatorname{rad}(U_1) \perp \ldots \perp \operatorname{rad}(U_r)$.

(b) *Si $U_1, \ldots, U_r$ son no singulares, entonces*

$$U_1 + \ldots + U_r = U_1 \perp \ldots \perp U_r.$$

(2) *Sea W un subespacio suplementario de* $\operatorname{rad}(V)$. *Se tiene*

$$V = \operatorname{rad}(V) \perp W$$

y W es un subespacio de V no singular. Además, $V/\operatorname{rad}(V)$ y W son espacios isométricos.

(3) *Si W y W' son subespacios de V y $V = \operatorname{rad}(V) \perp W = \operatorname{rad}(V) \perp W'$, entonces W y W' son isométricos.*

Demostración. (1) (*a*) Dado $v = \sum_{i=1}^r u_i \in \operatorname{rad}(V)$, con $u_i \in U_i$. Para cada $w_j \in U_j$, $j = 1, \ldots, r$, se tiene

$$u_j \cdot w_j = \sum_{i=1}^{r} u_i \cdot w_j = v \cdot w_j = 0,\ j = 1, \ldots, r.$$

Por tanto, $u_j \in \operatorname{rad}(U_j)$, para $j = 1, \ldots, r$. Así,

$$\operatorname{rad}(V) \subset \operatorname{rad}(U_1) + \ldots + \operatorname{rad}(U_r).$$

Recíprocamente, si $\sum_{i=1}^r u_i \in \sum_{i=1}^r \operatorname{rad}(U_i)$ y $v = \sum_{j=1}^r w_j$, con $u_i \in \operatorname{rad}(U_i)$ y $w_j \in U_j$, para $i, j = 1, \ldots, r$, entonces

$$(\sum_{i=1}^{r} u_i) \cdot (\sum_{j=1}^{r} w_j) = \sum_{i=1}^{r} u_i \cdot w_i = 0.$$

Por tanto $\sum_{i=1}^{r} u_i \in \operatorname{rad}(V)$.

(1) (b) Supongamos que $\sum_{i=1}^{r} u_i = 0$, con $u_i \in U_i$. Para cada $w \in U_j$ se tiene

$$w \cdot u_j = \sum_{i=1}^{r} w \cdot u_i = w \cdot (\sum_{i=1}^{r} u_i) = 0.$$

Por tanto $u_j \in \operatorname{rad}(U_j) = \{0\}$, $j = 1, \ldots, r$.

(2) Si W es un subespacio suplementario de $\operatorname{rad}(V)$, entonces $V = \operatorname{rad}(V) \oplus W = \operatorname{rad}(V) \perp W$. Por (1)$(a)$ $\operatorname{rad}(V) = \operatorname{rad}(\operatorname{rad}(V)) \perp \operatorname{rad}(W) = \operatorname{rad}(V) \perp \operatorname{rad}(W)$, ya que $\sigma_{\operatorname{rad}(V)} = 0$. Así, $\operatorname{rad}(W) \subset \operatorname{rad}(V) \cap \operatorname{rad}(W) = \{0\}$.

La aplicación $f\colon W \to V/\operatorname{rad}(V)$ dada por $f(w) = w + \operatorname{rad}(V)$ es una isometría. Para probarlo veamos que f es una aplicación biyectiva. En efecto, si $w + \operatorname{rad}(V) = \operatorname{rad}(V)$, entonces $w \in \operatorname{rad}(V)$, y por tanto $w = 0$. Además, para cada $u \in \operatorname{rad}(V)$, $w \in W$, se tiene

$$(u + w) + \operatorname{rad}(V) = (u + \operatorname{rad}(V)) + (w + \operatorname{rad}(V)) = \operatorname{rad}(V) + (w + \operatorname{rad}(V)) = w + \operatorname{rad}(V) = f(w)$$

La aplicación f es una isometría puesto que $w \cdot w' = f(w) \cdot f(w')$ $\forall\, w, w' \in W$.

(3) Por (2), existen isometrías $f\colon W \to V/\operatorname{rad}(V)$ y $f'\colon W' \to V/\operatorname{rad}(V)$. La aplicación $f'^{-1} \circ f\colon W \to W'$ es una isometría. □

Definición 3.14. Los subespacios W y W' de la proposición anterior se denominan *componentes no singulares* de V.

Lema 3.15. *Sean (V, σ) y (V', σ') espacios ortogonales sobre K. Sean U_1 y U_2 subespacios de V tales que $V = U_1 \perp U_2$ y sean U_1' y U_2' subespacios de V' tales que $V' = U_1' \perp U_2'$. Sean $f_1 : U_1 \to U_1'$ y $f_2 : U_2 \to U_2'$ isometrías. La aplicación*

$$f_1 \perp f_2\colon V \to V'$$

dada por $(f_1 \perp f_2)(u_1 + u_2) = f_1(u_1) + f_2(u_2)$ es una isometría.

Demostración. La aplicación $f_1 \perp f_2$ es una isometría puesto que es un isomorfismo de espacios vectoriales y además para todo $u_1, v_1 \in U_1$ y $u_2, v_2 \in U_2$, se tiene

$$\begin{aligned}(f_1 \perp f_2)(u_1 + u_2) \cdot (f_1 \perp f_2)(v_1 + v_2) =& (f_1(u_1) + f_2(u_2)) \cdot (f_1(v_1) + f_2(v_2)) \\ =& f_1(u_1) \cdot f_2(v_1) + f_1(u_1) \cdot f_2(v_2) \\ &+ f_2(u_2) \cdot f_1(v_1) + f_2(u_2) \cdot f_2(w_2) \\ =& u_1 \cdot v_1 + u_2 \cdot v_2 = (u_1 + u_2) \cdot (v_1 + v_2).\end{aligned}$$

□

Proposición 3.16. *Sean V y V' espacios ortogonales. Se tiene que V y V' son isométricos si, y sólo si, tienen igual dimensión y componentes no singulares isométricas.*

Demostración. Si V y V' son isométricos, entonces $\operatorname{rad}(V)$ y $\operatorname{rad}(V')$ son isomorfos y $V/\operatorname{rad}(V)$ y $V'/\operatorname{rad}(V')$ son isométricos. Sea $g\colon V/\operatorname{rad}(V) \to V'/\operatorname{rad}(V')$ una isometría y

$$V = \operatorname{rad}(V) \perp W, \quad V' = \operatorname{rad}(V') \perp W'.$$

Por la proposición 3.13 (2), existe una isometría $f\colon W \to V/\operatorname{rad}(V)$ y una isometría $f'\colon W' \to V'/\operatorname{rad}(V')$. La aplicación $f'^{-1} \circ g \circ f\colon W \to W'$ es una isometría. Recíprocamente, dado que $\dim_K \operatorname{rad}(V) = \dim_K V - \dim_K W = \dim_K V' - \dim_K W = \dim_K \operatorname{rad}(V')$, $\operatorname{rad}(V)$ y $\operatorname{rad}(V')$ son isomorfos. Sea $f\colon \operatorname{rad}(V) \to \operatorname{rad}(V')$ un isomorfismo y $f'\colon W \to W'$ una isometría. Se tiene que $f \perp f'\colon V \to V'$ es una isometría. □

***Observación* 3.17.** La proposición anterior permite reducir la clasificación de espacios ortogonales a la clasificación de espacios ortogonales no singulares.

Proposición 3.18. *Sea (V, σ) un espacio ortogonal no singular y sea U un subespacio de V. Se tiene*

(1) $\dim_K U + \dim_K U^\perp = \dim_K V$.

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

(3) $\operatorname{rad}(U) = \operatorname{rad}(U^\perp) = U \cap U^\perp$.

(4) *Si U es no singular, entonces $V = U \perp U^\perp$.*

(5) *Sean U y W subespacios de V. Si $V = U \perp W$, entonces $W = U^\perp$.*

Demostración. (1) Sea $B = \{v_1, \ldots, v_n\}$ una base de V, $B_U = \{u_1, \ldots, u_r\}$ una base de U y $u_i = b_{i1}v_1 + \ldots + b_{in}v_n$, $i = 1, \ldots, r$. Pongamos

$$C = \begin{pmatrix} b_{11} & \ldots & b_{1n} \\ \vdots & & \vdots \\ b_{r1} & \ldots & b_{rn} \end{pmatrix}.$$

La matriz C tiene rango r. Ya que V es no singular, el rango de σ es n y entonces la matriz $C\,G_\sigma^B$ tiene rango r.
El vector $v = \sum_{i=1}^n x_i v_i \in U^\perp$ si, y solo si,

$$u_i \cdot v = \begin{pmatrix} b_{i1} & \ldots & b_{in} \end{pmatrix} G_\sigma^B \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0,\ i = 1, \ldots, r.$$

Por tanto, $U^\perp$ es el conjunto de vectores cuyas coordenadas en B son soluciones del sistema de r ecuaciones lineales homogéneas en n variables

$$C\,G_\sigma^B \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0.$$

Dado que la matriz $C\,G_\sigma^B$ tiene rango r, $\dim_K U^\perp = n - r$.

(2) Se tiene que $U \subset U^{\perp\perp}$ y dado que $\dim_K U^\perp + \dim_K U^{\perp\perp} = \dim_K V$ y $\dim_K U^\perp + \dim_K U = \dim_K V$, $\dim_K U = \dim_K U^{\perp\perp}$. Así, $U = U^{\perp\perp}$
(3) $\operatorname{rad}(U^\perp) = U^\perp \cap U^{\perp\perp} = \operatorname{rad}(U)$.
(4) $\operatorname{rad}(U) = U \cap U^\perp = 0$, luego $U + U^\perp = U \perp U^\perp$. Dado que $\dim_K V = \dim_K U + \dim_K U^\perp$, se tiene que $V = U \perp U^\perp$.
(5) Dado que $W \subset U^\perp$ y $\dim W = n - \dim U = \dim U^\perp$, se tiene que $W = U^\perp$. □

Definición 3.19. Sea (V, σ) un espacio ortogonal sobre K y sea $v \in V$, $v \neq 0$. Se dice v es *isótropo* si $v^2 = 0$.

Lema 3.20. *Sea K un cuerpo de característica distinta de 2 y sea (V, σ) un espacio ortogonal sobre K. Si $\sigma \neq 0$, entonces existe un vector $v \in V$, $v \neq 0$, no isótropo.*

Demostración. Sea (V, σ) un espacio ortogonal. Supongamos que todos los vectores de V son isótropos. Para cada $v, w \in V$, se tiene

$$0 = (v + w)^2 = v^2 + 2\, v \cdot w + w^2 = 2\, v \cdot w.$$

Dado que la característica de K es distinta de 2, $v \cdot w = 0$. Luego $\sigma = 0$. □

***Observación* 3.21.** Si la característica de K es 2, existen espacios no singulares sobre K donde todos los vectores son isótropos. Por ejemplo, sea V el plano ortogonal sobre K con la forma bilineal cuya matriz de Gram respecto una la base B es

$$G_\sigma^B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Todos los vectores de V son isótropos y V es no singular.

Teorema 3.22. (Teorema de estructura de espacios ortogonales) *Sea K un cuerpo de característica distinta de 2 y sea (V, σ) un espacio ortogonal sobre K de dimensión $n \geq 1$. Existen vectores $v_1, \ldots, v_n$ tales que,*

$$V = \langle v_1 \rangle \perp \ldots \perp \langle v_n \rangle.$$

Demostración. Supongamos que V es no singular. Razonaremos por inducción sobre n. Para $n = 1$ es trivial. Supongamos que el teorema es cierto para espacios ortogonales sobre K de dimensión $n - 1$ y veamos que es cierto para espacios ortogonales de dimensión n. Sea (V, σ) un espacio ortogonal de dimensión n. Si $\sigma = 0$, cualquier base de V da un conjunto de vectores con esta propiedad. Si $\sigma \neq 0$ por el lema 3.20, existe un vector $v_1 \in V$, $v_1^2 \neq 0$. Por la proposición 3.18,

$$V = \langle v_1 \rangle \perp \langle v_1 \rangle^\perp$$

Aplicando la hipótesis de inducción a $(\langle v_1 \rangle^\perp, \sigma_{\langle v_1 \rangle^\perp})$ se tiene que existen vectores $v_2, \ldots, v_n \in \langle v_1 \rangle^\perp$ tales que $\langle v_1 \rangle^\perp = \langle v_2 \rangle \perp \ldots \perp \langle v_n \rangle$. Así,

$$V = \langle v_1 \rangle \perp \ldots \perp \langle v_n \rangle$$

Si V es singular, entonces $V = \mathrm{rad}(V) \perp W$ siendo W es un subespacio de V no singular. Por ser W no singular existen vectores $v_1, \ldots, v_r \in W$ tales que $W = \langle v_1 \rangle \perp \ldots \perp \langle v_r \rangle$. Sea $v_{r+1}, \ldots, v_n$ una base de $\mathrm{rad}(V)$. Se tiene que $V = \langle v_1 \rangle \perp \ldots \perp \langle v_n \rangle$. □

Definición 3.23. Sea (V, σ) es un espacio ortogonal sobre K. Se dice que la base $B = \{v_1, \ldots, v_n\}$ es una *base ortogonal* de V, si $v_i \cdot v_j = 0$ para todo $i \neq j$.

***Observación* 3.24.** Una base B de V es base ortogonal de (V, σ) si, y solo si, G_σ^B es una matriz diagonal.

Corolario 3.25. *Sea K un cuerpo de característica distinta de 2 y sea (V, σ) un espacio ortogonal sobre K. Existen bases ortogonales de V.*

Demostración. Por el teorema 3.22, existen vectores $v_1, \ldots, v_n$ tales que $V = \langle v_1 \rangle \perp \ldots \perp \langle v_n \rangle$. El conjunto $B = \{v_1, \ldots, v_n\}$ es una base ortogonal de V. □

***Observación* 3.26.** Si la característica de K es 2, entonces existen espacios ortogonales sobre K que no tienen bases ortogonales. El plano del ejemplo de la observación 3.21 no tiene bases ortogonales.

***Notación* 3.27.** Denotaremos por C la base canónica de K^n para $n > 0$; es decir,

$$C = \{e_1, \overset{n}{\ldots}, e_n\}, \quad e_i = (0, \ldots, \overset{i}{1}, \ldots, 0), \ i = 1, \ldots, n.$$

Corolario 3.28. *Sea K un cuerpo de característica distinta de 2 y sea $A \in M_n(K)$. Si A es una matriz simétrica entonces es congruente a una matriz diagonal.*

Demostración. Consideremos el espacio ortogonal (K^n, σ_A), donde σ_A es la forma bilineal de K^n cuya matriz de Gram respecto a la base canónica es A. Por el corolario 3.25, existe una base ortogonal B de (K^n, σ_A) y por tanto la matriz $G^B_{\sigma_A}$ es una matriz diagonal. Por la proposición 2.5, las matrices A y $G^B_{\sigma_A}$ son congruentes. □

El problema de clasificación de espacios ortogonales es uno de los problemas centrales de la teoría de espacios ortogonales. Se quiere determinar todas las clases de isometría de espacios ortogonales sobre un cuerpo dado. El método principal de clasificar espacios ortogonales es asociar invariantes a estos espacios de forma que el espacio quede determinado por estos invariantes.

***Notación* 3.29.** Si (K^n, σ) un espacio ortogonal tal que la matriz de Gram de σ respecto a la base canónica es la matriz $\operatorname{diag}(a_1, \ldots, a_n)$, entonces para simplificar la notación denotaremos (K^n, σ) por $\langle a_1, \ldots, a_n \rangle$.

4. Clasificación de espacios ortogonales sobre cuerpos cuadráticamente cerrados.

Se dice que un cuerpo K es *cuadráticamente cerrado* si todo elemento de K tiene raíz cuadrada. Los cuerpos algebraicamente cerrados, en particular el cuerpo de los números complejos, y los cuerpos finitos de característica 2 son cuerpos cuadráticamente cerrados. Existen también ejemplos de cuerpos cuadráticamente cerrados que no son algebraicamente cerrados. Por ejemplo, si $\mathbb{F}_q$ es un cuerpo finito de caraterística $p \neq 2$ con q elementos y $q \equiv 1 (\operatorname{mod} 4)$, entonces los cuerpos $\bigcup_{n \geq 1} \mathbb{F}_q(\sqrt[2^n]{\alpha})$, con $\alpha \in \mathbb{F}_q^* - \mathbb{F}_q^{*2}$, son cuadráticamente cerrados pero no son algebraicamente cerrados.

En esta sección consideraremos espacios ortogonales de dimensión finita sobre cuerpos cuadráticamente cerrados de característica distinta de 2.

Proposición 4.1. *Sea (V, σ) un espacio ortogonal sobre K. Si $\operatorname{rango} \sigma = r$ entonces existe una base ortogonal B de V tal que la matriz de Gram de σ respecto a B es la matriz diagonal:*

$$\operatorname{diag}(\overset{r}{1}, \ldots, 1, 0, \ldots, 0).$$

Demostración. Sea $\{v_1, \ldots, v_n\}$ una base ortogonal de V. Supongamos que los vectores $v_1, \ldots, v_n$ están ordenados de forma que

$$v_i^2 \neq 0,\ i = 1, \ldots, r, \quad v_i^2 = 0,\ i = r+1, \ldots, n.$$

Pongamos,

$$u_i = \left(\sqrt{v_i^2}\right)^{-1} v_i,\ i = 1, \ldots, r, \quad u_i = v_i,\ i = r+1, \ldots, n.$$

y $B = \{u_1, \ldots, u_n\}$. □

Veremos ahora que las clases de isometría de espacios ortogonales sobre un cuerpo cuadráticamente cerrado están determinadas por dos invariantes: la dimensión y el rango.

Teorema 4.2. (Teorema de clasificación) *Sean (V, σ) y (V', σ') espacios ortogonales sobre K . Se tiene que (V, σ) y (V', σ') son espacios ortogonales isométricos si, y solo si,* $\dim_K V = \dim_K V'$ *y* $\operatorname{rango} \sigma = \operatorname{rango} \sigma'$.

Demostración. Se sigue de la proposición anterior y del teorema 2.16. □

Corolario 4.3. *Sea (V, σ) un espacio ortogonal de dimensión n sobre K. Si el rango de σ es r, entonces (V, σ) es isométrico al espacio ortogonal $\langle 1, \overset{r}{\ldots}, 1, 0, \ldots, 0\rangle$.*

5. Espacios ortogonales sobre cuerpos ordenados.

En esta sección vamos a suponer que el cuerpo K es ordenado y vamos a clasificar los espacios ortogonales sobre cuerpos euclideanos.

Definición 5.1. Se dice que un cuerpo K es *ordenado*, si existe un subconjunto P cuyos elementos se llaman *positivos*, que cumple :

(1) $K = -P \cup \{0\} \cup P$. (unión disjunta).

(2) $P + P \subset P$.

(3) $P \cdot P \subset P$.

Propiedades 5.2. *Sea K un cuerpo ordenado, entonces se cumplen las siguientes propiedades :*

(1) *Para todo $a \in K^*$, $a^2 \in P$.*

(2) $1 \in P$.

(3) *La característica de K es cero.*

(4) *Si $a \in P$, entonces $a^{-1} \in P$.*

Demostración. (1) Sea $a \in K^*$. Si $a \in P$, entonces $a^2 \in P$. Si $a \notin P$, entonces $a \in -P$ y por tanto $-a \in P$. Así, $a^2 = (-a)^2 \in P$.

(2) Se sigue de la propiedad anterior, ya que $1 = 1^2 \in P$.

(3) $1 + \overset{r}{\ldots} + 1 \in P$, $\forall r > 0$.

(4) Si $a \in P$, dado que $a^{-1} = a(a^{-1})^2$, se obtiene que $a^{-1} \in P$. □

Definición 5.3. Sea K un cuerpo ordenado y P el conjunto de elementos positivos. Se dice que $a < b$ si $b - a \in P$

Proposición 5.4. *Sea K un cuerpo ordenado y P el conjunto de elementos positivos, la relación $<$ es transitiva.*

Demostración. Si $a < b$ y $b < c$, entonces $b - a$, $c - b \in P$. Por tanto,

$$c - a = (c - b) + (b - a) \in P \qquad \square$$

Ejemplos 5.5. Los cuerpos $\mathbb{R}$ y $\mathbb{Q}$ son cuerpos ordenados. El cuerpo de los complejos y los cuerpos finitos no son cuerpos ordenados.

Definición 5.6. Sea K un cuerpo ordenado y $\sigma\colon V \times V \to K$ una forma bilinear simétrica. Se dice que σ es *semidefinida positiva* si $v^2 \geq 0$, $\forall\, v \in V$. Se dice que σ es *definida positiva*, si $v^2 > 0$, para todo $v \in V$, $v \neq 0$. Se dice que σ es *semidefinida negativa* si $v^2 \leq 0$, $\forall\, v \in V$. Se dice que σ es *definida negativa* si $v^2 < 0$, para todo $v \in V$, $v \neq 0$.

Definición 5.7. Sea $B = \{v_1, \ldots, v_n\}$ una base ortogonal de V. Sea p es el número de vectores v_i de la base B tales que $v_i^2 > 0$ y q es el número de vectores v_i de B tales que $v_i^2 < 0$. Se llama *signatura* de σ y se escribe $\operatorname{sig}\sigma$, al par de números enteros (p, q).

***Observación* 5.8.** Si $\operatorname{sig}\sigma = (p, q)$ entonces $\operatorname{rango}\sigma = p + q$. En efecto, podemos suponer que $v_i^2 > 0$, para $i = 1, \ldots, p$, y $v_i^2 < 0$, para $i = p + 1, \ldots, p + q$, y entonces

$$G_\sigma^B = \operatorname{diag}(v_1^2, \ldots, v_p^2, v_{p+1}^2, \ldots, v_{p+q}^2, 0, \ldots, 0).$$

Teorema 5.9. (Ley de inercia de Sylvester) *La signatura de σ no depende de la base ortogonal de V considerada.*

Demostración. Sean $B = \{v_1, \ldots, v_n\}$, $B' = \{v_1', \ldots, v_n'\}$, bases ortogonales de (V, σ). Podemos suponer

$$\begin{aligned} &v_i^2 > 0,\ i = 1, \ldots, p, \quad v_i^2 < 0,\ i = p+1, \ldots, p+q, \quad v_i^2 = 0,\ i = p+q+1, \ldots, n. \\ &v_i'^2 > 0,\ i = 1, \ldots, p', \quad v_i'^2 < 0,\ i = p'+1, \ldots, p'+q', \quad v_i'^2 = 0,\ i = p'+q'+1, \ldots, n. \end{aligned}$$

Pongamos

$$\begin{aligned} &V_1 = \langle v_1, \ldots, v_p\rangle, \quad V_2 = \langle v_{p+1}, \ldots, v_{p+q}\rangle, \quad V_3 = \langle v_{p+q+1}, \ldots, v_n\rangle \\ &V_1' = \langle v_1', \ldots, v_{p'}'\rangle, \quad V_2' = \langle v_{p'+1}', \ldots, v_{p'+q'}'\rangle, \quad V_3' = \langle v_{p'+q'+1}', \ldots, v_n'\rangle \end{aligned}$$

Se tiene

$$V = V_1 \perp V_2 \perp V_3 = V_1' \perp V_2' \perp V_3'$$

Supongamos que $p > p'$. Se tiene

$$\dim(V_1 \cap (V_2' \perp V_3')) + \dim(V_1 + (V_2' \perp V_3')) = \dim V_1 + \dim(V_2' \perp V_3')$$

y dado que

$$\dim(V_1 + (V_2' \perp V_3')) \leq \dim V\,,$$

entonces

$$\begin{aligned} \dim(V_1 \cap (V_2' \perp V_3)) &\geq \dim V_1 + \dim(V_2' \perp V_3') - \dim V \\ &> \dim V_1' + \dim(V_2' \perp V_3') - \dim V = 0. \end{aligned}$$

Con lo cual concluímos que existe al menos un vector $v \in V_1 \cap (V_2' \perp V_3')$, equivalentemente $v^2 > 0$ y $v^2 \leq 0$ lo cual es una contradicción. De forma análoga se prueba que $p' > p$. El razonamiento para probar que $q = q'$ es similar. $\square$

***Observación* 5.10.** Sea K un cuerpo ordenado y (V,σ) un espacio ortogonal sobre K de dimensión n. Se tiene

σ es definida positiva si, y solo si, $\operatorname{sig}\sigma = (n,0)$.

σ es semidefinida positiva si, y solo si, $\operatorname{sig}\sigma = (r,0)$ con $r \leq n$.

σ es definida negativa si, y solo si, $\operatorname{sig}\sigma = (0,n)$.

σ es semidefinida negativa si, y solo si, $\operatorname{sig}\sigma = (0,r)$ con $r \leq n$.

Los espacios ortogonales sobre $\mathbb{R}$ de signatura $(n,0)$ se llaman *espacios euclídeos.*

La ley de inercia de Sylvester es válida en espacios ortogonales sobre un cuerpo ordenado. La dimensión y la signatura no describen por completo la estructura del espacio ortogonal; lo hacen en el caso particular en que todo elemento positivo de K es un cuadrado.

Definición 5.11. Se dice que un cuerpo ordenado K es *euclidiano* si todo elemento positivo es un cuadrado, es decir si $P = K^{*2}$, siendo P el conjunto de elementos positivos de K. Son ejemplo obvio de cuerpos euclidianos el cuerpo $\mathbb{R}$ de los números reales, y el cuerpo A de los números reales algebraicos, es decir $A = \overline{\mathbb{Q}} \cap \mathbb{R}$, siendo $\overline{\mathbb{Q}}$ la clusura algebraica de $\mathbb{Q}$ (tomada dentro del cuerpo de los números complejos), Otro ejemplo de cuerpo euclidiano es el cuerpo de los números reales constructibles $\tilde{\mathbb{Q}} \cap \mathbb{R}$, siendo $\tilde{\mathbb{Q}}$ el cuerpo de los números constructibles; $\mathbb{Q}$ no es un cuerpo euclidiano.

Proposición 5.12. *Sea K un cuerpo euclidiano y (V,σ) un espacio ortogonal sobre K. Si $\operatorname{sig}\sigma = (p,q)$, entonces existe una base ortogonal B de V tal que la matriz de Gram de σ respecto a B es la matriz diagonal que denotaremos por*

$$\operatorname{diag}(1,\overset{p}{\ldots},1,-1,\overset{q}{\ldots},-1,0,\ldots,0)$$

Demostración. Sea $\{v_1,\ldots,v_n\}$ una base ortogonal de V. Supongamos que los vectores $v_1,\ldots,v_n$ están ordenados de tal forma que

$$v_i^2 > 0,\ i = 1,\ldots,p, \quad v_i^2 < 0,\ i = p+1,\ldots,r, \quad v_i^2 = 0,\ i = r+1,\ldots,n.$$

Pongamos,

$$u_i = \left(\sqrt{v_i^2}\right)^{-1} v_i,\ i = 1,\ldots,p, \quad u_i = \left(\sqrt{-v_i^2}\right)^{-1} v_i,\ i = p+1,\ldots,r, \quad u_i = v_i,\ i = r+1,\ldots,n.$$

y $B = \{v_1,\ldots,v_n\}$. □

Teorema 5.13. (Teorema de clasificación) *Sea K un cuerpo euclidiano y (V,σ) y (V',σ') espacios ortogonales sobre K. Se tiene que (V,σ) y (V',σ') son espacios ortogonales isométricos si, y solo si $\dim_K V = \dim_K V'$ y $\operatorname{sig}\sigma = \operatorname{sig}\sigma'$.*

Demostración. Sean V y V' dos espacios ortogonales isométricos, existen bases B de V y B' de V' tales que $G_\sigma^B = G_{\sigma'}^{B'}$. Si $\operatorname{sig}\sigma = (p,q)$, la matriz G_σ^B es congruente a la matriz $\operatorname{diag}(1,\overset{p}{\ldots},1,-1,\overset{q}{\ldots},-1,0,\ldots,0)$. Dado que la matriz $G_{\sigma'}^{B'}$ es congruente a la matriz $\operatorname{diag}(1,\overset{p}{\ldots},1,-1,\overset{q}{\ldots},-1,0,\ldots,0)$, por la demostración del corolario 2.17 existe una base $\bar{B}'$ de V' tal que

$$G_{\sigma'}^{\bar{B}'} = \operatorname{diag}(1,\overset{p}{\ldots},1,-1,\overset{q}{\ldots},-1,0,\ldots,0).$$

Así, $\operatorname{sig}\sigma' = (p,q)$.

Recíprocamente si $\operatorname{sig}\ \sigma = \operatorname{sig}\sigma' = (p,q)$, existe una base B de V y una base B' de V' tal que $G_\sigma^B = \operatorname{diag}(1,\overset{p}{\ldots},1,-1,\overset{q}{\ldots},-1,0,\ldots,0) = G_{\sigma'}^{B'}$. Aplicando el teorema 2.16, V y V' son isométricos. □

Corolario 5.14. *Sea K un cuerpo euclidiano. Todo espacio ortogonal sobre K de dimensión n con $\operatorname{sig}\sigma = (p,q)$, es isométrico al espacio ortogonal $\langle 1,\overset{p}{\ldots},1,-1,\overset{q}{\ldots},-1,0,\ldots,0\rangle$.*

6. Isotropía y espacios hiperbólicos

En esta sección vamos a considerar espacios ortogonales de dimensión finita sobre cuerpos de característica distinta de 2.

Definición 6.1. Un *plano hiperbólico* es un espacio ortogonal no singular de dimensión 2 que contiene un vector isótropo. Un *espacio hiperbólico* es un espacio ortogonal que es suma ortogonal de planos hiperbólicos.

Un espacio ortogonal (V, σ) se dice que es *isotrópico* si tiene un vector isótropo. Un espacio ortogonal (V, σ) se dice que es *totalmente isotrópico* si $\sigma = 0$.

Un espacio ortogonal se dice que es *anisotrópico* si no tiene vectores isótropos.

***Observación* 6.2.** Los espacios anisotrópicos son no singulares.

Los espacios anisotrópicos de dimensión n sobre cuerpos euclidianos son los espacios de signatura $(n, 0)$ o $(0, n)$. En efecto supongamos que (V, σ) es anisotrópico y $\operatorname{sig}\sigma = (p, q)$, $p + q = n$. Si $p \neq 0$ y $q \neq 0$ y $B = \{v_1, \ldots, v_n\}$ es una base tal que

$$G_\sigma^B = \operatorname{diag}(1, \overset{p}{\ldots}, 1, -1, \overset{q}{\ldots}, -1).$$

entonces los vectores $v_i + v_j$ para $i \in \{1, \ldots, p\}$ y $j \in \{p+1, \ldots, n\}$ son vectores isotrópos de V.

Recíprocamente, sea (V, σ) un espacio ortogonal tal que $\operatorname{sig}\sigma = (n, 0)$ o $\operatorname{sig}\sigma = (0, n)$ y sea $B = \{v_1, \ldots, v_n\}$ una base de V tal que $G_\sigma^B = \operatorname{diag}(1, \ldots, 1)$ o $G_\sigma^B = \operatorname{diag}(-1, \ldots, -1)$. Si $v = \sum_{i=1}^n x_i v_i \neq 0$ y $x_j \neq 0$ para algún $j \in \{1, \ldots, n\}$, entonces

$$v^2 = \sum_{i=1}^n x_i^2 \neq 0 \quad \text{o} \quad v^2 = \sum_{i=1}^n -x_i^2 \neq 0$$

Los únicos espacios anisotrópicos sobre cuerpos cuadráticamente cerrados son los espacios ortogonales no singulares de dimensiones 0 o 1. En efecto, sea K un cuerpo cuadráticamente cerrado y V un espacio ortogonal sobre K. Si $\dim_K V = 1$ y $v_1 \in V$ es tal que $v_1^2 = 1$, entonces para cada $\lambda \in K - \{0\}$, se tiene que $(\lambda\, v_1)^2 = \lambda^2 \neq 0$. Si $\dim_K V \geq 2$, $B = \{v_1, \ldots, v_n\}$ es una base de V tal que $G_\sigma^B = \operatorname{diag}(1 \ldots 1)$ y $\varepsilon \in K$ es tal que $\varepsilon^2 = -1$, entonces el vector $v_1 + \varepsilon v_2$ es un vector isótropo.

Los planos hiperbólicos sobre cuerpos euclidianos son los de signatura $(1, 1)$ y los espacios hiperbólicos son los espacios ortogonales de dimensión n par y de signatura $(n/2, n/2)$.

Los planos hiperbólicos sobre cuerpos cuadráticamente cerrados son los planos no singulares y los espacios hiperbólicos son los espacios ortogonales no singulares de dimensión par.

Lema 6.3. *Sea V un espacio ortogonal y $u \in V$ un vector isótropo tal que $u \notin rad(V)$. Existe un plano hiperbólico P tal que $u \in P$.*

Demostración. Dado que $u \notin \operatorname{rad(V)}$, existe $v \in V$ tal que $u \cdot v \neq 0$. Se tiene que u y v son linealmente independientes, ya en el caso contrario $v = \lambda\, u$ con $\lambda \in K$ y por tanto $u \cdot v = \lambda u^2 = 0$. Pongamos $P = \langle u, v \rangle$. La matriz de Gram del plano P en la base $\{u, v\}$ es

$$\begin{pmatrix} 0 & u \cdot v \\ u \cdot v & v^2 \end{pmatrix}.$$

Así, P es un plano no singular que contiene un vector isótropo. □

Lema 6.4. *Sea V un plano hiperbólico y $u \in V$ un vector isótropo. Existe un único vector isótropo v tal que $u \cdot v = 1$.*

Demostración. Sea $\{u, w\}$ una base de V. Dado que V es no singular $u \cdot w \neq 0$. Calculamos todos los vectores $v = xu + yw$ tales que

$$v^2 = y^2 w^2 + 2xy\, u \cdot w = 0, \quad u \cdot v = y\, u \cdot w = 1$$

Se tiene

$$y = (u \cdot w)^{-1}, \quad x = -\frac{1}{2}\,(u \cdot w)^{-2}\, u^2.$$

□

Definición 6.5. Sea V un plano hiperbólico. El par $(u, v) \in V \times V$ se dice que es un *par hiperbólico* si

$$u^2 = 0, \quad v^2 = 0, \quad u \cdot v = 1.$$

Lema 6.6. *Sea (V, σ) un plano hiperbólico. Existen bases B y B' tales que*

$$G_\sigma^B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad G_\sigma^{B'} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Demostración. Sea $u \in V$ tal que $u^2 = 0$. Por el lema 6.4, existe un vector v tal que $v^2 = 0$ y $u \cdot v = 1$. Dado que $u \cdot v \neq 0$, los vectores u y v son linealmente independientes. Pongamos $v_1 = u$, $v_2 = v$ y $B = \{v_1, v_2\}$. Se tiene

$$G_\sigma^B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Pongamos

$$v_1' = v_1 + \frac{1}{2}\, v_2, \quad v_2' = v_1 - \frac{1}{2}\, v_2.$$

Se tiene

$$v_1'^2 = v_1^2 + \frac{1}{4}\, v_2^2 + v_1 \cdot v_2 = v_1 \cdot v_2 = 1$$
$$v_2'^2 = v_1^2 + \frac{1}{4}\, v_2^2 - v_1 \cdot v_2 = -v_1 \cdot v_2 = -1$$
$$v_1' \cdot v_2' = v_1^2 - \frac{1}{4}\, v_2^2 = 0.$$

Si $B' = \{v_1', v_2'\}$, entonces

$$G_\sigma^{B'} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

□

Lema 6.7. (1) *Sea (H, σ) un espacio hiperbólico de dimensión $2n$. Existe una base B de H tal que la matriz de Gram de σ en B es la matriz diagonal por bloques*

$$\begin{pmatrix} 1 & 0 & & & \\ 0 & -1 & & & \\ & & \ddots & & \\ & & & 1 & 0 \\ & & & 0 & -1 \end{pmatrix}, \qquad (\star)$$

(2) *Dos espacio hiperbólicos de igual dimensión son isométricos.*

Demostración. (1) $H = P_1 \perp \ldots \perp P_n$, donde P_i, para $i = 1, \ldots, n$, es un plano hiperbólico. Sea $\{u_i, v_i\}$ una base de P_i tal que $G^{B_i}_{\sigma_{P_i}} = \mathrm{diag}(1, -1)$, para $i = 1, \ldots, n$, y $B = \{u_1, \ldots, v_1, \ldots, u_n, v_n\}$. La matriz de Gram de σ en B es la matriz $(*)$.

(2) Sean (H, σ) y (H', σ') espacios hiperbólicos y B y B' bases de H y H', respectivamente, tales que las matrices de Gram de σ respecto a B y a σ' en B' son iguales a la matriz $(*)$. Por el teorema 2.16, (H, σ) y (H', σ') son isométricos. □

Definición 6.8. Sea V un espacio ortogonal sobre K. Se dice que V es universal si para cada $a \in K$ existe $v \in V$, tal que $v^2 = a$.

Lema 6.9. *Todo plano hiperbólico es universal.*

Demostración. Sea (u, v) un par hiperbólico y $a \in K$. Se tiene

$$a = (u + \frac{1}{2}\, a\, v)^2.$$

□

Corolario 6.10. *Sea K un cuerpo. Todo elemento de K se puede escribir como diferencia de dos cuadrados.*

Demostración. Consideremos el plano hiperbólico $\langle 1, -1\rangle$. Dado que $\langle 1, -1\rangle$ es universal, para cada $a \in K$ existe un vector $(b, c) \in K^2$ tal que $(b, c)^2 = b^2 + c^2 = a$. □

7. Teorema de Witt

En esta sección vamos a considerar espacios ortogonales sobre cuerpos de característica distinta de 2. Probaremos el teorema de Witt que afirma que toda isometría entre dos subespacios de un espacio ortogonal V se puede extender a una isometría de V.

Definición 7.1. Sean V y V' espacios ortogonales sobre K. Sea U un subespacio de V, W un subespacio de V' y $f\colon U \to W$ una isometría. Se dice que la isometría $f'\colon V \to V'$ *extiende* a f si $f'(u) = f(u)$, para cada $u \in U$; tambien se escribe $f'|_U = f$.

Lema 7.2. *Sea V un espacio ortogonal no singular y sea U un subespacio singular de V. Sea W una componente no singular de U y sean $u_1, \ldots, u_r$ los vectores de una base de* $\mathrm{rad}(U)$.

(1) *Existen vectores $v_1, \ldots, v_r$ en V tales que (u_i, v_i) es un par hiperbólico para $i = 1, \ldots, r$ y tales que los planos hiperbólicos $P_i = \langle u_i, v_i\rangle$, para $i = 1, \ldots, r$, sean ortogonales dos a dos y ortogonales a W.*

(2) *Si $\bar{U} = P_1 + \cdots + P_r + W$, entonces $\bar{U} = P_1 \perp \cdots \perp P_r \perp W$, $\bar{U}$ es no singular y $U \subset \bar{U}$.*

Demostración. Se tiene que $U = \mathrm{rad}(U) \perp W$.

(1) Lo probaremos por inducción sobre r. Si $r = 1$, entonces $U = \langle u_1\rangle \perp W$. Luego $u_1 \in W^\perp$. Por el lema 6.3, dado que $W^\perp$ es no singular, existe un plano hiperbólico $P_1 \subset W^\perp$ tal que $u_1 \in P_1$. Por el lema 6.4, P_1 contiene un par hiperbólico.

Supongamos el resultado cierto para $r-1$. Pongamos

$$U_0 = \langle u_1, \ldots, u_{r-1} \rangle \perp W.$$

Se tiene que $u_r \in U_0^\perp$ y $u_r \notin U_0$. Por ser V no singular, $\mathrm{rad}(U_0) = \mathrm{rad}(U_0^\perp)$ y entonces

$$\mathrm{rad}(U_0^\perp) = \langle u_1, \ldots, u_{r-1} \rangle.$$

Dado que $u_r \notin \mathrm{rad}(U_0^\perp)$, existe $v \in U_0^\perp$ tal que $u_r \cdot v \neq 0$. Por el lema 6.3, los vectores u_r y v son linealmente independientes y el plano $P_r = \langle u_r, v \rangle$ es un plano hiperbólico. Sea (u_r, v_r) un par hiperbólico que genera P_r. Puesto que $P_r \subset U_0^\perp$, entonces $U_0 \subset P_r^\perp$. Se tiene

$$U_0 = \mathrm{rad}(U_0) \perp W \subset P_r^\perp, \quad \mathrm{rad}(U_0) = \langle u_1, \ldots, u_{r-1} \rangle.$$

Utilizando la hipótesis de inducción en $P_r^\perp$ (que es un espacio no singular) existen vectores $v_1, \ldots, v_{r-1} \in P_r^\perp$ tales que cada par (u_i, v_i) es un par hiperbólico para $i = 1, \ldots, r-1$ y tales que los planos $P_i = \langle u_i, v_i \rangle$, para $i = 1, \ldots, r-1$, sean ortogonales dos a dos y ortogonales a W. Dado que son ortogonales a P_r y que P_r es ortogonal a W se tiene el resultado.

□

Proposición 7.3. *Sean V y V' un espacios ortogonales no singular. Sea U un subespacio singular de V y U' un subespacio singular de V'. Si $f\colon U \to U'$ es una isometría, entonces f se puede extender a una isometría entre dos subespacios no singulares de V y V', respectivamente.*

Demostración. Si U y U' son no singulares, una extensión de f es f. Supongamos que U y por tanto U' son singulares. Pongamos $U = \mathrm{rad}(U) \perp W$. Se tiene

$$U' = f(U) = f(\mathrm{rad}(U)) \perp f(W) = \mathrm{rad}(U') \perp f(W).$$

Sean $u_1 \ldots, u_r$ los vectores de una base de $\mathrm{rad}(U)$. Los vectores $f(u_1), \ldots, f(u_r)$ forman una base de $\mathrm{rad}(U')$. Por el lema 7.2, existen vectores existen vectores $v_1, \ldots v_r \in V$ y vectores $v_i' \in V'$, $i = 1, \ldots, r$, tales que cada par (u_i, v_i) es un par hiperbólico, cada par $(f(u_i), v_i')$ es un par hiperbólico y tales que los planos $P_1 = \langle u_1, v_i \rangle$, $i = 1, \ldots, r$ son ortogonales dos a dos y ortogonales a W y los planos $P_i' = \langle f(u_i), v_i' \rangle$, $i = 1, \ldots, r$, son ortogonales dos a dos y ortogonales a $f(W)$. Los espacios $\bar{U} = P_1 \perp \ldots \perp P_r \perp W$ y $\bar{U}' = P_1' \perp \ldots \perp P_r' \perp f(W)$ son no singulares. Por el lema 6.7 (2), la aplicación lineal $g\colon P_1 \perp \ldots \perp P_r \to P_1' \perp \ldots \perp P_r'$, dada por $g(u_i) = f(u_i)$, $g(v_i) = v'i$, para $i = 1, \ldots, r$, es una isometría. Luego, la aplicación $\bar{f} = g \perp f|_W\colon \bar{U} \to \bar{U}'$ es una isometría que extiende a f. □

Proposición 7.4. *Sea (V, σ) un espacio ortogonal no singular. Sea U un subespacio de V y $f\colon U \to U$ una isometría. Existe una isometría de V que extiende a f.*

Demostración. Si U es no singular entonces $V = U \perp U^\perp$. Dado que $1_{U^\perp}\colon U^\perp \to U^\perp$ es una isometría, $f \perp 1_{U^\perp}$ es una isometría que extiende a f.

Sea U es un subespacio singular de V, $U = \mathrm{rad}(U) \perp W$ y $u_1, \ldots, u_r$ son los vectores de una base de $\mathrm{rad}(U)$. Por la proposición 7.2, existen vectores $v_1, \ldots, v_r$ tales que los pares $(u_1, v_1), \ldots, (u_r, v_r)$ son pares hiperbólicos y los planos $P_i = \langle u_i, v_i \rangle$, para $i = 1, \ldots, r$, son ortogonales dos a dos y ortogonales a W. Pongamos $\bar{U} = P_1 \perp \ldots \perp P_r \perp W$.

Se tiene que $U = f(U) = f(\mathrm{rad}(U)) + f(W)$. Dado que $f\colon U \to U$ es una isometría, $U = \mathrm{rad}(U) \perp f(W)$ y $\{f(u_1), \ldots, f(u_r)\}$ es una base de $\mathrm{rad}(U)$. El espacio ortogonal $\bar{U}$ es no singular y $U \subset \bar{U}$.

Por la proposición 7.2, existen vectores $v'_1, \ldots, v'_r \in \bar{U}$ tales que los pares $(f(u_i), v'_i)$, para $i = 1, \ldots, r$, son hiperbólicos y los subespacios $P'_i = \langle f(u_i), v'_i \rangle$, para $i = 1, \ldots, r$, son ortogonales dos a dos y ortogonales a $f(W)$. Se tiene

$$P'_1 + \ldots + P'_r + f(W) = P'_1 \perp \ldots \perp P'_r \perp f(W) \subset \bar{U}.$$

Dado que $\dim_K(P'_1 \perp \ldots \perp P'_r \perp f(W)) = \dim_K \bar{U}$, se tiene que $\bar{U} = P'_1 \perp \ldots \perp P'_r \perp f(W)$. Por el lema 6.7 (2), existe una isometría $g\colon P_1 \perp \ldots \perp P_r \to P'_1 \perp \ldots \perp P'_r$. La isometría $\bar{f} = g \perp f|_W\colon \bar{U} \to \bar{U}$ extiende a f.

Dado que $\bar{U}$ es un subespacio no singular de V, por la primera parte de la demostración, $\bar{f}$ se extiende a una isometría de V. □

Teorema 7.5. (Teorema de Witt) Sea (V, σ) un espacio ortogonal no singular. Sean U y W subespacios isométricos. Toda isometría $f\colon U \to W$ se puede extender a una isometría de V.

Demostración. Si $U = W$ aplicando la proposición 7.4 se tiene el resultado.

Supongamos que $U \neq W$.

- Si $\dim U = \dim W = 1$. Sea $u \in U$, $u \neq 0$ y $f(u) = w$. Puesto que $\langle u \rangle = U$, $\langle w \rangle = W$ y $U \neq W$, los vectores u y w son linealmente independientes. La aplicación lineal $g\colon U + W \to U + W$ dada por $g(u) = w$ y $g(w) = u$ es una isometría. En efecto,

$$\begin{aligned} g(u) \cdot g(u) &= w \cdot w = f(u) \cdot f(u) = u \cdot u \\ g(w) \cdot g(w) &= u \cdot u = f(u) \cdot f(u) = w \cdot w \\ g(u) \cdot g(w) &= w \cdot u = u \cdot w. \end{aligned}$$

  Por la proposición 7.4, $g\colon U + W \to U + W$ se puede extender a una isometría de V.

- Supongamos que $\dim U = \dim W \geq 1$. Sea U y por tanto W no singular. Razonaremos por inducción sobre la dimensión n de V. Si $n = 1$, el teorema es trivial. Supongamos el teorema cierto para espacios ortogonales no singulares de dimensión menor que n. Sea $u \in U$ un vector no isótropo y sea $f(u) = w$. Entonces

$$U = \langle u \rangle \perp U', \quad W = \langle w \rangle \perp f(U'),$$

  donde U' es el subespacio ortogonal a $\langle u \rangle$ en U y $f(U')$ es el subespacio ortogonal a $\langle w \rangle$ en W. Dado que $f|_{\langle u \rangle}\colon \langle u \rangle \to \langle w \rangle$ es una isometría, por el caso anterior existe una isometría $g\colon V \to V$ que extiende a $f|_{\langle u \rangle}$. Se tiene

$$g(u) = w, \quad g(U) = \langle w \rangle \perp g(U').$$

  Dado que $f(U'), g(U') \subset \langle w \rangle^\perp$, $\langle w \rangle^\perp$ es no singular y $\dim \langle w \rangle^\perp = n-1$, por hipótesis de inducción la isometría

$$f|_{U'} \circ g^{-1}|_{g(U')}\colon g(U') \to f(U')$$

  se puede extender a una isometría $\tau\colon \langle w \rangle^\perp \to \langle w \rangle^\perp$. Consideremos la isometría

$$f' = (1_{\langle w \rangle} \perp \tau) \circ g\colon V \to V.$$

  Se tiene

$$\begin{aligned} f'(u) &= (1_{\langle w \rangle} \perp \tau)(w) = w = f(u),\ u \in U \\ f'(u') &= \tau(g(u')) = (f \circ g^{-1})(g)(u')) = f(u'),\ u' \in U'. \end{aligned}$$

  Por tanto f' es una extensión de f a V.

- Si U y por tanto W es singular, por la proposición 7.3, f se puede extender a una isometría entre dos espacion no singulares de V y esta última se puede extender, por el razonamiento anterior a una isometría de V. □

***Observación* 7.6.** Sea (V, σ) es un espacio ortogonal no singular de dimensión n sobre un cuerpo euclidiano. Si la signatura de σ es $(n, 0)$ o $(0, n)$, la demostracíón del teorema de Witt es fácil. En efecto, sea $f\colon U \to W$ una isometría, $\dim U = r$. Se tiene que $V = U \perp U^\perp = W \perp W^\perp$, $\dim U^\perp = \dim W^\perp = n - r$. Por el teorema de clasificación dado que $U^\perp$ y $W^\perp$ tienen la misma signatura $(n-r, 0)$ o $(0, n-r)$, entonces son isométricos. Si $g\colon U^\perp \to W^\perp$ es una isometría entonces $f \perp g\colon V \to V$ es una isometría que extiende a f.

***Observación* 7.7.** El teorema de Witt no es cierto, en general, si V es un espacio ortogonal singular. En efecto, consideremos el espacio vectorial V de dimensión 3 con la forma bilineal σ cuya matriz de Gram respecto a la base $B = \{v_1, v_2, v_3\}$ es la matriz

$$G_\sigma^B = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

(V, σ) es un espacio singular. La aplicación lineal $f\colon \langle v_3\rangle \to \langle v_1\rangle$ dada por $f(v_3) = v_1$, es una isometría. Si existiese una isometría $f'\colon V \to V$ extendiendo a f, entonces $f'(\mathrm{rad}(V)) = \mathrm{rad}(V)$. Esto último no es cierto, puesto que $\mathrm{rad}(V) = \langle v_3\rangle$ y $f'(\langle v_3\rangle) = \langle v_1\rangle \neq \langle v_3\rangle$.

El siguiente teorema se conoce también como el teorema de Witt.

Teorema 7.8. *Sean V y V' espacios ortogonales no singulares isométricos. Sea U un subespacio de V y U' un subespacio de V'. Si $f\colon U \to U'$ es una isometría, entonces f se puede extender a una isometría de V a V'.*

Demostración. Dado que V y V' son isométricos, existe una isometría $g\colon V \to V'$. Consideremos la isometría

$$(g^{-1}|_{U'}) \circ f\colon U \to g^{-1}(U').$$

Por el teorema de Witt, la isometría $(g^{-1}|_{U'}) \circ f$ se puede extender a una isometría $h\colon V \to V$. Consideremos la isometría $g \circ h\colon V \to V'$. Se tiene

$$(g \circ h)(u) = g(g^{-1}(f(u))) = f(u), \quad \forall\, u \in U.$$

Así, $g \circ h$ extiende a f. □

Corolario 7.9. (Ley de cancelación de Witt) Sean V y V' espacios ortogonales no singulares isométricos y sean U y W subespacios de V y U' y W' subespacios de V' tales que

$$V = U \perp W, \quad V' = U' \perp W'.$$

Si U y U' son no singulares e isométricos, entonces W y W' son isométricos.

Demostración. Sean $f\colon U \to U'$ una isometría. Por el teorema 7.8, existe una isometría $f'\colon V \to V'$ que extiende a f. Dado que $W = U^\perp$ y $W' = U'^\perp$, se tiene que $f'(W) = W'$. Así, $f'|_W\colon W \to W'$ es una isometría. □

Teorema 7.10. (Teorema de Witt para matrices) *Sean $A, A' \in M_n(K)$ matrices simétricas regulares y sean $S, S' \in M_r(K)$ y $T, T' \in M_{n-r}(K)$ matrices tales que*

$$A = \left(\begin{array}{c|c} S & 0 \\ \hline 0 & T \end{array}\right), \quad A' = \left(\begin{array}{c|c} S' & 0 \\ \hline 0 & T' \end{array}\right).$$

Si las matrices A y A' son congruentes y las matrices S y S' son congruentes, entonces las matrices T y T' son congruentes.

Demostración. Claramente las matrices S, S', T y T' son regulares y simétricas. Sea V un espacio vectorial sobre K de dimensión n y sea σ la forma bilineal simétrica en V cuya matriz de Gram en la base $B = \{v_1, \ldots, v_n\}$ es la matriz A. Sea V' otro espacio vectorial sobre K de dimensión n y σ' la forma bilineal simétrica cuya matriz de Gram en la base $B' = \{v_1, \ldots, v_n\}$ es A'. Dado que las matrices A y A' son regulares, los espacios ortogonales (V, σ) y (V', σ') son no singulares. Por el corolario 2.17, dado que las matrices A y A' son congruentes, (V, σ) y (V', σ') son isométricos. Sea $U = \langle v_1, \ldots, v_r \rangle$ y $U' = \langle v'_1, \ldots, v'_r \rangle$. La matriz de Gram de σ_U en la base $\{v_1, \ldots, v_r\}$ es S y la matriz de Gram de $\sigma_{U'}$ en la base $\{v'_1, \ldots, v'_r\}$ es S'. Dado que S y S' son matrices congruentes, los espacios (U, σ_U) y $(U', \sigma'_{U'})$ son isométricos. Se tiene

$$U^\perp = \langle v_{r+1}, \ldots, v_n \rangle, \quad U'^\perp = \langle v'_{r+1}, \ldots, v'_n \rangle.$$

La matriz de Gram de $\sigma_{U^\perp}$ en la base $\{v_{r+1}, \ldots, v_n\}$ es T y la matriz de Gram de $\sigma_{U'^\perp}$ en la base $\{v'_r, \ldots, v'_n\}$ es T'. Dado que (U, σ_U) y (U', σ'_U) son isométricos, por el corolario 7.9, se tiene que $U^\perp$ y $U'^\perp$ son isométricos. Así, las matrices T y T' son congruentes. □

8. El teorema de descomposición de Witt

En esta sección consideraremos espacios ortogonales sobre cuerpos de característica distinta de 2 y probaremos que todo espacio ortogonal admite una descomposición como suma ortogonal de un subespacio totalmente isotrópico, un subespacio hiperbólico y un espacio subespacio anisotrópico y que esta descomposición es única salvo isometrías.

Proposición 8.1. *Sea V un espacio ortogonal no singular. Todo subespacio totalmente isotrópico de V está contenido en un subespacio totalmente isotrópico maximal. Todos los subespacios totalmente isotrópicos maximales de V tienen la misma dimensión.*

Demostración. Dado que V es un espacio de dimensión finita todo subespacio totalmente isotrópico de V está contenido en un subespacio totalmente isotrópico maximal. Sean U y W subespacios totalmente isotrópicos maximales de V con $\dim_K U \leq \dim_K W$ y sea W' un subespacio de W de igual dimensión que U. Todo isomorfismo de espacios vectoriales $f\colon U \to W'$ es una isometría y por el teorema de Witt se puede extender a una isometría g de V. El subespacio $g^{-1}(W)$ es totalmente isotrópico y $U \subset g^{-1}(W)$. Luego, $U = g^{-1}(W)$ y $\dim_K U = \dim_K W$. □

Definición 8.2. Sea V un espacio ortogonal no singular. Se llama *índice de Witt* a la dimensión de los subespacios totalmente isotrópicos maximales de V; lo denotaremos por ind(V).

Teorema 8.3. (Teorema de descomposición de Witt) Sea V un espacio ortogonal. Se tiene que

$$V = V_0 \perp V_h \perp V_a,$$

siendo V_0 un subespacio totalmente isotrópico, V_h un subespacio hiperbólico (o cero) y V_a un subespacio anisotrópico. Además el subespacio totalmente isotrópico V_0, el subespacio hiperbólico (o cero) V_h y el subespacio anisotrópico V_a están determinados de forma única salvo una isometría.

Demostración. Veamos que esta descomposición existe. Sea W una componente no singular de V

$$V = \mathrm{rad}(V) \perp W.$$

Se tiene que $\mathrm{rad}(V)$ es totalmente isotrópico y W es no singular. Si W es isotrópico, por el lema 6.3, podemos escribir $W = P_1 \perp V_1$, donde P_1 es un plano hiperbólico. Si V_1 es también isotrópico podemos escribir $V_1 = P_2 \perp V_2$, donde P_2 es un plano hiperbólico Despues de un número finito de pasos, obtenemos una descomposición

$$V = \mathrm{rad}(V) \perp P_1 \perp \ldots \perp P_r \perp V_a,\ r \geq 0,$$

donde $\mathrm{rad}(V) = V_0$ es totalmente isotrópico, $P_1 \perp \ldots \perp P_r = V_h$ es hiperbólico (o cero) y V_a es anisotrópico. Así,

$$V = V_0 \perp V_h \perp V_a.$$

Para probar la unicidad, supongamos que $V = W_0 \perp W_h \perp W_a$, siendo W_0 un subespacio totalmente isotrópico, W_h un subespacio hiperbólico (o cero) y W_a un subespacio anisotrópico. Se tiene

$$\mathrm{rad}(\,V) = \mathrm{rad}(\,W_0) \perp \mathrm{rad}(\,W_h) \perp \mathrm{rad}(W_a) = \mathrm{rad}(\,W_0) = W_0,$$

luego $W_0 = V_0$. Por la proposición 3.13 (3), $V_h \perp V_a$ y $W_h \perp W_a$ son isométricos. Pongamos $W_h = P_1' \perp \ldots \perp P_s'$. Dado que $P_1 \cong P_1'$, por la ley de cancelación de Witt,

$$P_2 \perp \ldots \perp P_r \perp V_a \cong P_2' \perp \ldots \perp P_s' \perp W_a$$

De forma análoga, podemos cancelar un plano hiperbólico cada vez y dado que V_a y W_a son anisotrópicos tiene que ser $r = s$ y entonces $V_h \cong W_h$. Despues de cancelar los r planos hiperbólicos, obtenemos que $V_a \cong W_a$.

□

Definición 8.4. Diremos que V_a y W_a son unas *componentes anisotrópicas* de V.

Corolario 8.5. *Si (V, σ) es un espacio no singular, el índice de Witt de V coincide con $\frac{1}{2}\dim_K V_h$. El índice de Witt está determinado de forma única por la descomposición de Witt.*

Demostración. Sea U un subespacio totalmente isotrópico maximal de V, $\dim_K(U) = r$. Sea $\bar{U}$ el subespacio hiperbólico de dimensión $2r$ construido en el lema 7.2. Puesto que $\bar{U}$ es no singular, por la proposición 3.18 (4), $V = \bar{U} \perp \bar{U}^{\perp}$. El subespacio $\bar{U}^{\perp}$ es anisotrópico, puesto que si $v \in \bar{U}^{\perp}$ es un vector isótropo, entonces $U + \langle v \rangle$ es un subespacio totalmente isotrópico de V tal que $U \subsetneq U + \langle v \rangle$, lo cual contradice la maximalidad de U. Por la unicidad, salvo isometría, en el teorema de descomposición de Witt se tiene que $V_h = \bar{U}$ y $V_a = \bar{U}^{\perp}$. Así,

$$\mathrm{ind(V)} = \dim_{\mathrm{K}} \mathrm{U} = \mathrm{r} = \frac{1}{2}\ \dim_{\mathrm{K}} \mathrm{V_h}.$$

□

Proposición 8.6. *Sean V y V' espacios ortogonales no singulares. Se tiene que V y V' son isométricos si, y solo si, tienen igual dimensión y componentes anisotrópicas isométricas.*

Demostración. Sean

$$V = H \perp V_a, \quad V' = H' \perp V'_a,$$

donde H y H' son subespacios hiperbólicos y V_a y V'_a subespacios anisotrópicos. Si $f\colon V \to V'$ es una isometría, entonces $\dim_K V = \dim_K V'$ y se tiene

$$V' = f(H) \perp f(V_a),$$

donde $f(H)$ es hiperbólico y $f(V_a)$ es anisotrópico. Por el teorema de descomposición de Witt, $f(V_a)$ y V'_a son isométricos. Luego, V_a y V'_a son isométricos. Recíprocamente, si V y V' tienen igual dimensión y V_a y V'_a son isométricos, entonces H y H' tienen igual dimensión y por el lema 6.7 (2) son isométricos. Sean $f\colon H \to H'$ y $f'\colon V_a \to V'_a$ isometrías. Se tiene que $f \perp f'\colon V \to V'$ es una isometría. □

***Observación* 8.7.** De la proposición anterior se deduce que la clasificación de espacios ortogonales no singulares se reduce a la clasificación de espacios anisotrópicos. Por la proposición 3.16, la clasificación de espacios ortogonales se reduce a la clasificación de espacios no singulares. Por tanto, para clasificar espacios ortogonales basta clasificar espacios ortogonales anisotrópicos.

***Observación* 8.8.** El teorema de descomposición de Witt representa la extensión de la ley de inercia de Sylvester a cuerpos arbitrarios. En efecto, sea V un espacio ortogonal sobre un cuerpo euclidiano K, $B = \{v_1, \ldots, v_n\}$ y $B' = \{v'_1, \ldots, v'_n\}$ bases ortogonales de V. Supongamos que

$$\begin{aligned} &v_i^2 > 0,\ i = 1, \ldots, p, \quad v_i^2 < 0,\ i = p+1, \ldots, p+q, \quad v_i^2 = 0,\ = p+q+1, \ldots, n \\ &v_i'^2 > 0,\ i = 1, \ldots, p', \quad v_i^2 < 0,\ i = p'+1, \ldots, p'+q', \quad v_i'^2 = 0,\ i = p'+q', \ldots, n \end{aligned}$$

Se tiene

$$\operatorname{rad}(V) = \langle v_{p+q+1}, \ldots, v_n \rangle = \langle v'_{p'+q'+1}, \ldots v'_n \rangle,$$

y rango $\sigma = p + q = p' + q'$. Para probar la ley de inercia de Sylvester basta probar que $p = p'$. Si $p \leq q$ y $p' \leq q'$, entonces

$$\begin{aligned} V &= \langle v_1, \ldots, v_{2p} \rangle \perp \langle v_{2p+1}, \ldots, v_{p+q} \rangle \perp \operatorname{rad}(V) \\ V &= \langle v'_1, \ldots, v'_{2p'} \rangle \perp \langle v'_{2p'+1}, \ldots, v'_{p'+q'} \rangle \perp \operatorname{rad}(V), \end{aligned}$$

donde $\langle v_1, \ldots, v_{2p} \rangle$ y $\langle v'_1, \ldots, v'_{2p'} \rangle$ son hiperbólicos y $\langle v_{2p+1}, \ldots, v_{p+q} \rangle$ y $\langle v'_{2p'+1}, \ldots, v'_{p'+q'} \rangle$ son anisotrópicos. Por el teorema de descomposición de Witt los subespacios $\langle v_1, \ldots, v_{2p} \rangle$ y $\langle v'_1, \ldots, v'_{2p'} \rangle$ son isométricos. Así $p = p'$.

El caso $p \leq q$ y $p' > q'$ no se puede dar. En efecto, si $p \leq q$ y $p' > q'$ se tiene

$$V = \langle v'_1, \ldots, v'_{q'}, v'_{p'+1}, \ldots, v'_{p'+q'} \rangle \perp \langle v'_{q'+1}, \ldots, v'_{p'} \rangle \perp \operatorname{rad}(V),$$

donde $\langle v'_1, \ldots, v'_{q'}, v'_{p'+1}, \ldots, v'_{p'+q'} \rangle$ es hiperbólico y $\langle v'_{q'+1}, \ldots, v'_{p'} \rangle$ es anisotrópico definido positivo. Por el teorema de descomposición de Witt, $\langle v_{2p+1}, \ldots, v_{p+q} \rangle$ y $\langle v'_{q'+1}, \ldots, v'_{p'} \rangle$ son isométricos lo cual no puede ser cierto, puesto que $\langle v_{2p+1}, \ldots, v_{p+q} \rangle$ es definido negativo. Obsérvese que $\dim_K V_a = \mid p - q \mid$.

9. El grupo de Witt

En esta sección vamos definir el grupo de Witt de un cuerpo K. Vamos a suponer que el cuerpo K tiene característica distinta de 2.

Proposición 9.1. *Sean V y V' espacios vectoriales sobre K, σ y σ' formas bilineales simétricas sobre V y V', respectivamente. La aplicación $\sigma \oplus \sigma' \colon (V \times V') \times (V \times V') \to K$ dada por*

$$(\sigma \oplus \sigma')((v, v'), (w, w')) = \sigma(v, w) + \sigma'(v', w')$$

es una forma bilineal simétrica.

Es fácil probar que $\sigma \oplus \sigma'$ es una aplicación bilineal simétrica.

***Notación* 9.2.** Si (V, σ) y (V', σ') son espacios ortogonales sobre K, denotaremos por $(V \oplus V', \sigma \oplus \sigma')$ o por $V \oplus V'$ el espacio ortogonal $(V \times V', \sigma \oplus \sigma')$ y lo llamaremos la *suma ortogonal externa* de (V, σ) y (V', σ') .

Lema 9.3. (1) *Sean V y V' espacios ortogonales sobre K. Se tiene*

(a) *Las aplicaciones $i \colon V \to V \times \{0\}$ y $j \colon V' \to \{0\} \times V'$ dadas por:*

$$i(v) = (v, 0), \quad j(v') = (0, v')$$

son isometrías y $V \oplus V' = i(V) \perp j(V')$.

(b) *Si V y V' son no singulares, entonces $V \oplus V'$ es no singular.*

(c) *Sean B y B' bases de V y V', respectivamennte. La matriz de Gram de $\sigma \oplus \sigma'$ en la base $i(B) \cup j(B')$ es la matriz*

$$\left(\begin{array}{c|c} G_\sigma^B & 0 \\ \hline 0 & G_{\sigma'}^{B'} \end{array}\right).$$

(d) *Los espacios ortogonales $(V \oplus V')_a$ y $(V_a \oplus V_a')_a$ son isométricos.*

(e) *$V \oplus V'$ y $V' \oplus V$ son espacios isométricos.*

(f) *Sea V'' otro espacio ortogonal sobre K. Se tiene que $(V \oplus V') \oplus V''$ y $V \oplus (V' \oplus V'')$ son espacios isométricos.*

(2) *Sean V, W, V' y W' espacios ortogonales sobre K. Si $f \colon V \to W$ y $f' : V' \to W'$ son isometrías, entonces la aplicación*

$$f \oplus f' \colon V \oplus V' \to W \oplus W'$$

dada por $(f \oplus f')(v, v') = (f(v), f'(v'))$, es una isometría.

Demostración. (1) (a) Las aplicaciones $i \colon V \to V \times \{0\}$ y $j : V' \to \{0\} \times V'$ son isometrías ya que $(\sigma \oplus \sigma')(i(v), i(w)) = (\sigma \oplus \sigma')((v, 0)(w, 0)) = \sigma(v, w)$ y $(\sigma \oplus \sigma')(j(v'), j(w')) = (\sigma \oplus \sigma')((0, v'), (0, w')) = \sigma'(v', w')$.

Además se tiene

$$(v, v') = (v, 0) + (0, v') = i(v) + j(v)$$
$$(\sigma \oplus \sigma')((v, 0), (0, v')) = \sigma(v, 0) + \sigma(0, v') = 0$$

Por tanto $V \oplus V' = i(V) \perp j(V')$.

(1) (b) Si V y V' son no singulares, entonces $i(V)$ y $j(V')$ son no singulares y por la proposición 3.13, $i(V) \perp j(V')$ es no singular.

(1) (c) Sean $B = \{v_1, \ldots, v_n\}$, $B' = \{v'_1, \ldots, v'_n\}$ bases de V y V', respectivamente. Se tiene que $i(B)$ es base de $i(V)$ y $j(B')$ es base de $j(V')$. Por tanto $i(B) \cup j(B')$ es una base de $i(V) \perp j(V')$. Dado que

$$\begin{aligned}(\sigma \oplus \sigma')((v_i, 0)(v_j, 0)) &= \sigma(v_i, v_j)\\ (\sigma \oplus \sigma')((v_i, 0)(0, v'_j)) &= \sigma(v_i, 0) + \sigma'(0, v'_j) = 0\\ (\sigma \oplus \sigma')((0, v'_i)(0, v'_j)) &= \sigma'(v'_i, v'_j),\end{aligned}$$

se tiene

$$G_{\sigma\oplus\sigma'}^{i(B)\cup j(B')} = \left(\begin{array}{c|c} G_\sigma^B & 0 \\ \hline 0 & G_{\sigma'}^{B'} \end{array}\right),$$

(1) (d) Se sigue del teorema de descomposición de Witt. En efecto,

$$\begin{aligned}(V \oplus V')_a =& (i(V) \perp j(V'))_a = (i(V)_a \perp i(V)_h \perp j(V')_a \perp j(V')_h)_a\\ =& (i(V)_a \perp j(V')_a)_a,\end{aligned}$$

y $(i(V)_a \perp j(V')_a)_a$ es isométrico a $(i(V_a) \perp j(V'_a))_a = (V_a \oplus V'_a)_a$.

(1) (e) La aplicación $f\colon V \oplus V' \to V' \oplus V$, $f(v, v') = (v', v)$ es una isometría. En efecto,

$$\begin{aligned}(\sigma' \oplus \sigma)(f(v, v'), f(w, w')) =& (\sigma' \oplus \sigma)((v', v), (w', w)) = \sigma'(v', w') + \sigma(v, w)\\ =& (\sigma \oplus \sigma')((v, v'), (w, w')).\end{aligned}$$

(1) (f) Es fácil probar que la aplicación $f\colon (V \oplus V') \oplus V'' \to V' \oplus (V \oplus V'')$, dada por $f((v, v'), v'') = (v, (v', v''))$, es una isometría.

(2) Utilizando la notación $v \cdot w$ para la imagen por una forma bilineal del par (v, w) se tiene

$$\begin{aligned}(v_1, v'_1) \cdot (v_2, v'_2) =& v_1 \cdot v_2 + v'_1 \cdot v'_2 = f(v_1) \cdot f(v_2) + f'(v'_1) \cdot f'(v'_2)\\ =& (f(v_1), f'(v'_1)) \cdot (f(v_2), f'(v'_2)).\end{aligned}$$

□

Consideremos en la colección de espacios anisotrópicos la relación de equivalencia "ser isométricos". Si (V, σ) es un espacio anisotrópico, denotaremos por $[(V, \sigma)]$ o simplemente por $[V]$ su clase de isometría, es decir su clase de equivalencia con respecto a la relación "ser isométricos". Denotaremos por $W(K)$ el conjunto de clases de isometría de espacios anisotrópicos.

Proposición 9.4. *El conjunto $W(K)$ es un grupo. con la operación adición*

$$[V] \oplus [V'] = [(V \oplus V')_a],$$

donde $(V \oplus V')_a$ es la parte anisotrópica de $V \oplus V'$.

Demostración. La adición está bien definida ya que por el lema 9.3 se tiene que si V y V_1 son isométricos y V' y V'_1 son isométricos, entonces $V \oplus V'$ y $V_1 \oplus V'_1$ son isométricos y entonces por la proposición 8.6, $(V \oplus V')_a$ y $(V_1 \oplus V'_1)_a$ son también isométricos. La adición verifica la propiedad conmutativa ya que por el lema 9.3 los espacios $V \oplus V'$ y $V' \oplus V$ son isométricos y entonces $(V \oplus V')_a$ y $(V' \oplus V)_a$ son también isométricos. Así,

$$[V] \oplus [V'] = [(V \oplus V')_a] = [(V' \oplus V)_a] = [V'] \oplus [V].$$

La adición tiene elemento neutro ya que $[0] \oplus [V] = [(0 \oplus V)_a] = [V]$. La adición verifica la propiedad asociativa ya que por la proposición 9.3 (1) (d) y (f) y la proposición 8.6 se tiene

$$\begin{aligned}([V] \oplus [V']) \oplus [V''] =&[((V \oplus V')_a \oplus V'')_a] = [((V \oplus V') \oplus V'')_a] = [((V \oplus (V' \oplus V''))_a] \\ =&[(V \oplus (V' \oplus V'')_a)_a] = [V] \oplus ([V'] \oplus [V'']).\end{aligned}$$

La clase opuesta de $[(V, \sigma)]$ es la clase $[(V, -\sigma)]$. En efecto, sea $B = \{v_1, \ldots, v_n\}$ una base ortogonal de (V, σ). La base B también es base ortogonal de $(V, -\sigma)$. Si $\sigma(v_i, v_i) = a_i$, $i = 1, \ldots, n$, entonces

$$G_\sigma^B = \ \operatorname{diag}(a_1, \ldots, a_n), \quad G_{-\sigma}^B = \operatorname{diag}(-a_1, \ldots, -a_n)$$

y

$$G_{\sigma \oplus -\sigma}^{i(B) \bigcup j(B)} = \operatorname{diag}(a_1, \ldots, a_n, -a_1, \ldots, -a_n)$$

Se tiene

$$(V \oplus V, \sigma \oplus -\sigma) = \langle i(v_1), j(v_1) \rangle \perp \ldots \perp \langle i(v_n), j(v_n) \rangle$$

Cada $H_k = \langle i(v_k), j(v_k) \rangle$, $k = 1, \ldots, n$, es un plano hiperbólico, ya que la matriz de Gram de $(\sigma \oplus -\sigma)|_{H_k}$ en la base $\{i(v_k), j(v_k)\}$ es la matriz

$$\begin{pmatrix} a_k & 0 \\ 0 & -a_k \end{pmatrix},$$

que es regular y H_k tiene un vector isótropo, el vector $i(v_k) + j(v_k)$. Por tanto $(V \oplus V, \sigma \oplus -\sigma)$ es un espacio hiperbólico y por el teorema de descomposición de Witt su parte anisotrópica es $(0, 0)$. Así,

$$[(V, \sigma)] \oplus [(V, -\sigma)] = [(V \oplus V', \sigma \oplus -\sigma)_a] = [0].$$

□

Definición 9.5. Se llama *grupo de Witt* del cuerpo K al grupo $W(K)$.

***Observación* 9.6.** Si $\sigma \colon V \times V \to K$ y $\sigma' \colon V' \times V' \to K$ son formas bilineales simétricas, entonces la aplicación $\sigma \otimes \sigma' \colon (V \otimes_K V') \times (V \otimes_K V') \to K$ dada por

$$(\sigma \otimes \sigma')((v \otimes v'), (w \otimes w')) = \sigma(v, w)\, \sigma'(v', w')$$

es una forma bilineal simétrica. Si denotamos por $V \otimes_K V'$ el espacio ortogonal $(V \otimes_K V', \sigma \otimes \sigma')$, entonces $W(K)$ es un anillo commutativo y unitario con la operación producto

$$[(V, \sigma)] \otimes [(V', \sigma')] = [(V \otimes_K V')_a],$$

donde $(V \otimes_K V')_a$ es la parte anisotrópica de $V \otimes_K V'$. Con este producto $W(K)$ se denomina el anillo de Witt de K. El elemento unidad del anillo es el espacio ortogonal $\langle 1 \rangle$.

Demostración. Se razona como en la proposición 9.4. □

Definición 9.7. Se llama *ideal fundamental* del anillo de Witt $W(K)$ al conjunto

$$I(K) = \{[V] \in W(K) \mid \dim_K V \text{ par}\}$$

***Observación* 9.8.** $I(K)$ es un ideal de $W(K)$. En efecto, si $[V],[V'] \in I(K)$, $\dim_K V = 2m$, $\dim_K V' = 2n$, entonces $(V \oplus V')_a$ tiene dimensión par, puesto que $\dim_K(V \oplus V') = 2(m+n)$, la dimensión de $(V \oplus V')_h$ es par y

$$V \oplus V' = (V \oplus V')_a \perp (V \oplus V')_h.$$

Además, $[0] \in I(K)$ y si $[(V,\sigma)] \in I(K)$ entonces $-[(V,\sigma)] = [(V,-\sigma)] \in I(K)$. Si $[V] \in W(K)$, $\dim V = m$, y $[V'] \in I(K)$, $\dim V' = 2n$, se tiene que $\dim_K(V \otimes_K V') = 2mn$ y entonces $(V \otimes_K V')_a$ tiene dimensión par. Así, $[V] \otimes [V'] \in I(K)$.

Definición 9.9. Se llama *discriminante con signo* de un espacio ortogonal no singular V al elemento de K^*/K^{*2} dado por

$$\mathrm{dis}_\pm(\mathrm{V}) = (-1)^{\mathrm{n(n-1)/2}}\,\mathrm{dis(V)},$$

donde $\dim_K V = n$ y dis(V) es el discriminante de V de la definición 2.6.

***Observación* 9.10.** El *discriminante con signo* de un espacio hiperbólico es K^{*2}. En efecto, por el lema 6.7, si H es un espacio hiperbólico de dimensión $2r$, $\mathrm{dis(H)} = (-1)^{\mathrm{r}}\,\mathrm{K}^{*2}$.

Lema 9.11. *Si V es un espacio ortogonal no singular, entonces* $\mathrm{dis}_\pm(\mathrm{V}) = \mathrm{dis}_\pm(\mathrm{V_a})$*, siendo V_a una componente anisotrópica de V.*

Demostración. Pongamos $V = V_a \perp V_h$, $\dim_K V = m$, $\dim_K V_a = n$ y $\dim_K V_h = 2r$. Se tiene

$$\begin{aligned}\mathrm{dis}_\pm(\mathrm{V}) =& (-1)^{m(m-1)/2}\,\mathrm{dis(V)} = (-1)^{\mathrm{(n+2r)(n+2r-1)/2}}\mathrm{dis(V)}\\ =& (-1)^{n(n-1)/2}\,(-1)^{2r(2r-1)/2}\,\mathrm{dis(V_a)\,dis(V_h)}\\ =& (-1)^{n(n-1)/2}\,\mathrm{dis(V_a)} = \mathrm{dis}_\pm(\mathrm{V_a})\end{aligned}$$

□

***Observación* 9.12.** Dado que espacios ortogonales sobre K no singulares e isométricos tiene el mismo discriminante, se tiene una aplicación

$$\begin{array}{rcl}\mathrm{dis}_\pm\colon \mathrm{W(K)} & \to & K^*/K^{*2}\\ [(V,\sigma])& \longmapsto & (-1)^{n(n-1)/2}\,\mathrm{disc(V},\sigma)\\ 0 & \longmapsto & K^{*2},\end{array}$$

donde $\dim_K V = n$, que llamaremos *aplicación discriminante con signo*. Sin embargo, $\mathrm{dis}_\pm$ no es en general un homomorfismo de grupos. Por ejemplo $\mathrm{dis}_\pm([\langle 1\rangle]) = 1$, pero $\mathrm{dis}_\pm([\langle 1\rangle] \oplus [\langle 1\rangle]) = -1$, si $-1 \notin K^{*2}$. Sin embargo, la aplicación restricción de $\mathrm{dis}_\pm$ al ideal fundamental $I(K)$, que denotaremos también por $\mathrm{dis}_\pm$, es un homomorfismo de grupos,

Proposición 9.13. *La aplicación* $\mathrm{dis}_\pm\colon \mathrm{I(K)} \to \mathrm{K}^*/\mathrm{K}^{*2}$*,* $\mathrm{dis}_\pm([\mathrm{V}]) = (-1)^{\mathrm{r}}\,\mathrm{disc(V)}$*, si* $\dim V = 2r > 0$ *y* $\mathrm{dis}_\pm([0]) = \mathrm{K}^{*2}$*, es un homomorfismo de grupos suprayectivo.*

Demostración. Sean $[V]$ y $[V']$ elementos de $I(K)$, $\dim_K V = 2m$ y $\dim_K V' = 2n$. Se tiene

$$\mathrm{dis}_\pm(\mathrm{V}) = (-1)^{\mathrm{m}}\mathrm{dis(V)},\ \mathrm{dis}_\pm(\mathrm{V'}) = (-1)^{\mathrm{n}}\mathrm{dis(V')},\ \mathrm{dis}_\pm(\mathrm{V}\oplus\mathrm{V'}) = (-1)^{\mathrm{m}}\mathrm{dis(V}\oplus\mathrm{V'}).$$

Así,

$$\begin{aligned}\mathrm{dis}_\pm([\mathrm{V}]\oplus[\mathrm{V'}]) =& \mathrm{dis}_\pm((\mathrm{V}\oplus\mathrm{V'})_\mathrm{a}) = \mathrm{dis}_\pm(\mathrm{V}\oplus\mathrm{V'}) = (-1)^{\mathrm{(m+n)}}\mathrm{dis(V}\oplus\mathrm{V'})\\ =& (-1)^{(m+n)}\mathrm{dis(V)\,dis(V')} = \mathrm{dis}_\pm([\mathrm{V}])\,\mathrm{dis}_\pm([\mathrm{V'}]).\end{aligned}$$

La aplicación $\mathrm{dis}_\pm\colon \mathrm{I(K)} \to \mathrm{K}^*/\mathrm{K}^{*2}$ es suprayectiva, puesto que $d(0) = K^{*2}$ y si $a \in K^* - K^{*2}$ entonces $d([\langle 1,-a\rangle]) = a\,K^{*2}$. □

10. Ejemplos

El problema de clasificar espacios ortogonales no singulares sobre un cuerpo K es esencialmente equivalente al cálculo de su grupo de Witt . Por la ley de cancelación de Witt distintas clases de isometría de espacios ortogonales no singulares corresponden a diferentes elementos de $W(K)$. El cálculo del grupo de Witt es uno de los problemas básicos de la teoría de espacios ortogonales.

En esta sección se calcula el grupo de Witt de un cuerpo cuadráticamente cerrado y se caracterizan los cuerpos euclidianos o los pitagóricos por la estructura de su grupo de Witt.

Teorema 10.1. *Si K es un cuerpo cuadráticamente cerrado, entonces el grupo $W(K)$ es isomorfo al grupo $\mathbb{Z}/2\mathbb{Z}$.*

Demostración. Si K es un cuerpo cuadráticamente cerrado, los espacios anisotrópicos sobre K son el $\langle 0\rangle$ y los espacios ortogonales no singulares de dimensión 1. Por tanto

$$W(K) = \{[\langle 0\rangle], [\langle 1\rangle\},$$

es un grupo cíclico de orden 2. La aplicación

$$\begin{aligned} \mathbf{d}\colon\ W(K) &\longrightarrow \mathbb{Z}/2\,\mathbb{Z} \\ [\langle 0\rangle] &\rightsquigarrow\ 2\,\mathbb{Z} \\ [\langle 1\rangle] &\rightsquigarrow 1+2\,\mathbb{Z} \end{aligned}$$

es un isomorfismo de grupos. □

Teorema 10.2. *Son equivalentes*

(1) *K es un cuerpo euclidiano.*

(2) *El grupo $W(K)$ es isomorfo al grupo $\mathbb{Z}$ de los números enteros.*

Demostración. (1) $\Rightarrow$ (2) Sea K un cuerpo euclidiano (definición 5.11). Los espacios anisotrópicos sobre K son los espacios de signatura $(n,0)$ y los espacios de signatura $(0,n)$, $n \in \mathbb{N}$. Existen exactamente dos clases de isomorfía de espacios anisotrópicos en cada dimensión $n > 0$, la clase de los espacios de signatura $(n,0)$ de la cual un representante es el espacio $\langle 1,\overset{n}{\ldots},1\rangle$ y la de los espacios de signatura $(0,n)$, de la cual un representante es el espacio $\langle -1,\overset{n}{\ldots},-1\rangle$. Dado que

$$[\langle 1,\overset{n}{\ldots},1\rangle] = n\,[\langle 1\rangle], \quad [\langle -1,\overset{n}{\ldots},-1\rangle] = n\,[\langle -1\rangle] = (-n)\,[\langle 1\rangle]$$

se tiene que

$$W(K) = \{n\,[\langle 1\rangle] \mid n \in \mathbb{Z}\}$$

es el grupo cíclico generado por $[\langle 1\rangle]$. La aplicación signatura

$$\begin{aligned} \mathbf{s}\colon\ W(K) &\longrightarrow \mathbb{Z} \\ n[\langle 1\rangle] &\rightsquigarrow\ n \end{aligned}$$

es un isomorfismo de grupos.

(2) $\Rightarrow$ (1) Puesto que $W(K) \cong \mathbb{Z}$, el ideal fundamental $I(K)$ es un grupo cíclico. Dado que la aplicación discriminante con signo $\mathrm{dis}_{\pm}\colon \mathrm{I(K)} \to \mathrm{K^*/K^{*2}}$ es un homomorfismo de grupos sobreyectivo, K^*/K^{*2} es un grupo cíclico. Los elementos de K^*/K^{*2} distintos de K^{*2} tienen orden 2, luego

$\mid K^*/K^{*2} \mid \leq 2$. El caso $\mid K^*/K^{*2} \mid = 1$ no es posible, por 10.1. El elemento $[\langle 1\rangle]$ de $W(K)$ no tiene orden aditivo 2, luego $[\langle 1\rangle] \oplus [\langle 1\rangle] = [\langle 1, 1\rangle]$ es anisotrópico. Así, $-1 \notin K^{*2}$ y $K^*/K^{*2} = \{K^{*2}, -K^{*2}\}$.

Veamos que -1 no es suma de dos cuadrados. Supongamos que $-1 = a^2 + b^2$, $a, b \in K$ y consideremos el vector $u = (a, b) \in \langle 1, 1\rangle$. Se tiene que $u^2 = -1$ y si $w \in \langle u\rangle^{\perp}$, $w \neq 0$, entonces $\{u, w\}$ es una base ortogonal de $\langle 1, 1\rangle$ y $G_{\sigma}^{\{u,w\}} = \operatorname{diag}(-1, w^2)$, donde σ denota la estructura métrica en $\langle 1, 1\rangle$. Se tiene que $\operatorname{dis}\langle 1, 1\rangle = -w^2\, K^{*2}$, luego $w^2 = -c^2$ para algún $c \in K^*$. Si $v = c^{-1}\, w$, $v^2 = -1$ y entonces $G_{\sigma}^{\{u,v\}} = \operatorname{diag}(-1, -1)$, Así, $\langle 1, 1\rangle \cong \langle -1, -1\rangle$ y se tiene

$$4\,[\langle 1\rangle] = [\langle 1, 1\rangle] \oplus [\langle 1, 1\rangle] = [\langle 1, 1\rangle] \ominus [\langle -1, -1\rangle] = [(\langle 1, 1, -1, -1\rangle)_a] = [(\langle 1, -1\rangle + \langle 1, -1\rangle)_a] = 0,$$

puesto que $\langle 1, -1\rangle$ es un plano hiperbólico. Así, $[\langle 1\rangle]$ es un elemento de $W(K)$ de orden 4, lo que contradice que $W(K)$ es un grupo cíclico infinito.

Dado que $K^*/K^{*2} = \{K^{*2}, -K^{*2}\}$, se tiene que $K = K^{*2} \sqcup \{0\} \sqcup -K^{*2}$. Puesto que -1 no es suma de dos cuadrados, $a^2 + b^2 \notin -K^{*2}$, para todo $a, b \in K^*$ y así, $a^2 + b^2 \in K^{*2}$. Por tanto, $K^{*2} + K^{*2} \subset K^{*2}$. □

***Observación* 10.3.** Los isomorfismos de grupos **s** y **d** de los teoremas 10.1 y 10.2 son también isomorfismos de anillos.

Definición 10.4. Un cuerpo K es *pitagórico* si toda suma de dos cuadrados es un cuadrado.

Los cuerpos cuadráticamente cerrados y los cuerpos euclidianos son pitagóricos. Los cuerpos de característica 2 son pitagóricos, puesto que si K es un cuerpo de característica 2, $a^2 + b^2 = (a + b)^2$, para todo $a, b \in K$.

Teorema 10.5. *Sea K un cuerpo de característica distinta de 2. Son equivalentes*

(1) *K es un cuerpo pitagórico.*

(2) *$W(K) \cong \mathbb{Z}/2\,\mathbb{Z}$ o $W(K)$ es libre de torsión.*

Demostración. (1) $\Rightarrow$ (2) Si todo elemento de K es un cuadrado, entonces $W(K) \cong \mathbb{Z}/2\,\mathbb{Z}$ por el teorema 10.1.

Supongamos que no todo elemento es un cuadrado. Veamos que -1 no es suma de cuadrados. En efecto, si -1 es suma de cuadrados, entonces -1 es un cuadrado por ser K pitagórico y dado que todo elemento de K es una diferencia de cuadrados, para cada $x \in K$, existen $a, b \in K$ tales que $x = a^2 - b^2 = a^2 + (-1)\, b^2 \in K^2$, lo que contradice que $K \neq K^2$.

Para probar que $W(K)$ es libre de torsión consideremos un espacio anisotrópico $\langle a_1, \ldots, a_n\rangle$. Veamos que la suma ortogonal

$$\langle a_1, \ldots, a_n\rangle \overset{k)}{\ominus \ldots \ominus} \langle a_1, \ldots, a_n\rangle,$$

es un espacio anisotrópico. Supongamos que existe un vector isótropo

$$v = (x_{11}, \ldots, x_{1n}, \ldots, x_{k1}, \ldots, x_{kn}) \in \langle a_1, \ldots, a_n\rangle \ominus \ldots \ominus \langle a_1, \ldots, a_n\rangle.$$

Se tiene

$$a_1\,(x_{11}^2 + \ldots + x_{k1}^2) + \ldots + a_n\,(x_{1n}^2 + \ldots + x_{kn}^2) = 0.$$

con algún $x_{ij} \neq 0$. Dado que K es pitagórico, $x_{1j}^2 + \ldots + x_{kj}^2 = y_j^2$, para algún $y_j \in K$, $j = 1, \ldots, k$ y como -1 no es suma de cuadrados, algún $y_j \neq 0$. Así,

$$a_1\, y_1^2 + \ldots + a_n\, y_n^2 = 0.$$

con algún $y_j \neq 0$ y el vector $u = (y_1, \ldots, y_n) \in \langle a_1, \ldots, a_n \rangle$ es un vector isótropo, lo cual es una contradicción. Por tanto $k\,[\langle a_1, \ldots, a_n \rangle] \neq 0$ en $W(K)$.

(2) $\Rightarrow$ (1) Supongamos que $x \in K^*$ es suma de cuadrados, $x = a^2 + b^2$, pero no es un cuadrado. Entonces $W(K) \neq \mathbb{Z}/2\,\mathbb{Z}$. Consideremos el vector $u = (a, b) \in \langle 1, 1 \rangle$. Sea $w \in \langle u \rangle^{\perp}$, $w \neq 0$. Se tiene que $G_{\sigma}^{\{u,w\}} = \operatorname{diag}(x, w^2)$. Dado que $\operatorname{dis}(\langle 1, 1 \rangle) = K^{*2} = x\,w^2\,K^{*2}$, existe $c \in K^*$ tal que $x\,w^2\,c^2 = 1$. Si $v = c\,x\,w$, entonces $v^2 = x$ y por el corolario 2.17, $\langle 1, 1 \rangle \cong \langle x, x \rangle$. Dado que x no es un cuadrado, el plano $\langle 1, -x \rangle$ es anisotrópico, luego $[\langle 1, -x \rangle] \neq 0$ y se tiene

$$\begin{aligned} 2\,[\langle 1, -x \rangle] &= [\langle 1, -x \rangle] \oplus [\langle 1, -x \rangle] = [\langle 1, -x, 1, -x \rangle] = [\langle 1, 1 \rangle] \oplus [\langle -x, -x \rangle] \\ &= [\langle x, x \rangle] \oplus [\langle -x, -x \rangle] = [\langle x, -x \rangle] \oplus [\langle x, -x \rangle] = 0, \end{aligned}$$

por ser $\langle x, -x \rangle$ un plano hiperbólico Por tanto, si x es suma de cuadrados pero no es un cuadrado, $W(K)$ es un grupo con torsión.

□

Corolario 10.6. *Sea K es un cuerpo pitagórico de característica distinta de 2. Se tiene que $W(K) \cong \mathbb{Z}/2\,\mathbb{Z}$ si, y solo si, -1 es un cuadrado.*

Demostración. Si $-1 = a^2$, con $a \in K^*$ y $w = a\,e_2$, entonces $G_{\sigma}^{\{e_1,w\}} = \operatorname{diag}(1, -1)$, luego $\langle 1, 1 \rangle \cong \langle 1, -1 \rangle$ es un espacio universal. Así, todo elemento de K es una suma de 2 cuadrados, luego un cuadrado. Por el teorema 10.1, $W(K) \cong \mathbb{Z}/2\,Z$. Recíprocamente, si -1 no es un cuadrado, entonces por el teorema anterior, $W(K) \ncong \mathbb{Z}/2\,Z$.

□

11. Espacios ortogonales sobre cuerpos finitos

En este capítulo vamos a estudiar los espacios ortogonales sobre cuerpos finitos. Por la proposición 3.16, nos limitaremos a clasificar espacios ortogonales no singulares. Veremos que los espacios ortogonales sobre cuerpos finitos se clasifican por su dimensión y su discriminante.

Sea $\mathbb{F}_q$ un cuerpo de característica $p \neq 2$ de q elementos ($q = p^n$, p primo, $p \neq 2$) y $\mathbb{F}_q^*$ el grupo multiplicativo de los elementos no nulos de $\mathbb{F}_q$.

Lema 11.1. *La aplicación*

$$\begin{aligned} f \colon \mathbb{F}_q^* &\to \mathbb{F}_q^* \\ x &\rightsquigarrow x^2 \end{aligned}$$

es un homomorfismo de grupos cuya imagen $\mathbb{F}_q^{*2} = \{a^2 \mid a \in \mathbb{F}_q\}$ tiene orden $(q-1)/2$ e índice 2 en $\mathbb{F}_q^*$. Si $s \in \mathbb{F}_q^* - \mathbb{F}_q^{*2}$, entonces todo elemento de $\mathbb{F}_q^* - \mathbb{F}_q^{*2}$ es de la forma $s\,x^2$ con $x \in \mathbb{F}_q^*$. Además, todo elemento de $\mathbb{F}_q$ es suma de dos cuadrados.

Demostración. Dado que $\mathbb{F}_q^*$ es un grupo abeliano f es un homomorfismo de grupos. El núcleo de f es $\{1, -1\}$ y su grupo imagen $f(\mathbb{F}_q^*) = \mathbb{F}_q^{*2}$ tiene orden $(q-1)/2$, por ser isomorfo al grupo $\mathbb{F}_q^*/\{1, -1\}$. Por el teorema de Lagrange $\mathbb{F}_q^{*2}$ tiene índice 2 en $\mathbb{F}_q^*$. Así,

$$\mathbb{F}_q^*/\mathbb{F}_q^{*2} = \{\, \mathbb{F}_q^{*2}\,,\, s\,\mathbb{F}_q^{*2}\,\}, \quad s \in \mathbb{F}_q^* - \mathbb{F}_q^{*2},$$

y entonces $\mathbb{F}_q^* - \mathbb{F}_q^{*2} = s\,\mathbb{F}_q^{*2}$.

Todo elemento de $\mathbb{F}_q$ es suma de dos cuadrados. En efecto, sea $x \in \mathbb{F}_q$ y consideremos los conjuntos

$$\mathbb{F}_q^2 = \{a^2 \mid a \in \mathbb{F}_q\}, \quad x - \mathbb{F}_q^2 = x - \{a^2 \mid a \in \mathbb{F}_q\}.$$

Dado que los conjuntos $\mathbb{F}_q^2$ y $x - \mathbb{F}_q^2$ tienen cada uno $(q+1)/2$ elementos, su intersección es no vacía. Por tanto, existen $a, b \in \mathbb{F}_q$ tales que $x = a^2 + b^2$. □

Proposición 11.2. *Sea (V, σ) un espacio ortogonal no singular sobre $\mathbb{F}_q$ de dimensión 1. El espacio (V, σ) es isométrico al espacio ortogonal $\langle 1 \rangle$ o al espacio ortogonal $\langle s \rangle$.*

Demostración. Sea $V = \langle u \rangle$. Se tiene que $u^2 = a^2$ o $u^2 = s\,b^2$, con $a, b \in F_q^*$. Pongamos $v = a^{-1}\,u$, si $u^2 = a^2$, o $v = b^{-1}\,u$, si $u^2 = s\,b^2$. Se tiene que $v^2 = 1$ o $v^2 = s$. Si $B = \{v\}$, entonces

$$G_\sigma^B = \begin{pmatrix} 1 \end{pmatrix} \quad \text{o} \quad G_\sigma^{B'} = \begin{pmatrix} s \end{pmatrix}.$$

El resultado se sigue del teorema 2.16. □

Lema 11.3. *Sea (V, σ) un espacio ortogonal no singular sobre $\mathbb{F}_q$ de dimensión 2. Existe $v \in V$ tal que $v^2 = 1$.*

Demostración. Sea $s = a^2 + b^2$, $a, b \in \mathbb{F}_q$, y $u \in V$ tal que $u^2 \neq 0$.

Si $u^2 \in \mathbb{F}_q^{*2}$, entonces $u^2 = x^2$ para algún $x \in \mathbb{F}_q^*$ y tomamos $v = x^{-1}\,u$.

Si $u^2 \notin \mathbb{F}_q^{*2}$, pongamos $V = \langle u \rangle \perp \langle w \rangle$. Si $w^2 \in \mathbb{F}_q^{*2}$, entonces $w^2 = y^2$, con $y \in \mathbb{F}_q^*$, y tomamos $v = y^{-1}\,w$. Si $w^2 \notin \mathbb{F}_q^{*2}$, existen $x, y \in \mathbb{F}_q^*$ tales que $u^2 = x^2\,s$ y $w^2 = y^2\,s$ y tomamos $v = a(xs)^{-1}\,u + b(ys)^{-1}\,w$. □

Proposición 11.4. *Sea (V, σ) un espacio ortogonal no singular sobre $\mathbb{F}_q$ de dimensión 2. El espacio (V, σ) es isométrico al espacio ortogonal $\langle 1, -1 \rangle$ o al espacio ortogonal $\langle 1, -s \rangle$.*

Demostración. Por el lema 11.3, existe $u \in V$ tal que $u^2 = 1$. Pongamos $V = \langle u \rangle \perp \langle w \rangle$. Se tiene que $-w^2 = a^2$ o $-w^2 = s\,b^2$ con $a, b \in F_q^*$. Si $v = a^{-1}w$, cuando $-w^2 = a^2$ o $v = b^{-1}\,w$, cuando $-w^2 = s\,b^2$, entonces $v^2 = -1$ o $v^2 = -s$. Además, $V = \langle u \rangle \perp \langle v \rangle$. Si $B = \{u, v\}$, entonces

$$G_\sigma^B = \operatorname{diag}(1, -1) \quad \text{o} \quad G_\sigma^{B'} = \operatorname{diag}(1, -s).$$

Obsérvese que si $v^2 = -1$, entonces V es un plano hiperbólico y que si $v^2 = -s$, V es un plano anisotrópico. El resultado se sigue del teorema 2.16. □

Lema 11.5. *Si (V, σ) es un espacio ortogonal no singular sobre $\mathbb{F}_q$ de dimensión 2, entonces es universal.*

Demostración. Si $B = \{u, v\}$ es una base de V tal que $G_\sigma^B = \operatorname{diag}(1, -1)$, entonces (V, σ) es un plano hiperbólico y por el lema 6.9 es universal.

Supongamos que $G_\sigma^B = \operatorname{diag}(1, -\mathrm{s})$ y sea $\lambda \in \mathbb{F}_q$. Si $\lambda = a^2$ para algún $a \in \mathbb{F}_q^*$, entonces $(a\,u)^2 = \lambda$. Si $\lambda \notin \mathbb{F}_q^{*2}$, entonces $\lambda = a^2 + b^2 = c^2 s$, donde $a, b, c \in \mathbb{F}_q$ Si $-1 \in \mathbb{F}_q^{*2}$, entonces $-1 = d^2$ para algún $d \in \mathbb{F}_q$ y si $-1 \notin \mathbb{F}_q^{*2}$, entonces $s = -d^2$ para algún $d \in \mathbb{F}_q$. Si $\lambda \notin \mathbb{F}_q^{*2}$ y $-1 \in \mathbb{F}_q^{*2}$, entonces $(c\,d\,v)^2 = \lambda$. Si $\lambda \notin \mathbb{F}_q^{*2}$ y $-1 \notin \mathbb{F}_q^{*2}$, entonces $(a\,u + b\,d^{-1}\,v)^2 = \lambda$.

□

Lema 11.6. *Si V es un espacio ortogonal no singular sobre $\mathbb{F}_q$ de dimensión $n \geq 3$, entonces V es un espacio isótropo.*

Demostración. Por el lema 3.20, existe $v_1 \in V$ tal que v_1 es no isótropo. Puesto que V es no singular, $V = \langle v_1 \rangle \perp \langle v_1 \rangle^\perp$. Por ser $\langle v_1 \rangle^\perp$ no singular existe $v_2 \in \langle v_1 \rangle^\perp$ tal que v_2 es no isótropo. Los vectores $\{v_1, v_2\}$ son linealmente independientes puesto que si $v_2 = \lambda v_1$, entonces $v_2 \in \langle v_1 \rangle \cap \langle v_1 \rangle^\perp = \{0\}$. El plano $P = \langle v_1, v_2 \rangle$ es no singular y por ser V no singular, $P^\perp$ es no singular.

Sea $v \in P^\perp$ un vector no isótropo. Por el lema 11.5, existe un vector $w \in P$ tal que $w^2 = -v^2$. Se tiene que $v + w \neq 0$, y además

$$(v + w)^2 = v^2 + w^2 = 0. \qquad \square$$

Así, $v + w$ es un vestor isótropo de V.

Proposición 11.7. *Sea (V, σ) un espacio ortogonal no singular sobre $\mathbb{F}_q$ de dimensión $n \geq 3$.*

(1) *Si n es par, entonces (V, σ) es isométrico al espacio ortogonal $\langle 1, -1, \cdots, 1, -1 \rangle$ o al espacio ortogonal $\langle 1, -1, \cdots, 1, -1, 1, -s \rangle$.*

(2) *Si n es impar, entonces (V, σ) es isométrico al espacio ortogonal $\langle 1, -1, \cdots, 1, -1, 1 \rangle$ o al espacio ortogonal $\langle 1, -1, \cdots, 1, -1, s \rangle$.*

Demostración. (1) Sea n par. Si V es hiperbólico, por el lema 6.6, existe una base en la cual la matriz de Gram de σ es

$$\operatorname{diag}(1, -1, \cdots, 1, -1).$$

Si V no es hiperbólico, por el teorema de descomposición de Witt se tiene que $V = V_h \perp V_a$ y por el lema 11.6, $\dim V_a = 2$. Por la proposición 11.4 y por el lema 6.6, existe una base donde la matriz de Gram de σ es

$$\operatorname{diag}(1, -1, \cdots, 1, -1, 1, -s).$$

(2) Si n es impar, por el teorema de descompomposición de Witt, $V = V_h \perp V_a$ y por el lema 11.6, $V_a = \langle v \rangle$. De esta forma se obtiene que $V = V_h \perp \langle v \rangle$. Por la proposición 11.2, se puede tomar v de forma que $v^2 = 1$ o $v^2 = s$. Por tanto, existe una base donde la matriz de Gram de σ es

$$\operatorname{diag}(1, -1, \cdots, 1, -1, 1) \quad \text{o} \qquad \operatorname{diag}(1, -1, \cdots, 1, -1, s). \qquad \square$$

***Observación* 11.8.** Obsérvese que los dos espacios ortogonales de la proposición 11.7 (1), tienen discriminantes $(-1)^{\frac{n}{2}} \mathbb{F}_q^{*2}$ y $(-1)^{\frac{n}{2}} s\, \mathbb{F}_q^{*2}$, respectivamente, y por tanto no son isométricos. Los espacios ortogonales de la proposición 11.7 (2), tienen discriminantes

$$(-1)^{\frac{n-1}{2}} \mathbb{F}_q^{*2} \quad \text{o} \quad (-1)^{\frac{n-1}{2}} s\, \mathbb{F}_q^{*2}$$

respectivamente, y por tanto no son isométricos.

Teorema 11.9. *Sea $\mathbb{F}_q$ un cuerpo finito de característica $\neq 2$. Dos espacios ortogonales no singulares sobre $\mathbb{F}_q$ son isométricos si, y solo si, tienen igual dimensión e igual discriminante. En cada dimensión n existen exactamente 2 clases de isometría de espacios ortogonales no singulares de dimensión n.*

Demostración. Si dos espacios ortogonales no singulares son isométricos, entonces por la proposición 2.18 tienen igual discriminante.

Recíprocamente si dos espacios ortogonales no singulares sobre $\mathbb{F}_q$ tienen igual discriminante e igual dimensión por la observación anterior y por las proposiciones 11.7, 11.4 y 11.2 se sigue que son isométricos. $\square$

12. Grupo de Witt de un cuerpo finito

Sea $\mathbb{F}_q$ un cuerpo con q elementos de característica $p \neq 2$. Denotaremos por $\mid \mathbb{F}_q^* \mid$ el orden del grupo $\mathbb{F}_q^*$. En esta sección vamos a calcular el grupo de Witt de $\mathbb{F}_q$.

Lema 12.1. *Se tiene*

(1) $q \equiv 1(\mathrm{mod}\, 4)$*, si, y solo si,* $-1 \in \mathbb{F}_q^{*2}$.

(2) $q \equiv 3(\mathrm{mod}\, 4)$*, si, y solo si,* $-1 \notin \mathbb{F}^{*2}$.

Demostración. Dado que q es un número impar, $q \equiv 1(\mathrm{mod}\, 4)$ o $q \equiv 3(\mathrm{mod}\, 4)$; además, solo se puede dar una de estas dos condiciones, puesto que $(1 + 4\,\mathbb{Z}) \cap (3 + 4\,\mathbb{Z}) = \varnothing$. Es suficiente probar (1).

(1) Si $q \equiv 1(\mathrm{mod}\, 4)$, es decir $\mid \mathbb{F}_q^* \mid = q - 1 \in 4\mathbb{Z}$, entonces por ser $\mathbb{F}_q^*$ un grupo cíclico, existe un elemento $x \in \mathbb{F}_q^*$ de orden 4. Dado que x^2 tiene orden 2, se tiene que $x^2 = -1$. Así, $-1 \in \mathbb{F}_q^{*2}$.

Recíprocamente, si $-1 \in \mathbb{F}_q^{*2}$, entonces existe $x \in \mathbb{F}_q^*$ tal que $x^2 = -1$. Por tanto, el orden de x es 4 y teniendo en cuenta que el orden de un elemento es un divisor del orden del grupo, se tiene que $q - 1 = \mid \mathbb{F}_q* \mid \in 4\,\mathbb{Z}$. Así, $q \equiv 1(\mathrm{mod}\, 4)$. □

Teorema 12.2. *Sea $\mathbb{F}_q$ un cuerpo con q elementos de característica $p \neq 2$. Se tiene*

(1) *Si $q \equiv 1(\mathrm{mod}\, 4)$, entonces el grupo $W(\mathbb{F}_q)$ es isomorfo a $\mathbb{Z}/2\,\mathbb{Z} \times \mathbb{Z}/2\,\mathbb{Z}$.*

(2) *Si $q \equiv 3(\mathrm{mod}\, 4)$, entonces el grupo $W(\mathbb{F}_q)$ es isomorfo a $\mathbb{Z}/4\,\mathbb{Z}$.*

Demostración. (1) Si $-1 \in \mathbb{F}_q^{*2}$, entonces

$$W(F_q) = \{[\langle 0\rangle], [\langle 1\rangle], [\langle s\rangle], [\langle (1, -s)\rangle]\}.$$

Veamos que los elementos $[\langle 1\rangle]$, $[\langle s\rangle]$, $[\langle (1, -s)\rangle]$ tienen orden 2. Dado que

$$\begin{aligned}
&\mathrm{disc}\,\langle 1, 1\rangle = \mathbb{F}_q^{*2} = (-1)\mathbb{F}_q^{*2} = \ \mathrm{disc}\,\langle 1, -1\rangle \\
&\mathrm{disc}\,\langle s, s\rangle = s^2\mathbb{F}_q^{*2} = \mathbb{F}_q^{*2} \\
&\mathrm{disc}\,\langle 1, -s, 1, -s\rangle = (-s)^2\mathbb{F}_q^{*2} = \mathbb{F}_q^{*2} = \mathrm{disc}\,\langle 1, -1, 1, -1\rangle.
\end{aligned}$$

se tiene

$$\begin{aligned}
&[\langle 1\rangle] \oplus [\langle 1\rangle] = [\langle 1, 1\rangle_a] = [\langle 1, -1\rangle_a] = [(0)] \\
&[\langle s\rangle] \oplus [\langle s\rangle] = [\langle s, s\rangle_a] = [\langle 1, -1\rangle_a] = [(0)] \\
&[\langle 1, -s\rangle] \oplus [\langle 1, -s\rangle] = [\langle 1, -s, 1, -s\rangle_a] = [\langle 1, -1, 1, -1\rangle_a] = [(0)]
\end{aligned}$$

Por tanto $W(\mathbb{F}_q) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(2) Si $-1 \notin \mathbb{F}_q^{*2}$, tomando $s = -1$ se tiene

$$W(\mathbb{F}_q) = \{[\langle 0\rangle], [\langle 1\rangle], [\langle -1\rangle], [\langle 1, 1\rangle]\}.$$

Veamos que el elemento $[\langle 1\rangle]$ genera al grupo de Witt. En efecto,

$$\begin{aligned}
&[\langle 1\rangle] \oplus [\langle 1\rangle] = [\langle 1, 1\rangle_a] = [\langle 1, 1\rangle] \\
&[\langle 1\rangle] \oplus [\langle 1\rangle] \oplus [\langle 1\rangle] = [\langle 1, 1, 1\rangle_a] = [\langle 1, -1, -1\rangle_a] = [\langle -1\rangle] \\
&[\langle 1\rangle] \oplus [\langle 1\rangle] \oplus [\langle 1\rangle] \oplus [\langle 1\rangle] = [\langle 1\rangle] \oplus [\langle -1\rangle] = [(\langle 1, -1\rangle)_a] = [\langle 1, -1\rangle] = [\langle 0\rangle]
\end{aligned}$$

Luego $W(\mathbb{F}_q)$ es un grupo cíclico. Así, $W(\mathbb{F}_q) \cong \mathbb{Z}/4\mathbb{Z}$. □

***Observación* 12.3.** Obsérvese que los isomorfismos del teorema anterior son isomorfismos de anillos.

Bibliografía

[1] Artin, E., *Álgebra geométrica*, Limusa, México, 1992.

[2] Kostrikin, A. I. and Manin Y. I., *Linear algebra and geometry*, Gordon and Breach Science Publishers, Amsterdam, 1989.

[3] Elman, R., Lam T. Y., *Classification theorems for quadratic forms over fields*, Comm. Math. Helv. **49** (1974), 373–381.

[4] Lam T. Y., *Introduction to Quadratic Forms over Fields*, American Mathematical Society, Providence, RI, 2005.

[5] Milnor J., *Algebraic K-theory and quadratic forms*, Invent. Math. **9** (1969/1970), 318–344.

[6] Scharlau, W., *Quadratic and hermitian forms*, Springer-Berlag. Berlin, 1985.

[7] Scharlau, W., *On the History of the Algebraic Theory of Quadratic Forms*, Contem. Math. **272** (2000), 229–259.

[8] Snapper, E., Troyer, R. J., *Metric affine geometry*, Academic Press, London, 1971.

[9] Voevodsky V., *Motivic cohomology with $Z/2\,\mathbb{Z}$-coefficients*, Publ. Math. Inst. Hautes Études Sci. **98** (2003), 59–104.