"INTRODUCCIÓN A LA TEORÍA ALGEBRAICA DE FORMAS CUADRÁTICAS"

Jorge Alberto Guccione

En el siguiente apunte damos las primeras definiciones y propiedades básicas de la teoría algebraica de formas cuadráticas. Nosotros seguimos principalmente los primeros dos capítulos de "The Algebraic Theory of Quadratic Forms" de T. Y. Lam, pero ponemos el acento el aspecto algorítmico de las demostraciones. Esto se aplica especialmente al Teorema de cancelación de Witt y al Teorema de Cartan-Dieudonné.

Capítulo 1

1. Formas cuadráticas y espacios cuadráticos

Definición 1.1. *Sea F un cuerpo de característica distinta de 2. Un espacio cuadrático es un F-espacio vectorial V de dimensión finita provisto de una forma bilineal simétrica $B\colon V \times V \to F$.*

Dado un espacio cuadrático (V, B) se define la forma cuadrática $q_B\colon V \to F$ asociada a B por $q_B(v) = B(v, v)$. Un cálculo directo muestra que:

1) $q_B(\lambda v) = B(\lambda v, \lambda v) = \lambda^2 B(v, v) = \lambda^2 q_B(v)$,

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

Reciprocamente si $q\colon V \to F$ es una función tal que

1') $q(2v) = 4q(v)$,

2') La aplicación $B\colon V \times V \to F$ definida por $B(v, w) = \frac{1}{2}\left(q(v + w) - q(v) - q(w)\right)$ es bilineal,

entonces

$$q_B(v) = B(v, v) = \frac{1}{2}\left(q(2v) - 2q(v)\right) = q(v).$$

Esto muestra que tener una aplicación bilineal simétrica de $B\colon V \times V \to F$ es lo mismo que tener una función $q\colon V \to F$ que satisface 1') y 2'). A veces escribiremos (V, B, q), donde $B\colon V \times V \to F$ es una forma bilineal simétrica y $q = q_B$ es la forma cuadrática asociada a B, para denotar a un espacio cuadrático.

Fijemos una base $E = \{v_1, \ldots, v_n\}$ de V. La matriz de la forma bilineal simétrica $B\colon V \times V \to F$ en E, es la matriz simétrica $M_{B,E}$, de n filas y n columnas, que en la coordenada (i, j) tiene a $B(v_i, v_j)$. Denotemos con $[v]_E$ a las coordenadas de un vector v de V en la base E. Nosotros consideraremos a $[v]_E$ como un vector columna. Sean $v = \sum_{i=1}^n x_i v_i$ y $w = \sum_{i=1}^n y_i v_i$. Como B es bilineal,

$$B(v, w) = \sum_{i,j=1}^{n} B(v_i, v_j) x_i y_j = [w]_E^t M_{B,E} [v]_E,$$

donde $[w]_E^t$ es la matriz transpuesta de $[w]_E$. Sea ahora M una matriz simétrica de $n \times n$. Definiendo $B_{M,E}\colon V \times V \to F$ por $B_{M,E}(v,w) = [w]_E^t M [v]_E$, obtenemos una forma bilineal simétrica. Dado que, después de haber fijado una base de V, estas construcciones son recíprocas una de la otra, tener una forma bilineal simétrica es lo mismo que tener una matriz simétrica.

Dos espacios cuadráticos (V,B) y (V',B') son isométricos si existe un isomorfismo F-lineal $\sigma\colon V \to V'$ tal que $B'(\sigma(v),\sigma(w)) = B(v,w)$ para todo $v,w \in V$. Sea $\sigma\colon V \to V'$ una isometría, $E = \{v_1,\ldots,v_n\}$ y $E' = \{v_1',\ldots,v_n'\}$ bases de V y V' respectivamente y $[\sigma]_{E,E'}$ la matriz de σ en las bases E y E' (es decir la matriz definida por $[\sigma]_{E,E'}[v]_E = [\sigma(v)]_{E'}$). Entonces,

$$\begin{aligned}[w]_E^t M_{B,E} [v]_E &= B(v,w) = B'(\sigma(v),\sigma(w)) \\ &= [\sigma(w)]_{E'}^t M_{B',E'} [\sigma(v)]_{E'} \\ &= [w]_E^t [\sigma]_{E,E'}^t M_{B',E'} [\sigma]_{E,E'} [v]_E,\end{aligned}$$

de donde $M_{B,E} = [\sigma]_{E,E'}^t M_{B',E'} [\sigma]_{E,E'}$. En particular, tomando $V' = V$, $B' = B$ y $\sigma = id$ obtenemos que $M_{B,E} = C(E,E')^t M_{B,E'} C(E,E')$, donde $C(E,E') = [id]_{E,E'}$, es la matriz de cambio de base de E en E'. Recíprocamente, si M y M' son matrices congruentes de $n \times n$ y $P \in \mathrm{GL}(n,F)$ es tal que $M' = P^t M P$, entonces los espacios cuadráticos $B_{M,E}\colon F^n \times F^n \to F$ y $B_{M',E}\colon F^n \times F^n \to F$, obtenidos tomando E como la base canónica de F^n, son isométricos. Una isometría $\sigma\colon (F^n, B_{M',E}) \to (F^n, B_{M,E})$, está dada por $\sigma(v) = (Pv^t)^t$, donde v^t denota al transpuesto de v y $(Pv^t)^t$ denota al transpuesto de Pv^t.

La relación de isometría es una relación de equivalencia. A la clase correspondiente a un espacio cuadrático (V,B,q) la denominaremos clase de isometría de (V,B,q) (o (V,B) o de q). Por lo que hemos visto estas clases están en correspondencia con las clases definidas por la relación de congruencia entre matrices. Esta correspondencia, a la clase de un espacio cuadrático (V,B), le asigna la clase de la matriz $M_{B,E}$ de B en una base cualquiera E de V y, su inversa, a la clase de una matriz cuadrada M de $n \times n$, le asigna la clase del espacio cuadrático $B_{M,E}\colon F^n \times F^n \to F$, obtenido tomando E como la base canónica de F^n.

Ejemplo. Consideremos las formas cuadrática $q\colon F^2 \to F$ y $q'\colon F^2 \to F$, definidas por $q(x_1,x_2) = x_1x_2$ y $q'(x_1,x_2) = x_1^2 - x_2^2$, respectivamente. Dado que

$$q(x_1+x_2, x_1-x_2) = (x_1+x_2)(x_1-x_2) = x_1^2 - x_2^2 = q'(x_1,x_2),$$

q y q' son isométricas.

Sea (V,B) un espacio cuadrático y sea $S \subseteq V$ un subespacio. Entonces $(S, B_{|S\times S})$ es en si mismo un espacio cuadrático. Como es usual, se define el complemento ortogonal $S^\perp$ de V por $S^\perp = \{v \in V : B(v,w) = 0 \text{ para todo } w \in S\}$. El complemento ortogonal de V mismo es llamado el radical $\operatorname{rad} V$ de V.

Nota 1.2. Dado un espacio cuadrático (V,B), denotamos por $\varphi_B\colon V \to V^*$ a la aplicación $\varphi_B\colon V \to V^*$, definida por $\varphi_B(v)(w) = B(v,w)$. Es fácil ver que $\operatorname{Ker}(\varphi_B) = \operatorname{rad} V$ y que la matriz simétrica asociada a (V,B) en una base E de V cualquiera coincide con la matriz de φ_B, entre las bases E y dual de E. En consecuencia son equivalentes:

1) $\operatorname{rad} V = 0$.

2) La aplicación $\varphi_B \colon V \to V^*$, definida por $\varphi_B(v)(w) = B(v,w)$, es un isomorfismo.

3) Si $B(v,w) = 0$ para todo $w \in V$, entonces $v = 0$.

Si una de (y por lo tanto todas) estas afirmaciones es verdadera, se dice que (V,B) es un espacio cuadrático regular.

A continuación introducimos las sumas ortogonales. Sean (V_1,B_1) y (V_2,B_2) dos espacios cuadráticos. Definimos un espacio cuadrático

$$(V_1,B_1) \perp (V_2,B_2) = (V_1 \perp V_2, B_1 \perp B_2),$$

poniendo

$$V_1 \perp V_2 = V_1 \oplus V_2 \quad \text{y} \quad (B_1 \perp B_2)((v_1,v_2),(w_1,w_2)) = B_1(v_1,w_1) + B_2(v_2,w_2).$$

Es claro que $B_1 \perp B_2$ es simétrico y bilineal. Además $B(V_1,V_2) = 0$ y $B_{|V_i \times V_i} = B_i$ $(i = 1,2)$. El espacio cuadrático $(V_1,B_1) \perp (V_2,B_2)$ es llamado la suma ortogonal de (V_1,B_1) y (V_2,B_2). Notese que

$$q_B(v_1,v_2) = B((v_1,v_2),(v_1,v_2)) = B_1(v_1,v_1) + B_2(v_2,v_2) = q_{B_1}(v_1) + q_{B_2}(v_2).$$

Proposición 1.3. *Sea (V,B) un espacio cuadrático y S un subespacio de V. Se satisfacen:*

1) $S \cap S^\perp = \operatorname{rad} S$.

2) $\dim(S) + \dim\big(S^\perp\big) = \dim(V) + \dim(S \cap \operatorname{rad} V)$.

3) $S \cap \operatorname{rad} V \subseteq \operatorname{rad} S$ *y* $\dim\big(S + S^\perp\big) = \dim(V) - \big(\dim(\operatorname{rad} S) - \dim\big(S \cap \operatorname{rad} V\big)\big)$. *En particular* $V = S + S^\perp$ *si y sólo si* $\operatorname{rad} S = S \cap \operatorname{rad} V$.

4) $S + S^\perp = S \perp T$ *si y sólo si* T *es un complemento de* $\operatorname{rad} S$ *en* $S^\perp$.

5) $V = S \oplus S^\perp = S \perp S^\perp$ *si y sólo si* $\operatorname{rad} S = 0$.

6) ${S^\perp}^\perp = S + \operatorname{rad} V$.

Demostración. 1) Es trivial.

2) Sea $\varphi_B \colon V \to V^*$ el morfismo lineal definido por $\varphi_B(v)(w) = B(v,w)$. Como $\operatorname{rad} V = \operatorname{Ker}(\varphi_B)$ y $S^\perp$ es el subespacio de V anulado por $\varphi_B(S)$, tenemos

$$\dim\big(S^\perp\big) = \dim(V^*) - \dim(\varphi_B(S)) = \dim(V) - \dim(S) + \dim(S \cap \operatorname{rad} V).$$

3) Es claro que $S \cap \operatorname{rad} V \subseteq \operatorname{rad} S$. Por los items 1) y 2),

$$\begin{aligned}\dim\big(S + S^\perp\big) &= \dim(S) + \dim\big(S^\perp\big) - \dim(\operatorname{rad} S) \\ &= \dim(V) - \big(\dim(\operatorname{rad} S) - \dim\big(S \cap \operatorname{rad} V\big)\big).\end{aligned}$$

4) Si $S + S^\perp = S \perp T$, entonces

$$T \cap \operatorname{rad} S \subseteq T \cap S = 0 \quad \text{y} \quad S^\perp = (T+S) \cap S^\perp = T + (S \cap S^\perp) = T + \operatorname{rad} S,$$

donde la segunda igualdad se deduce de que $T \subseteq S^\perp$. Supongamos ahora que T es un complemento de $\operatorname{rad} S$ en $S^\perp$. Como $T \cap S = T \cap S^\perp \cap S = T \cap \operatorname{rad} S = 0$, tenemos

$$S + S^\perp = S + (\operatorname{rad} S + T) = (S + \operatorname{rad} S) + T = S + T = S \oplus T = S \perp T.$$

5) Si $V = S \oplus S^\perp$, entonces $\operatorname{rad} S = S \cap S^\perp = 0$. Veamos la recíproca. Dado que $S \cap S^\perp = \operatorname{rad} S = 0$ basta ver que $V = S + S^\perp$, lo que se deduce de que $\operatorname{rad} S = 0$ y del item 3).

6) Es claro que $S + \operatorname{rad} V \subseteq S^{\perp\perp}$. Dado que $S^\perp \cap \operatorname{rad} V = \operatorname{rad} V$, aplicando dos veces el item 2), obtenemos

$$\begin{aligned} \dim\big(S^{\perp\perp}\big) &= \dim(V) - \dim\big(S^\perp\big) + \dim(\operatorname{rad} V) \\ &= \dim(S) + \dim(\operatorname{rad} V) - \dim(S \cap \operatorname{rad} V) \\ &= \dim(S + \operatorname{rad} V), \end{aligned}$$

de donde el resultado se deduce inmediatamente. □

2. Criterio de representación y diagonalización de formas cuadráticas

Dado un cuerpo F, denotamos con $\dot{F}$ al grupo multiplicativo $F \setminus \{0\}$ de F.

Definición 2.1. *Sea $q\colon V \to F$ una forma cuadrática de dimensión n sobre F y sea $d \in \dot{F}$. Decimos que q representa a d si existe $v \in V$ tal que $q(v) = d$. Notese que v es automaticamente un vector no nulo. Escribiremos $D_F(q) = D(q)$ para denotar al conjunto de elementos de $\dot{F}$ que son representados por q. Este conjunto sólo depende de la clase de equivalencia de q. Dado un espacio cuadrático (V, B, q) denotamos con $D_B(V) = D(V)$ a $D(q)$.*

Si $a, d \in \dot{F}$, entonces claramente $d \in D(q)$ si y sólo si $da^2 \in D(q)$. Así $D(q)$ consiste de una unión de coclases de $\dot{F}$ módulo $\dot{F}^2$. Llamaremos a $\frac{\dot{F}}{\dot{F}^2}$ el grupo de clases de cuadrados de F y, por abuso de notación, también consideraremos a $D(q)$ como un subconjunto de $\frac{\dot{F}}{\dot{F}^2}$.

Dado $d \in F$, denotaremos con $\langle d \rangle$ a la clase de isometría del espacio quadrático unidimensional cuya forma cuadrática envía x en dx^2. Claramente $\langle d \rangle$ es regular si y sólo si $d \in \dot{F}$ y $\langle d \rangle \simeq \langle d' \rangle$ si y sólo si $d\dot{F}^2 = d'\dot{F}^2$. Dados $d_1, \ldots, d_n \in F$ escribiremos

$$\langle d_1, \ldots, d_n \rangle = \langle d_1 \rangle \perp \cdots \perp \langle d_n \rangle$$

y dados $d \in F$ y $n \in \mathbb{N}$ denotaremos con $n\langle d \rangle$ a la suma ortogonal $\langle d, \ldots, d \rangle$ de $\langle d \rangle$ consigo misma n veces.

Proposición 2.2 (Criterio de representación). *Sea (V, B) un espacio cuadrático y sea $d \in \dot{F}$. Entonces $d \in D_B(V)$ si y sólo si existe otro espacio cuadrático (V', B'), junto con una isometría $V \simeq \langle d \rangle \perp V'$.*

Demostración. Es claro que si $V \simeq \langle d \rangle \perp V'$, entonces $d \in D(V)$. Supongamos que $d \in D(V)$ y sea $v \in V$ tal que $d = q_B(v)$. Como Fv es regular, por el item 5) de la Proposición 1.3, $V = Fv \perp (Fv)^\perp$ □

Corolario 2.3. *Sea (V, B) un espacio cuadrático de dimensión n. Existen escalares $d_1, \ldots, d_n$ tales que $(V, B) \simeq \langle d_1, \ldots, d_n \rangle$.*

Demostración. Si $D_B(V)$ es vacío, entonces $B = 0$ y V es isométrico a $n\langle 0 \rangle$. Si existe algún $d \in D_B(V)$, entonces $V \simeq \langle d \rangle \perp V'$ para algún (V', B') y la demostración se termina fácilmente por inducción en n $\square$

Nota. Sea (V, B) un espacio cuadrático no nulo de dimensión n y sea $\{v_1, \ldots, v_n\}$ una base de V. Veamos como encontrar un vector $v \in V$ en el que q_B no se anula. Si alguno de los v_i's satisface esta condición, ya está. Podemos suponer entonces que $q_B(v_i) = 0$ para $1 \leq i \leq n$. Dado que B es no nulo existen $1 \leq i < j \leq n$ tal que $B(v_i, v_j) \neq 0$. Como

$$q_B(v_i + v_j) = q_B(v_i) + q_B(v_j) + 2B(v_i, v_j) = 2B(v_i, v_j),$$

resulta que $q_B(v_i + v_j) \neq 0$.

Otro método de diagonalización (Algoritmo de Lagrange). *Sea (V, B, q) un espacio cuadrático y sea $\{v_1, \ldots, v_n\}$ una base de V. Escribamos $a_{ij} = B(v_i, v_j)$, de modo que*

$$q(x_1 v_1 + \cdots + x_n v_n) = \sum_{1 \leq i,j \leq n} a_{ij} x_i x_j,$$

Queremos encontrar una base en la que q sea diagonal. Consideramos dos casos

1) Supongamos que algún $a_{ii} \neq 0$. Podemos suponer que $i = 1$ y escribir

$$\begin{aligned} q\left(\sum_{i=1}^{n} x_i v_i\right) &= a_{11} x_1^2 + \sum_{i=2}^{n} 2a_{1i} x_1 x_i + \sum_{2 \leq i,j \leq n} a_{ij} x_i x_j \\ &= \frac{1}{a_{11}} \left(\sum_{i=1}^{n} a_{1i} x_i\right)^2 - \sum_{2 \leq i,j \leq n} \frac{a_{1i} a_{1j}}{a_{11}} x_i x_j + \sum_{2 \leq i,j \leq n} a_{ij} x_i x_j. \end{aligned}$$

Sea $\{w_1, \ldots, w_n\}$ la base definida por

$$(a_{11} x_1 + \cdots + a_{1n} x_n) w_1 + x_2 w_2 + \cdots + x_n w_n = x_1 v_1 + \cdots + x_n v_n.$$

Si escribimos $y_1 = a_{11} x_1 + \cdots + a_{1n} x_n$ e $y_i = x_i$ para $i \neq 1$, obtenemos

$$q\left(\sum_{i=1}^{n} y_i w_i\right) = \frac{1}{a_{11}} y_1^2 + \sum_{2 \leq i,j \leq n} \left(a_{ij} - \frac{a_{1i} a_{1j}}{a_{11}}\right) y_i y_j.$$

2) $a_{11} = \cdots = a_{nn} = 0$. Podemos suponer entonces que $a_{12} \neq 0$ y escribir

$$\begin{aligned} q\left(\sum_{i=1}^{n} x_i v_i\right) &= \sum_{j=2}^{n} 2a_{1j} x_1 x_j + \sum_{2 \leq i < j \leq n} 2a_{ij} x_i x_j = x_1^2 + x_1 \left(-x_1 + \sum_{j=2}^{n} 2a_{1j} x_j\right) \\ &+ \sum_{j=3}^{n} \frac{a_{2j}}{a_{12}} \left[x_1 + \left(-x_1 + \sum_{i=2}^{n} 2a_{1i} x_i\right) - \left(\sum_{i=3}^{n} 2a_{1i} x_i\right)\right] x_j + \sum_{3 \leq i < j \leq n} 2a_{ij} x_i x_j. \end{aligned}$$

Sea $\{w_1, \ldots, w_n\}$ la base definida por

$$x_1 w_1 + \left(-x_1 + \sum_{i=2}^{n} 2a_{1i} x_i \right) w_2 + x_3 w_3 + \cdots + x_n w_n = x_1 v_1 + \cdots + x_n v_n.$$

Si escribimos $y_i = x_i$ para $i \neq 2$ e $y_2 = -x_1 + 2a_{12}x_2 + \cdots + 2a_{1n}x_n$, obtenemos

$$q\left(\sum_{i=1}^{n} y_i w_i \right) = y_1^2 + y_1 y_2 + \sum_{j=3}^{n} \frac{a_{2j}}{a_{12}} \left(y_1 + y_2 - \sum_{i=3}^{n} 2a_{1i} y_i \right) y_j + \sum_{3 \leq i < j \leq n} 2a_{ij} y_i y_j,$$

lo que reduce el problema al caso 1).

Ejemplo. Sea $q(x_1, x_2) = x_1 x_2$. Escribamos $y_2 = -x_1 + x_2$. Entonces

$$q(x_1, x_2) = x_1^2 + x_1(-x_1 + x_2) = x_1^2 + x_1 y_2 = (x_1 + \frac{1}{2} y_2)^2 - \frac{1}{4} y_2^2.$$

Así, poniendo $z_1 = x_1 + \frac{1}{2} y_2 = \frac{1}{2}(x_1 + x_2)$ y $z_2 = \frac{1}{2} y_2 = \frac{1}{2}(-x_1 + x_2)$, obtenemos $q(x_1, x_2) = z_1^2 - z_2^2$.

Sea $q \colon V \to F$ una forma cuadrática regular con coeficientes en F. El determinante de q es el elemento de $\frac{\dot{F}}{\dot{F}^2}$ definido por $\mathrm{d}(q) = \det(M_q) \pmod{\dot{F}^2}$, donde M_q es la matriz simétrica asociada a q en alguna base de V. Notese que si $q' \simeq q$, entonces $M_{q'} = C^t M_q C$, para alguna matriz no singular C y como $\det(C^t M_q C) = \det(M_q) \det(C)^2$, resulta que $\mathrm{d}(q') = \mathrm{d}(q)$. Esto muestra que el determinante de q sólo depende de la clase de isometría de q. También es claro que $\mathrm{d}(q_1 \perp q_2) = \mathrm{d}(q_1)\,\mathrm{d}(q_2)$. En particular si $(V, B) \simeq \langle d_1, \ldots, d_n \rangle$, entonces $d(q) = d_1 \cdots d_n \pmod{\dot{F}^2}$.

3. Plano hiperbólico y espacios hiperbólicos

Definición 3.1. *Sea v un vector no nulo en un espacio cuadrático (V, B). Si $q_B(v) = 0$ decimos que v es isotrópico y si $q_B(v) \neq 0$ que es anisotrópico. Recalquemos que si un vector $v \in V$ es isotrópico o anisotrópico, entonces por definición $v \neq 0$. El espacio cuadrático (V, B) es isotrópico si contiene algún vector isotrópico y es anisotrópico en otro caso. Es claro que un espacio anisotrópico es necesariamente regular. Finalmente decimos que (V, B) es totalmente isotrópico si todos los vectores no nulos de v son isotrópicos, es decir si $B = 0$.*

Proposición 3.2. *Sean $q = \langle a, b \rangle$ y $q' = \langle c, d \rangle$ dos formas binarias regulares. Entonces $q \simeq q'$ si y sólo si $\mathrm{d}(q) = \mathrm{d}(q')$ y q y q' representan a un elemento en común.*

Demostración. Supongamos que $\mathrm{d}(q) = \mathrm{d}(q')$ y que existe $e \in D(q) \cap D(q')$. Por el criterio de representación (Proposición 2.2) existe $e' \in \dot{F}$ tal que $q \simeq \langle e, e' \rangle$. Tomando determinantes, obtenemos que $ab\dot{F}^2 = ee'\dot{F}^2$, de donde $q \simeq \langle e, abe \rangle$. De la misma manera $q' \simeq \langle e, cde \rangle$ y, en consecuencia, $q \simeq q'$, ya que $ab\dot{F}^2 = cd\dot{F}^2$. La recíproca es inmediata $\square$

Proposición 3.3. *Sea (V, B, q) un espacio cuadrático de dimensión 2. Son equivalentes:*

1) V es regular e isotrópico.

2) V es regular y $\mathrm{d}(q) = -1$.

3) V es isométrico a $\langle 1, -1\rangle$.

Demostración. 1) $\implies$ 2) Sea $\{v_1, v_2\}$ una base ortogonal de V. La regularidad de q implica que $d_i = q(v_i) \neq 0$ $(i = 1, 2)$. Sea $x_1v_1 + x_2v_2$ un vector isotrópico. Por simetría podemos suponer que $x_1 \neq 0$. Entonces,

$$0 = q(x_1v_1 + x_2v_2) = x_1^2d_1 + x_2^2d_2 \implies d_1 = -\left(\frac{x_2}{x_1}\right)^2 d_2$$
$$\implies \mathrm{d}(q) = d_1d_2\dot{F}^2 = -1\dot{F}^2.$$

2) $\implies$ 3) Como $D(\langle 1, -1\rangle) = \dot{F}$, tenemos que $D(q) \cap D(\langle 1, -1\rangle) = D(q) \neq \emptyset$. Así, por la Proposición 3.2, $q \simeq \langle 1, -1\rangle$.

3) $\implies$ 1) Es trivial $\square$

Sea (V, B, q) como en el item 2) de la proposición anterior. Veamos como encontrar una base ortogonal $\{w_1, w_2\}$ de V tal que $q(w_1) = 1$ y $q(w_2) = -1$. Empecemos tomando una base ortogonal $\{v_1, v_2\}$ de V y escribamos $q(v_1) = d_1$ y $q(v_2) = d_2$. Por hipótesis existe $x \in \dot{F}$ tal que $d_1d_2 = -x^2$ (notese que en la demostración de que 1) implica 2) se obtiene este x). Es fácil ver que la base $\{w_1, w_2\}$ de V, definida por

$$w_1 = \frac{1 + d_1}{2d_1}v_1 + \frac{(1 - d_1)x}{2d_1d_2}v_2 \qquad \text{y} \qquad w_2 = \frac{1 - d_1}{2d_1}v_1 + \frac{(1 + d_1)x}{2d_1d_2}v_2$$

es ortogonal y que $q(w_1) = 1$ y $q(w_2) = -1$.

La clase de isometría de un espacio de dimensión 2 que satisface las condiciones de la Proposición 3.3 es llamada el plano hiperbólico (presumiblemente porque las gráficas de la ecuación $X_1^2 - X_2^2 = d$ son llamadas hipérbolas). El plano hiperbólico será denotado con H y juega un papel especial en la teoría de formas cuadráticas. Una suma ortogonal de planos hiperbólicos será llamado un espacio hiperbólico.

Definición 3.4. *Una forma cuadrática es universal si representa a todos los elementos no nulos de F.*

Teorema 3.5. *Sea (V, B, q) un espacio cuadrático regular. Se satisfacen:*

1) Cada subespacio totalmente isotrópico $U \subseteq V$ de dimensión positiva r está contenido en un subespacio hiperbólico $T \subseteq V$ de dimensión $2r$.

2) V es isotrópico si y sólo si contiene un plano hiperbólico (necesariamente como un sumando ortogonal por el item 5) de la Proposición 1.3).

3) Si V es isotrópico, es universal.

Demostración. Tomando $r = 1$ en 1) se deduce que 1) implica 2) y dado que, por el ejemplo anterior a la Nota 1.2, el plano hiperbólico es universal, 2) implica 3). Ahora probaremos 1) por inducción en r. Tomemos una base $\{v_1, \ldots, v_r\}$ de U y

sea S el subespacio de U generado por $\{v_2, \ldots, v_r\}$. Es claro que $U^\perp \subseteq S^\perp$. Dado que V es regular, por el item 2) de la Proposición 1.3,

$$\dim\big(S^\perp\big) = \dim(V) - \dim(S) > \dim(V) - \dim(U) = \dim\big(U^\perp\big).$$

Así, existe un vector $w_1 \in V$ que es ortogonal a $v_2, \ldots, v_r$, pero no a v_1. En particular, como v_1 es isotrópico, v_1 e w_1 son linealmente independientes. El subespacio $H_1 = Fv_1 + Fw_1$ tiene determinante

$$\mathrm{d}(H_1) = \det \begin{pmatrix} 0 & B(v_1, w_1) \\ B(v_1, w_1) & B(w_1, w_1) \end{pmatrix} \dot{F}^2 = -1\dot{F}^2,$$

y, por lo tanto, es hiperbólico. Por el item 5) de la Proposición 1.3, $V = H_1 \perp H_1^\perp$. Dado que $H_1^\perp$ contiene a $\{v_2, \ldots, v_r\}$, la demostración se sigue por inducción $\square$

Corolario 3.6 (primer teorema de representación). *Sea (V, B, q) un espacio cuadrático regular y sea $d \in \dot{F}$. Entonces $d \in D(q)$ si y sólo si $V \perp \langle -d \rangle$ es isotrópica.*

Demostración. Tomemos una base $\{v_1, \ldots, v_n\}$ de V tal que $q(x_1v_1 + \cdots + x_nv_n) = a_1x_1^2 + \cdots + a_nx_n^2$. Si existe una ecuación $d = a_1x_1^2 + \cdots + a_nx_n^2$ con $x_i \in F$, entonces $a_1x_1^2 + \cdots + a_nx_n^2 + (-d)1^2 = 0$, de dónde $V \perp \langle -d \rangle$ es isotrópica. Recíprocamente, supongamos que $(x_1v_1 + \cdots + x_nv_n, x_{n+1})$ es un vector isotrópico de $V \perp \langle -d \rangle$, de modo que $a_1x_1^2 + \cdots + a_nx_n^2 + (-d)x_{n+1}^2 = 0$. Si $x_{n+1} \neq 0$, entonces $d = a_1\left(\frac{x_1}{x_{n+1}}\right)^2 + \cdots + a_n\left(\frac{x_n}{x_{n+1}}\right)^2 \in D(q)$. Si, por el contrario $x_{n+1} = 0$, entonces $x_1v_1 + \cdots + x_nv_n$ es un vector isotrópico de (V, B, q). Así, por el item 3) del teorema anterior, (V, B, q) es universal y, en particular, $d \in D(q)$ $\square$

Corolario 3.7. *Para cada entero positivo r, las siguientes dos afirmaciones son equivalentes*

1) Toda forma cuadrática regular de dimensión r es universal.

2) Toda forma cuadrática de dimensión $r+1$ es isotrópica.

Demostración. Es trivial $\square$

4. Teoremas de descomposición y de cancelación

Teorema 4.1 (de descomposición de Witt). *Cada espacio cuadratico (V, B) se parte en una suma ortogonal $(V, B) = (V_t, B_t) \perp (V_h, B_h) \perp (V_a, B_a)$, donde V_t es totalmente isotrópico, V_h es hiperbólico o cero y V_a es anisotrópico. Además los tipos de isometría de V_t, V_h y V_a están unívocamente determinados. A (V_a, B_a) y (V_h, B_h) los denominamos la componente totalmente isotrópica e hiperbólica de (V, B) respectivamente.*

Demostración. (Existencia) Tomemos un subespacio V_0 tal que $V = V_0 \oplus \operatorname{rad} V = V_0 \perp \operatorname{rad} V$. Entonces $V_t = \operatorname{rad} V$ es totalmente isotrópico y V_0 es regular. Sea $U \subseteq V_0$ un subespacio totalmente isotrópico maximal de V_0. Por el Teorema 3.5, existe un espacio hiperbólico V_h cuya dimensión es el doble de la de U. Dado que V_h es regular, por el item 5) de la Proposición 1.3, $V_0 = V_h \perp V_a$ donde $V_a = V_h^\perp$. Dado que U es un subespacio totalmente isotrópico maximal de V_0, resulta que V_a es anisotrópico (si $v \in V_a$ fuera isotrópico, entonces $U \perp \langle v \rangle$ sería totalmente isotrópico). Esto prueba la existencia. La unicidad se deduce del siguiente teorema de cancelación $\square$

Teorema 4.2 (de cancelación de Witt). *Sean (V,B), (V',B'), (V_1,B_1) y (V_1',B_1') espacios cuadráticos arbitrarios. Si $V \simeq V'$ y $V \perp V_1 \simeq V' \perp V_1'$, entonces $V_1 \simeq V_1'$.*

Para demostrar la parte de unicidad del Teorema 4.1, supongamos que V tiene otra descomposición $V = V_t' \perp V_h' \perp V_a'$ con V_t totalmente isotrópico, V_h hiperbólico o cero y V_a anisotrópico, entonces $V_t' = \operatorname{rad} V = V_t$ y por el teorema de cancelación tenemos que $V_h \perp V_a \simeq V_h' \perp V_a'$. Escribamos $V_h \simeq mH$ y $V_h' \simeq m'H$. Podemos suponer que $m \leq m'$. Cancelando mH obtenemos $V_a \simeq V_a' \perp (m'-m)H$. Como V_a es anisotrópico, también debe serlo $V_a' \perp (m'-m)H$, de dónde $m' = m$ y $V_a \simeq V_a'$ $\square$

Definición 4.3. *El entero $m = \frac{\dim(V_h)}{2}$ unívocamente determinado en el teorema de descomposición de Witt es llamado el índice de Witt de (V,B).*

Observación 4.4. De la demostración de la existencia de la descomposición se deduce que si (V,q) es regular, el índice de descomposición de Witt es la dimensión de cada subespacio totalmente isotrópico maximal de V.

A continuación probamos el teorema de cancelación de Witt. Para la demostración necesitaremos la noción de reflexión de un hiperplano. Sea (V,B,q) un espacio cuadrático. Nosotros denotaremos con $\mathcal{O}_q(V) = \mathcal{O}(V)$ al grupo de isometrías de (V,B,q). Este grupo, llamado el grupo ortogonal de (V,B,q) es el grupo subyacente a la geometría del espacio cuadrático (V,B,q). La siguiente construcción asocia a cada vector anisotrópico v de V un elemento $\tau_v \in \mathcal{O}_q(V)$. El endomorfismo τ_v de V se define por

$$\tau_v(w) = w - \frac{2B(w,v)}{q(v)}v \qquad \text{para cada } w \in V.$$

Se satisfacen:

1) τ_v es evidentemente un automorfismo lineal.
2) τ_v es la identidad sobre $(Fv)^\perp$ y $\tau_v(v) = -v$. En particular τ_v es una involución, deja fijo el hiperplano $(Fv)^\perp$ y refleja el vector v a través de $(Fv)^\perp$ en $-v$.
3) $\tau_v \in \mathcal{O}_q(V)$. En efecto, esto se deduce fácilmente del item 2). Otra forma de verlo es la siguiente:

$$\begin{aligned} B\big(\tau_v(w),\tau_v(w')\big) &= B\left(w - \frac{2B(w,v)}{q(v)}v, w' - \frac{2B(w',v)}{q(v)}v\right) \\ &= B(w,w') + \frac{4B(w,v)B(w',v)}{q(v)^2}B(v,v) - \frac{4B(w,v)B(w',v)}{q(v)} \\ &= B(w,w'), \end{aligned}$$

   ya que $B(v,v) = q(v)$.
4) τ_v tiene determinante -1.

Lema 4.5 (Ley del paralelogramo). *Sea (V,B,q) un espacio cuadrático. Entonces $q(v+w) + q(v-w) = 2q(v) + 2q(w)$.*

Demostración. En efecto,

$$q(v+w) + q(v-w) = B(v+w, v+w) + B(v-w, v-w) = 2q(v) + 2q(w) \quad \square$$

Proposición 4.6. *Sea (V, B, q) un espacio cuadrático y sean $v, w \in V$ tales que $q(v) = q(w) \neq 0$. Se satisfacen:*

1) $v - w$ o $v + w$ es anisotrópico.

2) Si $v - w$ es anisotrópico, entonces τ_{v-w} es una isometría que envía v en w.

3) Si $v + w$ es anisotrópico, entonces $-\tau_{v+w}$ es una isometría que envía v en w.

Demostración. 1) Por el Lema 4.5, $q(v + w) + q(v - w) = 2q(v) + 2q(w) = 4q(v)$. Así, $q(v + w)$ y $q(v - w)$ no pueden ser ambos nulos.

2) Dado que $q(v - w) = B(v - w, v - w) = B(v, v) + B(w, w) - 2B(v, w) = 2B(v, v) - 2B(v, w) = 2B(v, v - w)$, tenemos

$$\tau_{v-w}(v) = v - \frac{2B(v, v - w)}{q(v - w)}(v - w) = v - (v - w) = w.$$

3) Por 2) $\tau_{v+w}(v) = -w$, de donde $-\tau_{v+w}(v) = w$ □

Demostración del Teorema 4.2. Supongamos primero que V (y por lo tanto también V') es totalmente isotrópico. Sea $\pi\colon V' \perp V_1' \to V_1'$ la proyección canónica. Afirmamos que si $\sigma\colon V \perp V_1 \to V' \perp V_1'$ es una isometría, entonces también lo es la función $\sigma_1\colon V_1 \to V_1'$, definida por $\sigma_1(v) = \pi(\sigma(v))$ para todo $v \in V_1$. Dado que, para todo $v, v' \in V_1$,

$$B_1'(\sigma_1(v), \sigma_1(v')) = (B' \perp B_1')(\sigma(v), \sigma(v')) = (B \perp B_1)(v, v') = B_1(v, v'),$$

σ_1 define una isometría entre V_1 y V_1'. Probemos ahora el caso general. Por lo que hemos visto, podemos suponer, cancelando el radical de V con el de V', que V y V' son regulares. Tomemos $v \in V$ y $v' \in V'$ tales que $B(v, v) = B'(v', v') \neq 0$. Para ello hay que elegir $v \in V$ tal que $B(v, v) \neq 0$ y tomar v' como la imagen de v por una isometría $\sigma''\colon V \to V'$. Sea $\sigma\colon V \perp V_1 \to V' \perp V_1'$ una isometría. Dado que $B'(\sigma(v), \sigma(v)) = B'(v', v')$, por la Proposición 4.6 podemos elegir $\sigma' \in \mathcal{O}(V' \perp V_1')$ tal que $\sigma'(\sigma(v)) = v'$. Así $\sigma' \circ \sigma\colon V \perp V_1 \to V' \perp V_1'$ envía v en v' y, por lo tanto, induce una isometría de $(Fv)^\perp \perp V_1$ en $(Fv')^\perp \perp V_1'$, donde $(Fv)^\perp$ y $(Fv')^\perp$ denotan a los complementos ortogonales de Fv y Fv' en V y V', respectivamente. Como σ'' induce una isometría entre $(Fv)^\perp$ y $(Fv')^\perp$, la demostración se termina por inducción en la dimensión de V □

5. Teorema de equivalencia de cadena de Witt

Este teorema describe la equivalencia de dos formas diagonales en términos de la equivalencia de formas binarias. Primero comenzamos con el siguiente resultado

Teorema 5.1. *Sean (V, q_V) y (W, q_W) dos espacios cuadráticos y sean $\{v_1, \ldots, v_n\}$ y $\{w_1, \ldots, w_n\}$ bases ortogonales de (V, q_V) y (W, q_W) respectivamente. Si (V, q_V) y (W, q_W) son isométricos, entonces existe una familia $\{v_1^j, \ldots, v_n^j\}$ $(0 \leq j \leq m)$ de bases ortogonales de (V, q_V) tal que*

1) $v_i^0 = v_i$ para todo $1 \leq i \leq n$,

2) Para cada $0 \leq j < m$ existen i_j e i_j' tales que $v_i^{j+1} = v_i^j$ para todo $i \notin \{i_j, i_j'\}$ y $Fv_{i_j}^{j+1} + Fv_{i_j'}^{j+1} = Fv_{i_j}^j + Fv_{i_j'}^j$,

3) $q_V(v_i^m) = q_W(w_i)$ para todo $1 \leq i \leq n$.

Demostración. Sea $\sigma\colon (W, q_W) \to (V, q_V)$ una isometría. Hacemos la demostración de manera algorítmica:

1) Sea h el mínimo índice tal que $q_W(w_h) \neq 0$. Escribamos $x_1v_1 + \cdots + x_nv_n = \sigma(w_h)$ y elijamos una familia maximal $\{x_{l_1}, \ldots, x_{l_s}\}$ tal que $x_{l_1}^2 q_V(v_{l_1}) + \cdots + x_{l_s}^2 q_V(v_{l_s}) = 0$. El complemento $\{x_{i_1}, \ldots, x_{i_r}\}$ de esta familia tiene la propiedad de que $x_{i_1}^2 q_V(v_{i_1}) + \cdots + x_{i_r}^2 q_V(v_{i_r}) = q_W(w_h)$ y de que ninguna subsuma de esta suma se anula.

2) Definimos la base ortogonal $\{v_1^1, \ldots, v_n^1\}$ de V, por $v_i^1 = v_i$ si $i \neq i_1$ y $v_{i_1}^1 = x_{i_1}v_{i_1}$.

3) Definimos recursivamente las bases ortogonales $\{v_1^j, \ldots, v_n^j\}$ de V $(1 < j \leq r)$, por

$$\begin{aligned} v_i^{j+1} &= v_i^j \text{ si } i \notin \{i_j, i_{j+1}\}, \\ v_{i_{j+1}}^{j+1} &= v_{i_j}^j + x_{i_{j+1}}^j v_{i_{j+1}}^j, \\ v_{i_j}^{j+1} &\in \left(Fv_{i_{j+1}}^{j+1}\right)^\perp \subseteq Fv_{i_j}^j + Fv_{i_{j+1}}^j. \end{aligned}$$

4) Observamos que la cadena $\{v_1^j, \ldots, v_n^j\}$ $(1 \leq j \leq r)$ cumple con las propiedades 1) y 2) del enunciado y que $v_{i_r}^r = x_{i_1}v_{i_1} + \cdots + x_{i_r}v_{i_r}$, de modo que $q_V(v_{i_r}^r) = q_W(w_h)$.

5) Si $i_r \neq h$, obtenemos mediante la transposición de v_{i_r} con los elementos que están entre él y v_h una cadena de bases $\{v_1^j, \ldots, v_n^j\}$ ortogonales de V $(r+1 \leq j \leq r+h-i_r)$ tal que $v_h^{r+h-i_r} = v_{i_r}^r$

6) Por el teorema de cancelación de Witt podemos encontrar un isomorfismo de $Fv_1^{r+h-i_r} + \cdots + Fv_{h-1}^{r+h-i_r} + Fv_{h+1}^{r+h-i_r} + \cdots + Fv_n^{r+h-i_r}$ en $Fw_1 + \cdots + Fw_{h-1} + Fw_{h+1} + \cdots + Fw_n$. Ahora continuamos, empezando de vuelta con el item 1). El proceso se termina cuando, después de sucesivas cancelaciones, llegamos a espacios de dimensión 0 $\square$

A continuación introducimos la noción de equivalencia simple de formas diagonales. Sean $q = \langle a_1, \ldots, a_n\rangle$ y $q' = \langle a_1', \ldots, a_n'\rangle$. Decimos que q y q' son simplemente equivalentes si existen dos índices $1 \leq i_1 \leq i_2 \leq n$ tales que

1) $\langle a_{i_1}, a_{i_2}\rangle \simeq \langle a_{i_1}', a_{i_2}'\rangle$,
2) $a_i = a_i'$ para todo $i \notin \{i_1, i_2\}$.

Más generalmente decimos que q y q' son equivalentes en cadena si existe una sucesión de formas diagonales $q_0, \ldots, q_m$ tales que $q_0 = q$, $q_m = q'$ y q_{i+1} es simplemente equivalente a q_i para todo $0 \leq i < m$. La relación de equivalencia en cadena es claramente una relación de equivalencia sobre las formas diagonales de una dimensión fija. Nosotros denotaremos esta relación por $q \sim q'$. Es claro que $q \sim q'$ implica que $q \simeq q'$. A continuación establecemos la inversa de esto.

Teorema 5.2 (de equivalencia de cadena de Witt). *Sean $q = \langle a_1, \ldots, a_n\rangle$ y $q' = \langle a_1', \ldots, a_n'\rangle$ dos formas diagonales arbitrarias de la misma dimensión. Si $q \simeq q'$, entonces $q \sim q'$.*

Demostración. Sea $\{e_i : 1 \leq i \leq n\}$ la base canónica de F^n. Por el Teorema 5.1, existe una familia $\{v_1^j, \ldots, v_n^j\}$ $(0 \leq j \leq m)$ de bases ortogonales de (F^n, q) tal que

1) $v_i^0 = e_i$ para todo $1 \leq i \leq n$,
2) Para cada $0 \leq j < m$ existen i_j e i'_j tales que $v_i^{j+1} = v_i^j$ para todo $i \notin \{i_j, i'_j\}$ y $Fv_{i_j}^{j+1} + Fv_{i'_j}^{j+1} = Fv_{i_j}^j + Fv_{i'_j}^j$,
3) $q(v_i^m) = q'(e_i)$ para todo $1 \leq i \leq n$.

Para cada $0 \leq j \leq m$ denotemos con q_j a la forma diagonal $\langle q(v_1^j), \ldots, q(v_n^j)\rangle$. Es claro que $q_0 = q$ y que $q_m = q'$. Así, para terminar la demostración es suficiente ver que si $\sigma_j \colon F^n \to F^n$ es el isomorfismo definido por:

1) $\sigma_j(e_i) = e_i$ para todo $i \notin \{i_j, i'_j\}$,
2) $\sigma_j(e_{i_j}) = x_{i_j}e_{i_j} + x_{i'_j}e_{i'_j}$ y $\sigma_j(e_{i'_j}) = y_{i_j}e_{i_j} + y_{i'_j}e_{i'_j}$, donde x_{i_j}, $x_{i'_j}$, y_{i_j} e $y_{i'_j}$ están dados por $v_{i_j}^{j+1} = x_{i_j}v_{i_j}^j + x_{i'_j}v_{i'_j}^j$ y $v_{i'_j}^{j+1} = y_{i_j}v_{i_j}^j + y_{i'_j}v_{i'_j}^j$,

entonces $q_{j+1} = q_j \circ \sigma_j$. En efecto,

$$q_{j+1}(e_{i_j}) = q(v_{i_j}^{j+1}) = x_{i_j}^2 q(v_{i_j}^j) + x_{i'_j}^2 q(v_{i'_j}^j) = x_{i_j}^2 q_j(e_{i_j}) + x_{i'_j}^2 q_j(e_{i'_j}) = q_j(\sigma_j(e_{i_j})),$$
$$q_{j+1}(e_{i'_j}) = q(v_{i'_j}^{j+1}) = y_{i_j}^2 q(v_{i_j}^j) + y_{i'_j}^2 q(v_{i'_j}^j) = y_{i_j}^2 q_j(e_{i_j}) + y_{i'_j}^2 q_j(e_{i'_j}) = q_j(\sigma_j(e_{i'_j}))$$

y

$$q_{j+1}(e_i) = q(v_i^{j+1}) = q(v_i^j) = q_j(e_i) = q_j(\sigma(e_i)) \qquad \text{si } i \notin \{i_j, i'_j\} \quad \square$$

6. Producto de formas cuadráticas

Sean (V_1, B_1, q_1) y (V_2, B_2, q_2) dos espacios cuadráticos sobre F. Definimos el producto $(V_1 \otimes V_2, B_1 \otimes B_2, q_1 \otimes q_2)$, por

$$(B_1 \otimes B_2)(v_1 \otimes v_2, v'_1 \otimes v'_2) = B_1(v_1, v'_1)B_2(v_2, v'_2).$$

Por definición

$$(q_1 \otimes q_2)(v_1 \otimes v_2) = (B_1 \otimes B_2)(v_1 \otimes v_2, v_1 \otimes v_2) = B_1(v_1, v_1)B_2(v_2, v_2) = q_1(v_1)q_2(v_2).$$

Proposición 6.1. *Se satisfacen:*

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

Demostración. Sean (V_1, B_1, q_1) y (V_2, B_2, q_2) dos espacios cuadráticos sobre F. Es fácil ver que el isomorfismo lineal $\sigma \colon V_1 \otimes V_2 \to V_2 \otimes V_1$ definido por $\sigma(v_1 \otimes v_2) = v_2 \otimes v_1$ satisface $(B_2 \otimes B_1) \circ \sigma = B_1 \otimes B_2$. Así, $(V_1 \otimes V_2, B_1 \otimes B_2, q_1 \otimes q_2) \simeq (V_2 \otimes V_1, B_2 \otimes B_1, q_2 \otimes q_1)$. Esto prueba el item 1). La demostración de los item 2) y 3) es similar. $\square$

Usando la propiedad distributiva obtenemos que

$$\langle a_1, \ldots, a_n\rangle\langle b_1, \ldots, b_m\rangle \simeq \langle a_1b_1, \ldots, a_ib_j, \ldots, a_nb_m\rangle.$$

Corolario 6.2. *Para cada forma cuadrática regular q, tenemos que $q \otimes H \simeq \dim(q)H$, donde $\dim(q)H$ denota a la suma ortogonal de H consigo misma $\dim(q)$ veces.*

Demostración. Por la propiedad distributiva basta probarlo para $q = \langle a \rangle$, pero

$$\langle a \rangle \langle 1, -1 \rangle \simeq \langle a, -a \rangle,$$

que por la Proposición 3.3 es isomorfo a H. □

De ahora en más escribiremos también B_1B_2 en lugar de $B_1 \otimes B_2$ y q_1q_2 en lugar de $q_1 \otimes q_2$.

Apéndice: Generación del grupo ortogonal por reflexiones

El proposito de este apéndice es probar el siguiente teorema de estructura para el grupo ortogonal de un espacio cuadrático.

Teorema de Cartan-Dieudonné. *Sea (V, B, q) un espacio cuadrático regular de dimensión n. Cada isometría $\sigma \in \mathcal{O}_q(V)$ es una composición de a lo sumo n reflexiones de hiperplanos.*

Antes de demostrar este importante teorema, daremos algunos de sus Corolarios

Corolario 1. *Cada isometría tiene determinante ± 1. Las isometrías que tienen determinante 1 forman un subgrupo $\mathcal{SO}_q(V)$ de índice 2 de $\mathcal{O}_q(V)$. Este subgrupo es el núcleo del morfismo $\det\colon \mathcal{O}_q(V) \to \{1, -1\}$ y se llama el grupo especial ortogonal de q.*

Corolario 2. *Supongamos que σ se puede expresar como la composición de n reflexiones. Entonces la primera (y similarmente la última) de estas reflexiones, puede ser elegida arbitrariamente.*

Demostración. Escribamos σ como una composición de reflexiones $\sigma = \tau_1 \circ \cdots \circ \tau_n$ y sea τ una reflexión dada. Consideremos la isometría $\tau \circ \sigma$. Por el teorema, podemos escribir $\tau \circ \sigma$ como una composición de reflexiones $\tau \circ \sigma = \tau_2' \circ \cdots \circ \tau_r'$ con $r \leq n + 1$. Ahora, dado que $\det(\sigma) = (-1)^n = (-1)^r$, resulta que $r = n \pmod 2$. En consecuencia, de la desigualdad $r \leq n+1$ se obtiene que $r \leq n$. Dado que $\tau^{n-r} = id$, podemos escribir $\sigma = \tau \circ \tau_2' \circ \cdots \circ \tau_r' \circ \tau^{n-r}$, lo que termina la demostración. □

Corolario 3. *Si $\dim(V) = 2$, entonces cada isometría con determinante -1 es una reflexión y si $\dim(V) \leq 3$ entonces cada $\sigma \in \mathcal{SO}_q(V)$ es la composición de dos reflexiones.*

Corolario 4. *Se satisfacen:*

1) *Si $\sigma \in \mathcal{O}_q(V)$ es la composición de r reflexiones, donde r es menor o igual que n, entonces la dimensión del subespacio de vectores dejados fijos por σ es al menos $n - r$.*
2) *Si $\sigma \in \mathcal{O}_q(V)$ no deja fijo a ningún vector no nulo, entonces σ no puede ser escrito como una composición de menos de n reflexiones.*

Demostración. 1) Escribamos σ como una composición $\sigma = \tau_1 \circ \cdots \circ \tau_r$ de r reflexiones y sea U_j el hiperplano de los puntos dejados fijos por τ_j. Es claro que $U_1 \cap \cdots \cap U_r$ consiste de vectores dejados fijos por σ y que $\dim(U_1 \cap \cdots \cap U_r) \geq n - r$.

2) Es una consecuencia inmediata de 1). $\square$

A continuación daremos la demostración del teorema. Para cada isometría σ denotamos con $\widetilde{\sigma}$ a $\sigma - id$.

Lema 1. *Se satisfacen:*

1) $\mathrm{Ker}(\widetilde{\sigma}) = \mathrm{Im}(\widetilde{\sigma})^{\perp}$.

2) $\mathrm{Ker}(\widetilde{\sigma})^{\perp} = \mathrm{Im}(\widetilde{\sigma})$.

3) $\mathrm{Im}(\widetilde{\sigma}) \subseteq \mathrm{Ker}(\widetilde{\sigma})$ *si y sólo si* $\mathrm{Im}(\widetilde{\sigma})$ *es totalmente isotrópico.*

Demostración. 1) Para todo $v, w \in V$, tenemos

$$\begin{aligned} B(v, \widetilde{\sigma}(w)) &= B(v, \sigma(w) - w) = B(v, \sigma(w)) - B(v, w) \\ &= B(v, \sigma(w)) - B(\sigma(v), \sigma(w)) = -B(\widetilde{\sigma}(v), \sigma(w)). \end{aligned}$$

Así,

$$\begin{aligned} v \in \mathrm{Im}(\widetilde{\sigma})^{\perp} &\iff B(\widetilde{\sigma}(v), w) = 0 \text{ para todo } w \in V \\ &\iff \widetilde{\sigma}(v) \in \mathrm{rad}\, V = 0 \\ &\iff v \in \mathrm{Ker}(\widetilde{\sigma}). \end{aligned}$$

2) Se sigue inmediatamente del item 1) y del item 6) de la Proposición 1.3.

3) Se sigue de que,

$$\mathrm{Im}(\widetilde{\sigma}) \text{ es totalmente isotrópico } \iff \mathrm{Im}(\widetilde{\sigma}) \subseteq \mathrm{Im}(\widetilde{\sigma})^{\perp}$$

y del item 1). $\square$

Lema 2. *Para cada* $v \in V$*, tenemos*

$$B(\widetilde{\sigma}(v), \widetilde{\sigma}(v)) = -2B(\widetilde{\sigma}(v), v).$$

En particular $\widetilde{\sigma}(v)$ *es nulo o isotrópico si y sólo si es ortogonal a* v*.*

Demostración. En efecto

$$\begin{aligned} B(\widetilde{\sigma}(v), \widetilde{\sigma}(v)) &= B(\sigma(v) - v, \sigma(v) - v) \\ &= B(\sigma(v), \sigma(v)) - 2B(\sigma(v), v) + B(v, v) \\ &= 2\big(B(v, v) - B(\sigma(v), v)\big) = -2B(\widetilde{\sigma}(v), v). \quad \square \end{aligned}$$

Lema 3. *Supongamos que* $\mathrm{Ker}(\widetilde{\sigma})$ *es totalmente isotrópico y* $\dim(V) = 2$*. Entonces si* $v \in V$ *es anisotrópico, también* $\widetilde{\sigma}(v)$ *es anisotrópico.*

Demostración. Sea $v \in V$ anisotrópico. Como $\mathrm{Ker}(\widetilde{\sigma})$ es totalmente isotrópico, $\widetilde{\sigma}(v) \neq 0$. Supongamos que $\widetilde{\sigma}(v)$ es isotrópico. Entonces, por el Lema 2, v es ortogonal a $\widetilde{\sigma}(v)$. Así, $V = Fv \perp F\widetilde{\sigma}(v)$, lo que es una contradicción, ya que $\widetilde{\sigma}(v)$ pertenece al radical de $Fv \perp F\widetilde{\sigma}(v)$, pero V es regular por hipótesis. $\square$

Demostración del Teorema de Cartan-Dieudonné

Paso 1). Supongamos que existe $w \in \mathrm{Ker}(\widetilde{\sigma})$ anisotrópico. En este caso σ induce una isometría en $(Fw)^\perp$ y, por inducción, la restricción de σ a $(Fw)^\perp$ puede ser escrita como una composición de a lo sumo $n-1$ reflexiones en $(Fw)^\perp$. Cada una de estas reflexiones se extiende de manera única a una reflexión de V que deja fijo w. Es claro que σ es la composición de estas reflexiones.

Paso 2). Supongamos que $\mathrm{Ker}(\widetilde{\sigma})$ es totalmente isotrópico (es decir que $\mathrm{Ker}(\widetilde{\sigma}) \subseteq \mathrm{Ker}(\widetilde{\sigma})^\perp$). Entonces, por el item 2) del Lema 1, $\mathrm{Ker}(\widetilde{\sigma}) \subseteq \mathrm{Im}(\widetilde{\sigma})$. Supongamos ahora que $\mathrm{Im}(\widetilde{\sigma})$ es estrictamente mayor que $\mathrm{Ker}(\widetilde{\sigma})$. Por el item 3) del Lema 1 esto implica que $\mathrm{Im}(\widetilde{\sigma})$ contiene vectores anisotrópicos. Afirmamos que existe un vector $\widetilde{\sigma}(v)$, anisotrópico y tal que v también es anisotrópico. Veamos como encontrarlo. Si $\dim(V) = 2$, entonces (considerando una base de V y procediendo como en la nota que sigue al Corolario 2.3) podemos tomar v anisotrópico y aplicar el Lema 3. Si no, tomamos $\widetilde{\sigma}(v)$ anisotrópico (de nuevo, considerando una base de $\mathrm{Im}(\widetilde{\sigma})$ y procediendo como en la nota que sigue al Corolario 2.3). Si v es anisotrópico, ya está. Si no tomamos un vector w ortogonal a v y anisotrópico. Para encontrarlo incluímos a v en un espacio hiperbólico H, como está indicado en el Teorema 3.5 y buscamos w en $H^\perp$ (tomando una base de $H^\perp$ y usando nuevamente el procedimiento descripto en la nota que sigue al Corolario 2.3). Si $\widetilde{\sigma}(w)$ es anisotrópico, también está. Podemos suponer entonces que $\widetilde{\sigma}(w)$ es nulo o isotrópico. Afirmamos que cualquiera sea $\epsilon \in \dot{F}$, el vector $w + \epsilon v$ es anisotrópico. En efecto

$$B(v + \epsilon w, v + \epsilon w) = B(v, v) + \epsilon^2 B(w, w) = \epsilon^2 B(w, w) \neq 0.$$

Veamos ahora como encontrar ϵ tal que $\widetilde{\sigma}(v + \epsilon w)$ también sea anisotrópico. Por el Lema 2, esto es lo mismo que encontrar ϵ tal que

$$\begin{aligned} 0 &\neq B(\widetilde{\sigma}(v + \epsilon w), v + \epsilon w) \\ &= B(\widetilde{\sigma}(v), v) + \epsilon\big(B(\widetilde{\sigma}(w), v) + B(\widetilde{\sigma}(v), w)\big) + \epsilon^2 B(\widetilde{\sigma}(w), w) \\ &= B(\widetilde{\sigma}(v), v) + \epsilon\big(B(\widetilde{\sigma}(w), v) + B(\widetilde{\sigma}(v), w)\big), \end{aligned}$$

donde la última igualdad se deduce de que por el Lema 2, $B(\widetilde{\sigma}(w), w) = 0$. Ahora si tuvieramos

$$0 = B(\widetilde{\sigma}(v), v) + \epsilon\big(B(\widetilde{\sigma}(w), v) + B(\widetilde{\sigma}(v), w)\big),$$

para dos valores distintos de ϵ, obtendríamos que

$$B(\widetilde{\sigma}(v), v) = 0 = B(\widetilde{\sigma}(w), v) + B(\widetilde{\sigma}(v), w).$$

Pero por el Lema 2 la primera igualdad es falsa. Podemos tomar entonces $\epsilon = 1$ o $\epsilon = -1$ para asegurarnos de encontrar $v + \epsilon w \in V$ tal que tanto $v + \epsilon w$ como $z = \widetilde{\sigma}(v + \epsilon w)$ sean anisotrópicos. Por la Proposición 4.6, $\tau_z(\sigma(v + \epsilon w)) = v + \epsilon w$. Por el Paso 1), $\tau_z \circ \sigma$ se expresa como la composición de a lo sumo $n-1$ reflexiones, de donde $\sigma = \tau_z \circ (\tau_z \circ \sigma)$ es la composición de a lo sumo n reflexiones.

Paso 3). Supongamos que $\mathrm{Ker}(\widetilde{\sigma})$ es totalmente isotrópico y que $\mathrm{Ker}(\widetilde{\sigma}) = \mathrm{Im}(\widetilde{\sigma})$. Por el teorema de la dimensión

$$n = \dim(\mathrm{Ker}(\widetilde{\sigma})) + \dim(\mathrm{Im}(\widetilde{\sigma})) = 2\dim(\mathrm{Ker}(\widetilde{\sigma})).$$

Así, n es par. (Como $\mathrm{Ker}(\widetilde{\sigma})$ es totalmente isotrópico, esta ecuación junto con el item 1) del Teorema 3.5, implica que V es un espacio hiperbólico, pero nosotros

no usaremos esta información). Ademas σ actúa como la identidad sobre $\mathrm{Ker}(\widetilde{\sigma})$ e induce la identidad en $V/\mathrm{Ker}(\widetilde{\sigma})$, ya que $\widetilde{\sigma}(V) \subseteq \mathrm{Ker}(\widetilde{\sigma})$. En particular $\det(\sigma) = 1$. Tomemos una reflexion cualquiera τ. Como $\det(\tau \circ \sigma) = -1$ no podemos estar con $\tau \circ \sigma$ en la situación del Paso 3). Así, procediendo como en los Pasos 1) y 2) podemos expresar $\tau \circ \sigma$ como una composición de a lo sumo n reflexiones. Pero como n es par y $\det(\tau \circ \sigma) = -1$ debemos tener a lo sumo $n-1$ reflexiones, de donde $\sigma = \tau \circ (\tau \circ \sigma)$ es la composición de a lo sumo n reflexiones. $\square$

Ejercicios

Ejercicio 1. *Pruebe que el grupo de isometrías del espacio n-dimencional cuadrático $n\langle 1\rangle$ es isomorfo al grupo de matrices ortogonales de $n \times n$ sobre F.*

Ejercicio 2. *Sea $V = M_n(F)$ considerado como espacio vectorial de dimensión n^2 sobre F. Pruebe que la aplicación $B\colon V \times V \to F$, definida por $B(X,Y) = \mathrm{tr}(XY)$, define un espacio cuadrático regular (V,B). Muestre que (V,B) es isométrico a $n\langle 1\rangle \perp \frac{n(n-1)}{2}H$ y encuentre una base ortogonal para (V,B). Resuelva el mismo problema con la forma $B'\colon V \times V \to F$, definida por $B'(X,Y) = \mathrm{tr}(XY^t)$, y muestre que (V,B') es isométrico a $n^2\langle 1\rangle$.*

Ejercicio 3. *Sea V como en el ejercicio anterior. Consideremos la aplicación $B_U\colon V \times V \to F$, definida por $B_U(X,Y) = \mathrm{tr}(XUY^tU^{-1})$, donde $U \in M_n(F)$ es una matriz simétrica inversible. Pruebe que B_U es una forma bilineal simétrica y no singular. Haga cálculos explícitos para $n = 2$ y $U = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ y muestre que en este caso (V, B_U) es hiperbólico.*

Ejercicio 4. *Sea K/F una extensión finita y separable. Muestre que la aplicación $B\colon K \times K \to F$, definida por $B(x,y) = \mathrm{tr}(xy)$, define un espacio cuadrático regular (K,B). Encuentre una diagonalización para el caso $F = \mathbb{Q}$ y $K = \mathbb{Q}(\sqrt[3]{2})$.*

Ejercicio 5. *Sea $a, b \in \dot{F}$ y f una una forma cuadrática regular. Pruebe que $f \perp \langle a\rangle$ representa $-b$ si y sólo si $f \perp \langle b\rangle$ representa $-a$.*

Ejercicio 6. *Sean $a, b \in F$ tales que $c = a^2 + b^2 \neq 0$. Pruebe que el espacio $\langle 1, 1, -c, -c\rangle$ es hiperbólico.*

Ejercicio 7. *Sea f una forma cuadrática isotrópica sobre un cuerpo de más de 5 elementos. Muestre que existe una diagonalización en la que f tiene un vector isotrópico que no tiene ninguna coordenada nula.*

Ejercicio 8. *Supongamos que F es la intersección de los subcuerpos $F_1, \ldots, F_n$ en algún medio ambiente. Pruebe que si $\dot{F}_i/\dot{F}_i^2$ es finito para cada i, entonces $\dot{F}/\dot{F}^2$ también es finito.*

Ejercicio 9. *Sea A un dominio de factorización única. Denotemos con U al grupo de unidades de A y con F a su cuerpo de fracciones. Pruebe que $\dot{F}/\dot{F}^2$ es el producto directo de U/U^2 y de un $\mathbb{Z}/2\mathbb{Z}$ espacio vectorial, que tiene por base a un conjunto de representantes de los primos de A. Concluya que si $A = \mathbb{Z}$ y $\{p_1, \ldots, p_n\}$ y $\{q_1, \ldots, q_n\}$ son conjuntos de primos positivos distintos, entonces $\langle p_1, \ldots, p_n\rangle = \langle q_1, \ldots, q_n\rangle$ si y sólo si $\{p_1, \ldots, p_n\} = \{q_1, \ldots, q_n\}$.*

Ejercicio 10. *Pruebe que las siguientes condiciones son equivalentes*

1) Toda forma de dimensión 4 *sobre* F *con determinante* -1 *es isotrópica.*

2) Toda forma de dimensión par sobre F *con determinante* -1 *es isotrópica.*

3) Toda forma de dimensión 3 *sobre* F *representa a su propio determinante.*

4) Toda forma de dimensión impar sobre F *representa a su propio determinante.*

Ejercicio 11. *Pruebe el siguiente teorema de extensión de Witt: Sea* V *un espacio cuadrático regular y sean* U_1 *y* U_2 *subespacios de* V*. Toda isometría de* U_1 *en* U_2 *se extiende a una isometría de* V *en si mismo.*

Ejercicio 12. *Usando el teorema de cancelación de Witt, muestre que si* U *es un subespacio de dimensión* $m+r$ *en un espacio hiperbólico* mH*, entonces el índice de Witt de* U *es al menos* r*.*

Ejercicio 13. *Sea* $a \in \dot{F}$*. Pruebe que* $D(\langle 1, a\rangle)$ *es un subgrupo de* $\dot{F}$*.*

Ejercicio 14. *Sean* φ *y* σ *dos formas regulares. Pruebe que si* $D(\varphi)$ *es un subgrupo de* $\dot{F}$*, entonces* $D(\varphi)D(\varphi\otimes\sigma) = D(\varphi\otimes\sigma)$*.*

Ejercicio 15. *Pruebe que si* σ *tiene índice de Witt* m*, entonces* $\varphi\otimes\sigma$ *tiene índice de Witt mayor o igual que* $m\dim(\varphi)$ *y* $\varphi\perp\sigma$ *tiene índice de Witt menor o igual que* $m+\dim(\varphi)$*.*

Capítulo 2

1. Definición de $\widehat{W}(F)$ y de $W(F)$

Dado un cuerpo F denotamos con $M(F)$ al conjunto de las clases de isometría de formas cuadráticas regulares sobre F. En realidad $M(F)$ dotado de la estructura aditiva $\perp$ y multiplicativa $\otimes$ es un semianillo conmutativo. Por el Teorema de cancelación de Witt la estructura aditiva de este semianillo es cancelativa. De la misma manera que los naturales se pueden extender a los enteros, $M(F)$ se puede incluír en un anillo $\widehat{W}(F)$, que se llama el anillo de Grothendieck-Witt de F. En general dado un semianillo M cuya suma es cancelativa se define una relación $\sim$ en $M\times M$, por

$$(x,y)\sim(x',y') \quad \text{si y sólo si} \quad x+y'=x'+y.$$

El hecho de que la suma de M sea cancelativa implica que $\sim$ es una relación de equivalencia. El anillo de Grothendieck, $\mathrm{Groth}(M)$ de M es, por definición, el conjunto de clases $(M\times M)/\sim$, de esta relación, con las operaciones de suma y producto inducidas por

$$(x,y)+(x',y')=(x+x',y+y') \quad \text{y} \quad (x,y)(x',y')=(xx'+yy',xy'+yx').$$

Es fácil ver que las operaciones de $\mathrm{Groth}(M)$ están bien definidas y que $\mathrm{Groth}(M)$ es un anillo (siendo la clase de (x,y) la opuesta de la de (y,x)). Además la aplicación $i\colon M\to\mathrm{Groth}(M)$, que envía $i(x)$ en la clase de $(x,0)$, respeta la suma y el producto. De aqui en adelante vamos a identificar cada $x\in M$ con $i(x)$. Notemos que la clase de (x,y) es igual a $i(x)-i(y)$. Así, $\mathrm{Groth}(M)$ está generado aditivamente por M. Por último cada morfismo de semianillos f, de M en un anillo R, se extiende de manera única a un morfismo de anillo $f\colon \mathrm{Groth}(M)\to R$, dado por $f(x-y)=f(x)-f(y)$.

Definición 1.1. *El anillo de Grothendieck-Witt* $\widehat{W}(F)$ *de* F *es por definición* $\mathrm{Groth}(M(F))$.

Dado un espacio cuadrático (V, B, q) sobre F, vamos a denotar con el mismo símbolo (V, B, q) a su clase de isometría. Cada elemento de $\widehat{W}(F)$ tiene la forma $q_1 - q_2$, donde q_1 y q_2 son formas cuadráticas regulares. Como la aplicación $\dim\colon M(F) \to \mathbb{Z}$, definida por $\dim((V, B, q)) = \dim(V)$, es un morfismo de semianillos, queda definido un morfismo de anillos $\dim\colon \widehat{W}(F)$ por $\dim((V_1, B_1, q_1) - (V_2, B_2, q_2)) = \dim(V_1) - \dim(V_2)$. El núcleo $\widehat{I}F$ de este morfismo de anillos es llamado el ideal de aumentación de $\widehat{W}(F)$.

Proposición 1.2. *La sucesión exacta corta*

$$0 \to \widehat{I}F \to \widehat{W}(F) \xrightarrow{\dim} \mathbb{Z} \to 0$$

es partible como sucesión de grupos y el morfismo $s\colon \mathbb{Z} \to \widehat{W}(F)$ *definido por* $s(n) = n\langle 1\rangle$ *es una sección de* dim. *Así, la aplicación*

$$\widehat{W}(F) \to \mathbb{Z} \oplus \widehat{I}F,$$

que envía q *en* $(\dim(q), q - \dim(q)\langle 1\rangle)$ *es un isomorfismo de grupos. Dado que* $\widehat{W}(F)$ *está aditivamente generado por las clases de las formas regulares de dimensión* 1, *esto muestra en particular que* $\widehat{I}F$ *está aditivamente generado por las expresiones de la forma* $\langle a\rangle - \langle 1\rangle$ *con* $a \in \dot{F}$. *La estructura de producto de* $\mathbb{Z} \oplus \widehat{I}F$, *obtenida a través de este isomorfismo es* $(m, \alpha)(n, \beta) = (mn, n\alpha + m\beta + \alpha\beta)$.

Del Corolario 6.2 se deduce fácilmente que $\mathbb{Z}.H$ es un ideal de $\widehat{W}(F)$.

Definición 1.3. *El anillo de Witt de* F *es por definición el anillo cociente* $W(F) = \widehat{W}(F)/\mathbb{Z}.H$.

Proposición 1.4. *Se satisfacen:*

1) *Los elementos de* $W(F)$ *estan en correspondencia con las clases de isometría de todas las formas anisotrópicas.*
2) *Dos formas cuadráticas regulares* q *y* q' *representan el mismo elemento en* $W(F)$ *si y sólo si* $q_a \simeq q'_a$, *donde* q_a *es la componente anisotrópica de* q *y* q'_a *es la componente anisotrópica de* q'.
3) *Si* q *y* q' *son dos formas cuadráticas regulares y* $\dim(q) = \dim(q')$, *entonces* q *y* q' *representan el mismo elemento en* $W(F)$ *si y sólo si* $q \simeq q'$.

Demostración. Los items 2) y 3) se deducen fácilmente del item 1). Veamos este. Sea $a \in \dot{F}$. Dado que $\langle a, -a\rangle \simeq H$, tenemos que $\langle -a\rangle = -\langle a\rangle$ en $W(F)$. Usando esto se deduce fácilmente que todo elemento de $W(F)$ está representado por una forma cuadrática regular. Es claro que si $q = q_a \perp q_h$ entonces q y q_a representan al mismo elemento de $W(F)$. Así, cada elemento de $W(F)$ está representado por una forma cuadrática anisotrópica. Por último supongamos que q y q' son formas cuadráticas anisotrópicas que representan al mismo elemento de $W(F)$. Por definición existe un entero m tal que $q = q' + mH$ en $\widehat{W}(F)$. Sin pérdida de generalidad podemos suponer que $m \geq 0$. Entonces $q \simeq q' \perp mH$ y así, como q y q' son anisotrópicas, $q \simeq q'$. $\square$

A la imagen de $\widehat{I}F$ por la proyección canónica $\pi\colon \widehat{W}(F) \to W(F)$, la denotaremos IF. Dado que $\dim(H) = 2$, tenemos que $\widehat{I}F \cap \mathbb{Z}.H = 0$. Así, π induce un isomorfismo de $\widehat{I}F$ en IF.

Proposición 1.5. *Una forma regular q representa un elemento en IF si y sólo si* $\dim(q)$ *es par.*

Demostración. $\Rightarrow$) Es claro que podemos suponer que q es una forma binaria $q = \langle a, b\rangle$. Entonces q es la imagen de $\langle a\rangle - \langle -b\rangle \in \widehat{I}F$ bajo la proyección canónica $\pi\colon \widehat{W}(F) \to W(F)$.

$\Leftarrow$) Si q representa un elemento en IF, entonces existe una ecuación $q = q_1 - q_2 + m.H$ en $\widehat{W}(F)$, donde q_1 y q_2 son formas cuadráticas regulares de la misma dimensión y $m \in \mathbb{Z}$. Así, $\dim(q) = 2m$. $\square$

El epimorfismo de anillos $\dim\colon \widehat{W}(F) \to \mathbb{Z}$ induce otro epimorfismo de anillos $\dim_0\colon W(F) \to \mathbb{Z}/2\mathbb{Z}$. Por Proposición 1.5 el núcleo de $\dim_0$ es IF.

2. Grupo de clases de cuadrados

El determinante $\mathrm{d}\colon M(F) \to \dot{F}/\dot{F}^2$ es un morfismo de semigrupos y por lo tanto se extiende a un morfismo de grupos $\mathrm{d}\colon \widehat{W}(F) \to \dot{F}/\dot{F}^2$. Como $\mathrm{d}(H) = -1.\dot{F}^2$ este morfismo no se factoriza a través de $W(F)$. Definimos el determinante con signo $\mathrm{d}_\pm(q)$ de una forma cuadrática regular q poniendo $\mathrm{d}_\pm(q) = (-1)^{n(n-1)/2}\,\mathrm{d}(q)$, donde n es la dimensión de q. La ventaja obvia de $\mathrm{d}_\pm(q)$ sobre $\mathrm{d}(q)$ es que $\mathrm{d}_\pm(H) = 1.\dot{F}^2$. Sin embargo la fórmula $\mathrm{d}_\pm(q_1 \perp q_2) = \mathrm{d}_\pm(q_1)\,\mathrm{d}_\pm(q_2)$ es falsa, de modo que $\mathrm{d}_\pm$ ni siquiera determina un morfismo de $W(F)$ en $\dot{F}/\dot{F}^2$. Para solucionar este problema definimos un morfismo que parte de $W(F)$, llega a una extensión de $\dot{F}/\dot{F}^2$ por $\mathbb{Z}/2\mathbb{Z}$ y combina a $\mathrm{d}_\pm$ con $\dim_0$. Denotemos con $Q(F)$ al conjunto $\mathbb{Z}/2\mathbb{Z} \times \dot{F}/\dot{F}^2$. En $Q(F)$ definimos un producto, poniendo

$$(e, d)(e', d') = (e + e', (-1)^{ee'} dd').$$

Es fácil ver que este producto es asociativo y conmutativo y que tiene a $(0, 1)$ como neutro. Dado que

$$(e, d)(e, (-1)^e d) = (e + e, (-1)^{ee}(-1)^e dd) = (0, 1),$$

cada elemento (e, d) de $Q(F)$ tiene a $(e, (-1)^e d)$ como inversa y así, $Q(F)$ es un grupo. También es claro que la aplicaciones $i\colon \dot{F}/\dot{F}^2 \to Q(F)$ y $\pi\colon Q(F) \to \mathbb{Z}/2\mathbb{Z}$, definidas por $i(d) = (0, d)$ y $\pi(e, d) = e$ son morfismos de grupos y que

$$1 \to \frac{\dot{F}}{\dot{F}^2} \xrightarrow{i} Q(F) \xrightarrow{\pi} \frac{\mathbb{Z}}{2\mathbb{Z}} \to 0.$$

es una la sucesión exacta corta.

Nota. Por definición $Q(F)$ es una extensión partible de $\dot{F}/\dot{F}^2$ si y sólo si π es una retracción. Es decir si existe $(1, x) \in Q(F)$ tal que $(1, x)^2 = (0, 1)$ en $Q(F)$. Como $(1, x)^2 = (0, -1x^2)$, esto ocurre si y sólo si -1 es un cuadrado en F.

Proposición 2.1. *La aplicación* $(\dim_0, \mathrm{d}_\pm)\colon M(F) \to Q(F)$ *es un epimorfismo de semianillos. Así se extiende a un epimorfismo de anillos* $(\dim_0, \mathrm{d}_\pm)\colon \widehat{W}(F) \to Q(F)$ *que se factoriza a través de $W(F)$. Además este epimorfismo induce un isomorfismo f de $W(F)/I^2F$ en $Q(F)$.*

Demostración. Sean q y q' dos formas cuadráticas regulares de dimensiones n y n' respectivamente. Tenemos

$$\begin{aligned}(\dim_0, \mathrm{d}_\pm)(q)(\dim_0, \mathrm{d}_\pm)(q') &= (n, (-1)^{n(n-1)/2}\,\mathrm{d}(q))(n', (-1)^{n'(n'-1)/2}\,\mathrm{d}(q')) \\ &= (n+n', (-1)^{nn'}(-1)^{(n(n-1)+n'(n'-1))/2}\,\mathrm{d}(q)\,\mathrm{d}(q')) \\ &= (n+n', (-1)^{nn'}(-1)^{(n+n')(n+n'-1)/2}\,\mathrm{d}(q \perp q')) \\ &= (\dim_0, \mathrm{d}_\pm)(q \perp q').\end{aligned}$$

Además $(\dim_0, \mathrm{d}_\pm)$ es claramente sobreyectiva ya que $(\dim_0, \mathrm{d}_\pm)(\langle a\rangle) = (1, a)$ y $(\dim_0, \mathrm{d}_\pm)(\langle 1, -a\rangle) = (0, a)$. Por la propiedad universal de $\widehat{W}(F)$ este morfismo se extiende de manera única a un epimorfismo $(\dim_0, \mathrm{d}_\pm)\colon \widehat{W}(F) \to Q(F)$. Dado que $(\dim_0, \mathrm{d}_\pm)(H) = (0, 1)$, este último se factoriza a través de un morfismo $\overline{(\dim_0, \mathrm{d}_\pm)}\colon W(F) \to Q(F)$. Como

$$\overline{(\dim_0, \mathrm{d}_\pm)}(\langle a, b\rangle \otimes \langle c, d\rangle) = \overline{(\dim_0, \mathrm{d}_\pm)}(\langle ac, ad, bc, bd\rangle) = (0, 1),$$

$\overline{(\dim_0, \mathrm{d}_\pm)}$ se anula en I^2F y queda así inducido un epimorfismo f de $W(F)/I^2F$ en $Q(F)$. Veremos ahora que f es un isomorfismo, mediante el tramite de definir la inversa $g\colon Q(F) \to W(F)/I^2F$ de f. Ponemos

$$g(0, a) = \langle 1, -a\rangle \pmod{I^2F} \quad \text{y} \quad g(1, a) = \langle a\rangle \pmod{I^2F}.$$

Dado que

$$\begin{aligned}g((0,a)(0,b)) &= g(0, ab) = \langle 1, -ab\rangle = \langle 1, -a, 1, -b\rangle = g(0,a) + g(0,b) \pmod{I^2F}, \\ g((1,a)(1,b)) &= g(0, -ab) = \langle 1, ab\rangle = \langle a, b\rangle = g(1,a) + g(1,b) \pmod{I^2F}, \\ g((0,a)(1,b)) &= g(1, ab) = \langle ab\rangle = \langle 1, -a, b\rangle = g(0,b) + g(1,b) \pmod{I^2F},\end{aligned}$$

g es un morfismo, que es sobreyectivo ya que $g(1, a) = \langle a\rangle$. La demostración se termina observando que $f \circ g$ es la identidad de $Q(F)$. $\square$

Nota. *La estructura de producto de $Q(F)$, obtenida a través del isomorfismo de $W(F)/I^2F$ en $Q(F)$, está dada por:*

$$(1, a) * (1, b) = (1, ab), \quad (1, a) * (0, b) = (0, b) \quad y \quad (0, a) * (0, b) = (0, 1).$$

Con este producto en $Q(F)$, la aplicación $\pi\colon Q(F) \to \mathbb{Z}/2\mathbb{Z}$ se convierte en un morfismo de anillos. Esto puede ser verificado directamente, pero también es consecuencia de que π se identifica con el morfismo de $W(F)/I^2F$ en $\mathbb{Z}/2\mathbb{Z}$, inducido por $\dim_0$.

Corolario 2.2. *Tenemos*

1) *f induce un isomorfismo de IF/I^2F en $\dot{F}/\dot{F}^2$.*
2) *I^2F consiste de las clases de formas regulares de dimensión par q, que satisfacen $\mathrm{d}(q) = (-1)^{n(n-1)/2}$, donde n es la dimensión de q.*

Proposición 2.3. *La aplicación* $(\dim, \mathrm{d})\colon \widehat{W}(F) \to \mathbb{Z} \oplus \frac{\dot{F}}{\dot{F}^2}$, *induce un isomorfismo* $\widehat{f}$ *de* $\frac{\widehat{W}(F)}{\widehat{I}^2F}$ *en* $\mathbb{Z} \oplus \frac{\dot{F}}{\dot{F}^2}$.

Demostración. Es inmediato que $(\dim, \mathrm{d})$ es sobreyectiva y como

$$(\dim, \mathrm{d})\big((\langle a\rangle - \langle 1\rangle)(\langle b\rangle - \langle 1\rangle\big) = (\dim, \mathrm{d})(\langle 1, ab\rangle - \langle a, b\rangle) = (0, 1),$$

por la Proposición 1.2, $(\dim, \mathrm{d})$ se anula en $\widehat{I}^2F$. Para ver que $\widehat{f}$ es un isomorfismo, construímos una inversa $\widehat{g}\colon \mathbb{Z} \oplus \frac{\dot{F}}{\dot{F}^2} \to \frac{\widehat{W}(F)}{\widehat{I}^2F}$ de $\widehat{f}$, definiendo

$$\widehat{g}(n, a) = (n-1)\langle 1\rangle + \langle a\rangle \qquad (\mathrm{mod}\ \widehat{I}^2F).$$

Como, $\langle 1, ab\rangle \Longleftrightarrow \langle a, b\rangle \ (\mathrm{mod}\ \widehat{I}^2F)$,

$$\begin{aligned}\widehat{g}[(n, a)(m, b)] = \widehat{g}(n+m, ab) &= (n+m-1)\langle 1\rangle + \langle ab\rangle = (n+m-2)\langle 1\rangle + \langle 1, ab\rangle \\ &= (n-1)\langle 1\rangle + \langle a\rangle + (m-1)\langle 1\rangle + \langle b\rangle = \widehat{g}(n, a) + \widehat{g}(m, b),\end{aligned}$$

de donde $\widehat{g}$ es un homomorfismo. Es claro que $\widehat{f} \circ \widehat{g}$ es la identidad. Como $\widehat{g}$ también es sobreyectiva, ya que $\widehat{g}(1, a) = \langle a\rangle$, tenemos que $\widehat{f}$ es un isomorfismo. $\square$

Nota. La estructura de producto de $\mathbb{Z} \oplus \frac{\dot{F}}{\dot{F}^2}$, obtenida a través de $\widehat{f}$ está dada por $(n, a) * (m, b) = (nm, a^m b^n)$.

Corolario 2.4. *Se satisfacen*

1) La restricción de $\widehat{f}$ *define un isomorfismo de* $\frac{\widehat{I}F}{\widehat{I}^2F}$ *en* $\frac{\dot{F}}{\dot{F}^2}$.

2) $\widehat{I}^2F$ *consiste de los elementos de* $\widehat{I}F$ *que tienen determinante igual a* 1.

Nota. Hay un diagrama conmutativo

$$\begin{array}{ccc} \frac{\widehat{W}(F)}{\widehat{I}^2F} & \xrightarrow{\ \widehat{f}\ } & \mathbb{Z} \oplus \frac{\dot{F}}{\dot{F}^2} \\ \big\downarrow \pi & & \big\downarrow \theta \\ \frac{W(F)}{I^2F} & \xrightarrow{\ \widehat{f}\ } & Q(F), \end{array}$$

donde π está inducida por la proyección canónica de $\widehat{W}(F)$ en $W(F)$ y θ está definida por $\theta(n, a) = (\overline{n}, (-1)^{n(n-1)/2}a)$, donde $\overline{n}$ denota a la clase de n en $\mathbb{Z}/2\mathbb{Z}$.

Corolario 2.5. *Las siguientes afirmaciones son equivalentes:*

1) $\widehat{W}(F)$ *es un grupo finitamente generado.*

2) $\widehat{W}(F)$ *es noetheriano.*

3) $W(F)$ *es noetheriano.*

4) IF *es un ideal finitamente generado de* $W(F)$.

5) $\frac{\dot{F}}{\dot{F}^2}$ *es un grupo finito.*

Demostración. 1) $\Longrightarrow$ 2), 2) $\Longrightarrow$ 3) y 3) $\Longrightarrow$ 4) son triviales.

4) $\Longrightarrow$ 5) $\frac{IF}{I^2F}$ es un $\frac{W(F)}{IF}$-módulo finitamente generado. Así, como $\frac{W(F)}{IF} \simeq \frac{\mathbb{Z}}{2\mathbb{Z}}$, el conjunto $\frac{IF}{I^2F}$ es finito. Se sigue del Corolario 2.4 que $\frac{\dot{F}}{\dot{F}^2}$ es finito.

5) $\Longrightarrow$ 1) Por el teorema de diagonalización $\widehat{W}(F)$ está generado como grupo por $\langle a\rangle$ con $a \in \frac{\dot{F}}{\dot{F}^2}$. Así si $\frac{\dot{F}}{\dot{F}^2}$ es finito, entonces $\widehat{W}(F)$ es un grupo finitamente generado. $\square$

3. Algunos cálculos elementales

Decimos que un cuerpo F es cuadráticamente cerrado si contiene a las raíces cuadradas de cada uno de sus elementos.

Proposición 3.1. *Son equivalentes:*

1) F *es cuadráticamente cerrado.*

2) $\dim\colon \widehat{W}(F) \to \mathbb{Z}$ *es un isomorfismo de anillos.*

3) $\dim_0\colon W(F) \to \frac{\mathbb{Z}}{2\mathbb{Z}}$ *es un isomorfismo de anillos.*

Demostración. 1) $\implies$ 2) Si F es cuadráticamente cerrado, entonces $\langle a\rangle \simeq \langle 1\rangle$ para cada $a \in \dot{F}$. Así, cada forma q regular es isomorfa a $\dim(q)\langle 1\rangle$. Ahora es claro que dim es un isomorfismo de anillos.

2) $\implies$ 3) Se lo deduce inmediatamente de que $\dim(\widehat{W}(F)H) = 2\mathbb{Z}$.

3) $\implies$ 1) Sea $a \in \dot{F}$. Como $\dim(\langle a\rangle) = \dim(\langle 1\rangle)$, por la Proposición 1.4 $\langle a\rangle \simeq \langle 1\rangle$. Así, existe $x \in F$ tal que $a = 1.x^2$. $\square$

Proposición 3.2. *Son equivalentes:*

1) En F *toda suma de cuadrados es un cuadrado y* $\frac{\dot{F}}{\dot{F}^2} \simeq \{1, -1\}$.

2) En F *toda suma de cuadrados es un cuadrado y* $\frac{\dot{F}}{\dot{F}^2}$ *tiene dos elementos.*

3) Para cada $n \in \mathbb{N}$ *la forma* $n\langle 1\rangle$ *es anisotrópica y* $\frac{\dot{F}}{\dot{F}^2}$ *tiene dos elementos.*

4) Para cada $n \in \mathbb{N}$ *la forma* $n\langle 1\rangle$ *es anisotrópica y* $\frac{\dot{F}}{\dot{F}^2} \simeq \{1, -1\}$.

5) $W(F)$ *es isomorfo a* $\mathbb{Z}$.

6) Salvo isometría, $n\langle 1\rangle$ *y* $n\langle -1\rangle$ *son las únicas dos formas anisotrópicas de dimensión* n*, para cada* $n \in \mathbb{N}$.

7) Existen exactamente dos clases de isometría de formas anisotrópicas de dimensión 1 *y al menos una de dimensión* n*, para cada* $n \in \mathbb{N}$.

8) $2\langle 1\rangle$ *es anisotrópica y* $\widehat{W}(F)$ *es isomorfo a* $\mathbb{Z}[\mathbb{Z}/2\mathbb{Z}]$.

Demostración. 1) $\implies$ 2) Es trivial.

2) $\implies$ 3) Supongamos que $n\langle 1\rangle$ no es anisotrópica. Entonces $n\langle 1\rangle$ contiene un espacio hiperbólico y por lo tanto es universal. En consecuencia, todo elemento de $\dot{F}$ es una suma de cuadrados. Por hipótesis esto implica que todo elemento de $\dot{F}$ es un cuadrado, lo que contradice que $\frac{\dot{F}}{\dot{F}^2}$ tiene dos elementos.

3) $\implies$ 4) Si -1 fuera un cuadrado, entonces $2\langle 1\rangle$ sería isométrica a $\langle 1, -1\rangle$ y, por lo tanto, no sería anisotrópica.

4) $\implies$ 5) Sea q una forma regular de dimensión n. Como $\frac{\dot{F}}{\dot{F}^2} \simeq \{1, -1\}$, hay una isometría entre q y una suma de $\langle 1\rangle$'s y $\langle -1\rangle$'s. Pero, si q es anisotrópica debe ser $q \simeq n\langle 1\rangle$ o $q \simeq n\langle -1\rangle$. Esto muestra que $\langle 1\rangle$ genera $W(F)$. Como por hipótesis, $\langle 1\rangle$ es un elemento sin torsión del grupo $W(F)$ tenemos que $W(F)$ es isomorfo a $\mathbb{Z}$.

5) $\implies$ 1) Sea $a \in \dot{F}$. Dado que $\langle a\rangle$ es anisotrópica, existe $n \geq 0$ tal que $\langle a\rangle \simeq n\langle 1\rangle$ o $\langle a\rangle \simeq n\langle -1\rangle$ (porque $\langle 1\rangle$ es el neutro multiplicativo de $W(F)$ y $\langle -1\rangle = -\langle 1\rangle$ en $W(F)$). Por razones de dimensión debe ser $n = 1$. Así, $\langle a\rangle \simeq \langle 1\rangle$ o $\langle a\rangle \simeq \langle -1\rangle$. En el primer caso existe $x \in F$ tal que $a = x^2$ y en el segundo existe $x \in F$ tal que $-a = x^2$. Dado que -1 no es un cuadrado (pues de lo contrario

tendríamos que $-\langle 1\rangle = \langle -1\rangle = \langle 1\rangle$ en $W(F)$ y $W(F)$ no sería isomorfo a $\mathbb{Z}$), resulta que $\frac{\dot{F}}{\dot{F}^2} \simeq \{1,-1\}$. Veamos que una suma de cuadrados es un cuadrado. Sea $c = \sum_{i=1}^n x_i^2$ un elemento no nulo de F. Por lo que vimos $\langle c\rangle \simeq \langle 1\rangle$ o $\langle c\rangle \simeq \langle -1\rangle$. Si $\langle c\rangle \simeq \langle -1\rangle$, entonces existe $y \in \dot{F}$ tal que $-1 = cy^2 = \sum_{i=1}^n (x_i y)^2$. De esto se obtiene que $(n+1)\langle 1\rangle$ es isotrópica, de donde $\langle 1\rangle$ no es un elemento sin torsión del grupo $W(F)$. Como esto contradice que $W(F) \simeq \mathbb{Z}$, resulta que $\langle c\rangle \simeq \langle 1\rangle$, lo que implica que c es un cuadrado.

5) $\implies$ 6) Es inmediato que $n\langle 1\rangle$ y $n\langle -1\rangle$ son las dos únicas formas anisotrópicas de dimensión n.

6) $\implies$ 7) Es trivial.

7) $\implies$ 5) Por hipótesis existen dos formas regulares $\langle a\rangle$ y $\langle b\rangle$ no isométricas de dimensión 1, tales que cualquier otra forma regular de dimensión 1 es isométrica a una de ellas. Es claro que podemos suponer que $a = 1$. Veamos que $\langle -1\rangle$ es isométrica a $\langle b\rangle$. Supongamos que no es así. Entonces $\langle -1\rangle \simeq \langle 1\rangle$. Esto implica que $\langle b\rangle \simeq \langle -b\rangle$, de donde una forma regular de dimensión 2 es necesariamente isométrica a $\langle 1,-1\rangle$, $\langle b,-b\rangle$ o $\langle 1,b\rangle$. Como las dos primeras son isotrópicas, las únicas posibles formas anisotrópicas de dimensión 3 son $\langle 1,1,b\rangle$ y $\langle 1,b,b\rangle$ y como ninguna de estas es isotrópica, tenemos una contradicción. Así $\langle b\rangle \simeq \langle -1\rangle$, de donde toda forma anisotrópica de dimensión n es isométrica a $n\langle 1\rangle$ o a $n\langle -1\rangle$. En particular $\langle 1\rangle$ genera $W(F)$ como grupo. Ahora, dado que en cada dimensión hay al menos una formas anisotrópicas, en $W(F)$ debe ser $n\langle 1\rangle \neq 0$ para todo $n \geq 1$ (ya que $\langle -1\rangle$ es el opuesto aditivo de $\langle 1\rangle$ en $W(F)$), lo que muestra que $W(F)$ es isomorfo a $\mathbb{Z}$.

5) $\implies$ 8) Es claro que $\langle 1\rangle$ y $\langle -1\rangle$ generan $\widehat{W}(F)$. Veamos que son independientes. Supongamos que $a\langle 1\rangle + b\langle -1\rangle = 0$ en $\widehat{W}(F)$. Pasando a $W(F)$ se obtiene que $a = b$. Pero entonces $0 = a\langle 1\rangle + b\langle -1\rangle = a\langle 1,-1\rangle = aH$ en $\widehat{W}(F)$, lo que implica que $a = 0$. Finalmente como

$$(a\langle 1\rangle + b\langle -1\rangle)(c\langle 1\rangle + d\langle -1\rangle) = (ac+bd)\langle 1\rangle + (ad+bc)\langle -1\rangle,$$

resulta que $\widehat{W}(F)$ es isomorfo a $\mathbb{Z}[\mathbb{Z}/2\mathbb{Z}]$.

8) $\implies$ 5) Sea $\theta\colon \widehat{W}(F) \to \mathbb{Z}[\mathbb{Z}/2\mathbb{Z}]$ un isomorfismo. Escribamos $\mathbb{Z}/2\mathbb{Z}$ en forma multiplicativa $\mathbb{Z}/2\mathbb{Z} = \{g,1\}$ y pongamos $\theta(\langle -1\rangle) = \alpha + \beta g$. Como $\langle -1\rangle^2 = \langle 1\rangle$,

$$1 = (\alpha+\beta g)^2 = \alpha^2 + \beta^2 + 2\alpha\beta g,$$

de donde $\alpha + \beta g \in \{1,-1,g,-g\}$. Si $\theta(\langle -1\rangle) = 1$, entonces $\langle -1\rangle \simeq \langle 1\rangle$, lo que implica que $2\langle 1\rangle \simeq \langle 1,-1\rangle$ no es anisotrópica y, si $\theta(\langle -1\rangle) = -1$, entonces $\theta(\langle 1,-1\rangle) = \theta(\langle 1\rangle) + \theta(\langle -1\rangle) = 0$, lo que implica que $\langle 1,-1\rangle = 0$ en $\widehat{W}(F)$, lo que es falso. Así, $\theta(\langle -1\rangle) = \pm g$. Es fácil ver ahora que $W(F) = \frac{\widehat{W}(F)}{\langle H\rangle} \simeq \frac{\mathbb{Z}[\mathbb{Z}/2\mathbb{Z}]}{\langle \theta(H)\rangle} \simeq \mathbb{Z}$. $\square$

Nota 3.3. Supongamos que estamos en la situación de la Proposición 3.2 y que (V,q) es una forma cuadrática regular de dimensión n. La cantidad de 1's y -1's que aparecen en una diagonalización de (V,q) formada por 1's y -1's es independiente de la diagonalización. En efecto, escribamos $(V,q) = (V_a,q_a) \perp (V_h,q_h)$, donde (V_a,q_a) es anisótropica y (V_h,q_h) es hiperbólica. El mínimo entre la cantidad n_+ de 1's y n_- de -1's que aparecen es el índice de Witt de (V,q) y como $q_a = (n_+ - n_-)\langle 1\rangle$

en $W(F)$ y $W(F) \simeq \mathbb{Z}$, este número $n_+ - n_-$ también está determinado por (V, q). A $n_+ - n_-$ se lo denomina la signatura de (V, q). Por otro lado, como $n_+ + n_- = n$, la signatura de (V, q), determina a n_+ y a n_-. Así, la clase de isometría a la que pertenece una forma regular está determinada por su dimensión y su signatura. Esta propiedad se denomina Ley de Sylvester. Notese que la signatura es un morfismo de semigrupos de $M(F)$ en $\mathbb{Z}$ que se extiende a un epimorfismo $\widehat{W}(F) \to \mathbb{Z}$. El núcleo de este epimorfismo es $\mathbb{Z}H$. Así, el isomorfismo de $W(F)$ en $\mathbb{Z}$ está inducido por la signatura.

Nota. Sea $\mathbb{F}_q$ un cuerpo finito de q elementos con q impar y sea $x \in \dot{\mathbb{F}}_q$ un generador de $\dot{\mathbb{F}}_q$. Es claro que x^m con $0 \leq m < q$ es un cuadrado si y sólo si m es par. Así, $\frac{\dot{F}_q}{\dot{F}_q^2}$ tiene dos elementos. Nosotros podemos denotar estas clases por 1 y s. Como $x^{(q-1)/2}$ es distinto de 1 y elevado al cuadrado da 1, debe ser $x^{(q-1)/2} = -1$. Así, -1 es un cuadrado si y sólo si $(q-1)/2$ es par o, en otras palabras, si y sólo si $q \equiv 1 \pmod 4$. En consecuencia cuando $q \equiv 3 \pmod 4$, podemos elegir $s = -1$.

Proposición 3.4. *Si $F = \mathbb{F}_q$ es un cuerpo finito, entonces toda forma regular binaria es universal.*

Demostración. Escribamos $\frac{\dot{F}}{\dot{F}^2} = \{1, s\}$ y veamos primero que s se puede tomar como una suma de dos cuadrados (como 1 y s son la únicas clases de cuadrados, esto es lo mismo que decir que $\langle 1, 1\rangle$ es universal). Si -1 es un cuadrado o, en otras palabras, $q \equiv 1 \pmod 4$, entonces $\langle 1, 1\rangle \simeq \langle 1, -1\rangle$ es hiperbólico y por lo tanto universal. Supongamos ahora que -1 no es un cuadrado. Consideremos los conjuntos $\dot{F}^2$ y $1 + \dot{F}^2$ de F. Es claro que estos conjuntos tienen el mismo cardinal $(q-1)/2$. Dado que $1 \in \dot{F}^2$ y $1 \notin 1 + \dot{F}^2$ estos conjuntos son distintos. En consecuencia, existe un elemento de la forma $1 + z^2$ que no está en $\dot{F}^2$. Como $-1 \notin \dot{F}^2$, tenemos que $1 + z^2 \neq 0$ y así, podemos tomar $s = 1 + z^2$. Veamos ahora que toda forma regular binaria es universal. Como 1 y s son las únicas clases de cuadrados, hay a lo sumo tres formas binarias no equivalentes $\langle 1, 1\rangle$, $\langle 1, s\rangle$ y $\langle s, s\rangle$. Ya vimos que la primera es universal. Es claro que la segunda representa a 1 y a s y por lo tanto también es universal. Veamos que también lo es la última. Dado $z \in \dot{F}$, elijamos x_1 y x_2 tales que $s^{-1}z = x_1^2 + x_2^2$. Entonces $sx_1^2 + sx_2^2 = s(x_1^2 + x_2^2) = ss^{-1}z = z$. $\square$

Teorema 3.5. *Son equivalentes:*

1) *Toda forma regular binaria es universal.*
2) *Toda forma regular binaria representa al* 1.
3) *Dos formas regulares son isométricas si y sólo si tienen la misma dimensión y el mismo determinante.*
4) *Dos formas anisotrópicas son isométricas si y sólo si tienen la misma dimensión y el mismo determinante.*
5) $\widehat{I}^2 F = 0$.
6) $I^2 F = 0$.
7) $\mathrm{d}\colon \widehat{I}F \to \frac{\dot{F}}{\dot{F}^2}$ *es un isomorfismo.*
8) $\mathrm{d}_\pm\colon IF \to \frac{\dot{F}}{\dot{F}^2}$ *es un isomorfismo.*

9) La aplicación $\widehat{f}\colon \widehat{W}(F) \to \mathbb{Z} \oplus \frac{\dot{F}}{\dot{F}^2}$ *que envía* q *en* $(\dim(q), \mathrm{d}(q))$ *es un isomorfismo de grupos.*

10) La aplicación $f\colon W(F) \to Q(F)$ *que envía* q *en* $(\dim_0(q), \mathrm{d}_\pm(q))$ *es un isomorfismo de grupos.*

Demostración. 1) $\implies$ 2) Es trivial.

2) $\implies$ 3) Sea $\langle a_1, a_2\rangle$ una forma regular binaria. Puesto que $\langle a_1, a_2\rangle$ representa al 1, tenemos que $\langle a_1, a_2\rangle \simeq \langle 1, a_1a_2\rangle$. Por inducción, una forma regular arbitraria $q = \langle a_1, \ldots, a_n\rangle$ es isomorfa a $\langle 1, \ldots, 1, \mathrm{d}(q)\rangle$.

3) $\implies$ 1) Sea $\langle a_1, a_2\rangle$ una forma regular binaria y sea $b \in \dot{F}$. Dado que $\langle a_1, a_2\rangle$ y $\langle b, ba_1a_2\rangle$ tienen la misma dimensión y el mismo determinante, son isomorfas. El resultado se deduce ahora inmediatamente de que $\langle b, ba_1a_2\rangle$ representa a b.

3) $\iff$ 9) Es inmediato.

5) $\iff$ 9) Por la Proposición 2.3.

5) $\iff$ 7) Por el item 1) del Corolario 2.4.

4) $\implies$ 10) Es inmediato.

6) $\implies$ 10) Por la Proposición 2.1.

6) $\iff$ 8) Por el item 1) del Corolario 2.2.

5) $\iff$ 6) Por que la proyección canónica de $\widehat{W}(F)$ en $W(F)$ induce un isomorfismo de $\widehat{I}F$ en IF y, por lo tanto, también de $\widehat{I}^2F$ en I^2F. $\square$

Corolario 3.6. *Sea* $F = \mathbb{F}_q$ *con* q *impar. Se satisfacen:*

1) Si $q \equiv 1 \pmod 4$, *entonces* $W(F)$ *es isomorfo a* $\frac{\mathbb{Z}}{2\mathbb{Z}}[\dot{F}/\dot{F}^2]$.

2) Si $q \equiv 3 \pmod 4$, *entonces* $W(F)$ *es isomorfo a* $\frac{\mathbb{Z}}{4\mathbb{Z}}$.

Demostración. 1) En lo que sigue utilizaremos la nota acerca del producto de $Q(F)$ que sigue a la Proposición 2.1. Supongamos que $q \equiv 1 \pmod 4$ o, en otras palabras que -1 es un cuadrado. Entonces la sucesión

$$1 \to \frac{\dot{F}}{\dot{F}^2} \to Q(F) \to \frac{\mathbb{Z}}{2\mathbb{Z}} \to 0$$

se parte. La sección de $\frac{\mathbb{Z}}{2\mathbb{Z}}$ en $Q(F)$ identifica 0 con $(0,1)$ y 1 con $(1,1)$ (que son los neutros aditivo y multiplicativo de $Q(F)$ respectivamente). Sea $\dot{F}/\dot{F}^2 = \{1, s\}$ y escribamos $e = (1,1)$ y $g = (1,s)$. Dado que cada elemento de $Q(F)$ se escribe de manera única como una combinación lineal de e y g con escalares en $\{(0,1),(1,1)\}$ y que $g^2 = e = e^2$ y $eg = g = ge$, resulta que $Q(F)$ se identifica con $\frac{\mathbb{Z}}{2\mathbb{Z}}[\dot{F}/\dot{F}^2]$ (ya que $\frac{\dot{F}}{\dot{F}^2}$ tiene 2 elementos y es por lo tanto isomorfo al grupo $\{e, g\}$).

2) Como en este caso la sucesión mencionada en la demostración del item 1) no se parte y como $\frac{\dot{F}}{\dot{F}^2}$ es isomorfo a $\frac{\mathbb{Z}}{2\mathbb{Z}}$, resulta que $Q(F)$ es isomorfo a $\frac{\mathbb{Z}}{4\mathbb{Z}}$. Como -1 no es un cuadrado, podemos tomar $\frac{\dot{F}}{\dot{F}^2} = \{1, -1\}$. Un cálculo directo muestra que $(1,1)$ genera a $Q(F)$ como grupo aditivo. Usando que $(1,1)$ es el neutro multiplicativo de $Q(F)$ (ver la nota acerca de la estructura de producto de $Q(F)$) se comprueba fácilmente que la aplicación de $\frac{\mathbb{Z}}{4\mathbb{Z}}$ en $Q(F)$ que envía i en $i(1,1)$ $(0 \le i \le 3)$ es un isomorfismo de anillos. $\square$

Ejercicios

Ejercicio 1. *Pruebe que si* $\langle a_1, \ldots, a_n\rangle = \langle b_1, \ldots, b_n\rangle$*, entonces*

$$(\langle a_1\rangle - 1)\ldots(\langle a_n\rangle - 1) = (\langle b_1\rangle - 1)\ldots(\langle b_n\rangle - 1)$$

en $\widehat{W}(F)$*.*

Ejercicio 2. *Pruebe que* IF *es el único ideal maximal de* $W(F)$ *que contiene al* 2*.*

Ejercicio 3. *Diagonalize la siguentes formas sobre* $\mathbb{R}$ *y calcule sus signaturas.*

1) $q_1 = x^2 + y^2 + z^2 + xy + xz + yz$*,*

2) $q_2 = y^2 + 2z^2 + 4xy + 2xz$*,*

3) $q_3 = x_1x_2 + x_2x_3 + \cdots + x_{n-1}x_n$*.*

Ejercicio 4. *Pruebe que* $W(F)$ *es finito si y sólo si* -1 *es una suma de cuadrados en* F *y* $\dot{F}/\dot{F}^2$ *es finito.*

Ejercicios del Capítulo 1

Ejercicio 1. *Se lo deduce inmediatamente de las definiciones.*

Ejercicio 2. *Denotemos con e_{ij} $(1 \leq i, j \leq n)$ a la matriz que tiene un 1 en la coordenada (i, j) y 0 en las demás. Los conjuntos*

$$\{e_{11}, \ldots, e_{nn}, \frac{e_{12}+e_{21}}{2}, \frac{e_{12}-e_{21}}{2}, \ldots, \frac{e_{n-1,n}+e_{n,n-1}}{2}, \frac{e_{n-1,n}-e_{n,n-1}}{2}\},$$
$$\{e_{11}, e_{12}, \ldots, e_{1n}, e_{21}, e_{22}, \ldots, e_{2n}, \ldots, e_{n1}, e_{n2}, \ldots, e_{nn}\},$$

son bases ortogonales de $M_n(F)$ para la formas bilineales $B(X,Y) = \operatorname{tr}(XY)$ y $B'(X,Y) = \operatorname{tr}(XY^t)$ respectivamente. En la primera base la forma cuadrática queda $n\langle 1\rangle \perp \frac{n(n-1)}{2} H$ y en la segunda $n^2\langle 1\rangle$.

Ejercicio 3. *Es claro que B_U es bilineal. Dado que $U^t = U$, tenemos*

$$\begin{aligned}\operatorname{tr}\big(XUY^tU^{-1}\big) &= \operatorname{tr}\big((XUY^tU^{-1})^t\big) = \operatorname{tr}\big((U^{-1})^tYU^tX^t\big)\\ &= \operatorname{tr}\big(U^{-1}YUX^t\big) = \operatorname{tr}\big(YUX^tU^{-1}\big),\end{aligned}$$

de donde B_U es simétrica. Finalmente $\operatorname{tr}\big(XUY^tU^{-1}\big) = 0$ para todo X equivale a $UY^tU^{-1} = 0$, lo que a su vez equivale a $Y = 0$. Cuando $n = 2$ y $U = \left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right)$, tenemos

$$\begin{aligned}B_U(X,Y) &= \operatorname{tr}\left[\begin{pmatrix}x_{11} & x_{12}\\ x_{21} & x_{22}\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix}y_{11} & y_{21}\\ y_{12} & y_{22}\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\right]\\ &= \operatorname{tr}\left[\begin{pmatrix}x_{11} & -x_{12}\\ x_{21} & -x_{22}\end{pmatrix}\begin{pmatrix}y_{11} & -y_{21}\\ y_{12} & -y_{22}\end{pmatrix}\right]\\ &= x_{11}y_{11} - x_{12}y_{12} - x_{21}y_{21} + x_{22}y_{22}.\end{aligned}$$

Una base ortogonal de este espacio es $e_{11}, e_{12}, e_{21}, e_{22}$. En esta base la forma cuadrática es $2H$.

Ejercicio 4. *Es claro que $B(x,y) = \operatorname{tr}_{K/F}(xy)$ es bilineal y simétrica. Dado que K/F es separable la traza $\operatorname{tr}_{K/F}$ es no nula. Sea $z \in K$ tal que $\operatorname{tr}_{K/F}(z) \neq 0$. Si $x \neq 0$, entonces $B(x, x^{-1}z) = \operatorname{tr}_{K/F}(z) \neq 0$. Esto muestra que B es regular. Una base diagonal para $F = Q$ y $K = Q(\sqrt[3]{2})$ es $\{1, \sqrt[3]{2} + \sqrt[3]{4}, \sqrt[3]{2} - \sqrt[3]{4}\}$.*

Ejercicio 5. *Supongamos que $f \perp \langle a\rangle$ representa $-b$. Entonces existen $\vec{x} \in F^{\dim(f)}$ e $y \in F$, tales que $f(\vec{x}) + ay^2 = -b$. Si $y = 0$, entonces $f \perp \langle b\rangle$ es isotrópica y por lo tanto universal (item 3) del Teorema 3.5). En particular $f \perp \langle b\rangle$ representa $-a$. Si $y \neq 0$, entonces $f(y^{-1} \cdot \vec{x}) + b\left(\frac{1}{y}\right)^2 = -a$, de donde $f \perp \langle b\rangle$ también en este caso representa $-a$. Por simetría, si $f \perp \langle b\rangle$ representa $-a$, entonces $f \perp \langle a\rangle$ representa $-b$.*

Ejercicio 6. *Los vectores $(a, b, 1, 0)$ y $(-b, a, 0, 1)$ son isotrópicos y ortogonales. Así generan un subespacio totalmente isotrópico de dimensión 2 de F^4. Por el item 1) del Teorema 3.5, $\langle 1, 1, -c, -c\rangle$ es hiperbólico.*

Ejercicio 7. *Por el item 2) del Teorema 3.5, existe una base en la que f tiene la forma $x_1^2 - x_2^2 + a_3x_3^2 + \cdots + a_nx_n^2$. Sea $c = -(a_3 + \cdots + a_n)$. Si $c \neq \pm 1$, entonces $\left(\frac{c+1}{2}, \frac{c-1}{2}, 1, \ldots, 1\right)$ es un vector isotrópico con coordenadas no nulas; si $c = 1$, entonces $\left(\frac{5}{4}, \frac{3}{4}, 1, \ldots, 1\right)$ es un vector isotrópico con coordenadas no nulas; y si $c = -1$, entonces $\left(\frac{3}{4}, \frac{5}{4}, 1, \ldots, 1\right)$ es un vector isotrópico con coordenadas no nulas.*

Ejercicio 8. *Vamos a probar que $\natural \frac{\dot{F}}{\dot{F}^2} \leq \prod_{i=1}^n \natural \frac{\dot{F}_i}{\dot{F}_i^2}$. Es claro que podemos suponer que $n = 2$. Veamos primero que $(\dot{F}_1 \cap \dot{F}_2)^2 = \dot{F}^2 \cap \dot{F}^2$. La inclusión $(\dot{F}_1 \cap \dot{F}_2)^2 \subseteq \dot{F}^2 \cap \dot{F}^2$ es obvia. Si $x \in \dot{F}^2 \cap \dot{F}^2$, existen y_1 e y_2 en $\dot{F}_1$ y $\dot{F}_2$ respectivamente, tales que $x = y_1^2 = y_2^2$. Entonces $y_1 = \pm y_2$, de donde $y_1 \in \dot{F}_1 \cap \dot{F}_2$. Esto muestra que $\dot{F}^2 \cap \dot{F}^2 \subseteq (\dot{F}_1 \cap \dot{F}_2)^2$. Usando ahora las sucesiones exactas*

$$1 \to \frac{\dot{F}_1^2 \cap \dot{F}_2}{\dot{F}_1^2 \cap \dot{F}_2^2} \to \frac{\dot{F}_1 \cap \dot{F}_2}{\dot{F}_1^2 \cap \dot{F}_2^2} \to \frac{\dot{F}_1 \cap \dot{F}_2}{\dot{F}_1^2 \cap \dot{F}_2} \to 1,$$

$$1 \to \frac{\dot{F}_1^2 \cap \dot{F}_2}{\dot{F}_1^2 \cap \dot{F}_2^2} \to \frac{\dot{F}_2}{\dot{F}_2^2} \quad y \quad 1 \to \frac{\dot{F}_1 \cap \dot{F}_2}{\dot{F}_1^2 \cap \dot{F}_2} \to \frac{\dot{F}_1}{\dot{F}_1^2},$$

se deduce fácilmente que $\natural \frac{\dot{F}_1 \cap \dot{F}_2}{(\dot{F}_1 \cap \dot{F}_2)^2} = \natural \frac{\dot{F}_1 \cap \dot{F}_2}{\dot{F}_1^2 \cap \dot{F}_2^2} \leq \natural \frac{\dot{F}_1}{\dot{F}_1^2} \natural \frac{\dot{F}_2}{\dot{F}_2^2}$.

Ejercicio 9. *Sea p_i $(i \in I)$ un conjunto de representantes de los primos de A. Un elemento de $\dot{F}$ se escribe de manera única como $u \prod_{i \in I} p_i^{\alpha_i}$, con todos los $\alpha_i \in \mathbb{Z}$ nulos, salvo un número finito. Además este elemento está en $\dot{F}^2$ si y sólo si $u \in U^2$ y los α_i's son pares. Así dos elementos $u \prod_{i \in I} p_i^{\alpha_i}$ y $v \prod_{i \in I} p_i^{\beta_i}$ son iguales módulo $\dot{F}^2$ si y sólo si $u \equiv v \pmod{U^2}$ y $\alpha_i \equiv \beta_i \pmod 2$ $(i \in I)$. El resultado se deduce inmediatamente de estos hechos. Supongamos ahora que $A = \mathbb{Z}$ y que $\langle p_1, \ldots, p_n \rangle \simeq \langle q_1, \ldots, q_n \rangle$ con $\{p_1, \ldots, p_n\}$ y $\{q_1, \ldots, q_n\}$ primos positivos distintos. Supongamos que $p_1 < \cdots < p_n$ y $q_1 < \cdots < q_n$. Entonces*

$$p_1 \ldots p_n = \mathrm{d}(\langle p_1, \ldots, p_n \rangle) = \mathrm{d}(\langle q_1, \ldots, q_n \rangle) = q_1 \ldots q_n, \qquad (\mathrm{mod}\ \dot{F}^2),$$

de donde $p_i = q_i$ para todo $1 \leq i \leq n$.

Ejercicio 10. *1) $\implies$ 2) Sea $f = a_1X_1^2 + \cdots + a_{2n}X_{2n}^2$ una forma de dimensión $2n$ y cuyo determinante es -1. Por la Proposici'on 3.2, podemos suponer que n es mayor que 2. Supongamos que el resultado vale para formas de dimensión menor que $2n$. Entonces existen $(x_1, \ldots, x_{2n-2})$ e $(y_{2n-2}, y_{2n-1}, y_{2n}, y_{2n+1})$ no nulos, tales que*

$$a_1x_1^2 + \cdots + a_{2n-3}x_{2n-3}^2 + a_{2n-2}a_{2n-1}a_{2n}x_{2n-2}^2 = 0$$

y

$$a_{2n-2}y_{2n-2}^2 + a_{2n-1}y_{2n-1}^2 + a_{2n}y_{2n}^2 - a_{2n-2}a_{2n-1}a_{2n}y_{2n+1}^2 = 0.$$

Si $x_{2n-2} = 0$ el vector $(x_1, \ldots, x_{2n-3}, 0, 0, 0)$ es un vector isotrópico de f y si $y_{2n+1} = 0$, el vector $(0, \ldots, 0, y_{2n-2}, y_{2n-1}, y_{2n})$ es un vector isotrópico de f. Podemos suponer entonces que $x_{2n-2} \neq 0 \neq y_{2n+1}$. Sea $z_{2n-i} = \frac{x_{2n-2}y_{2n-i}}{y_{2n+1}}$ $(i = 0, 1, 2)$. Entonces, de la segunda de las ecuaciones de arriba obtenemos,

$$a_{2n-2}a_{2n-1}a_{2n}x_{2n-2}^2 = a_{2n-2}z_{2n-2}^2 + a_{2n-1}z_{2n-1}^2 + a_{2n}z_{2n}^2.$$

Observese que esto muestra en particular que los z_{2n-i} ($i = 0, 1, 2$) no son todos nulos. Reemplazando este resultado en la primera de las ecuaciones se deduce que $(x_1, \ldots, x_{2n-3}, z_{2n-2}, z_{2n-1}, z_{2n})$ es un vector isotrópico de f.

2) $\implies$ 1) Es trivial.

1) $\implies$ 3) Sea $a_1X_1^2 + a_2X_2^2 + a_3X_3^2$ una forma cuadŕatica regular de dimensión 3. Por el item 1) existe $(x_1, x_2, x_3, x_4) \in F^4$ no nulo tal que $a_1x_1^2 + a_2x_2^2 + a_3x_3^2 - a_1a_2a_3x_4^2 = 0$. Si $x_4 \neq 0$, entonces $a_1a_2a_3 = a_1\left(\frac{x_1}{x_4}\right)^2 + a_2\left(\frac{x_2}{x_4}\right)^2 + a_3\left(\frac{x_3}{x_4}\right)^2$. Si, por el contrario $x_4 = 0$, entonces $a_1X_1^2 + a_2X_2^2 + a_3X_3^2$ es isotrópica y por lo tanto universal (item 3) del Teorema 3.5), de donde también representa a $a_1a_2a_3$.

3) $\implies$ 1) Sea $a_1X_1^2+a_2X_2^2+a_3X_3^2+a_4X^4$ una forma cuadŕatica con determinante -1 (es decir tal que $a_1a_2a_3a_4 = -z^2$ para algún $z \in \dot{F}$). Por hipótesis, existe $(x_1, x_2, x_3) \in F^3$ tal que $a_1x_1^2 + a_2x_2^2 + a_3x_3^2 = a_1a_2a_3$. Así, $a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4\left(\frac{z}{a_4}\right)^2 = 0$, de donde $a_1X_1^2 + a_2X_2^2 + a_3X_3^2 + a_4X_4^2$ es isotrópica.

2) $\implies$ 4) Es similar a 1) $\implies$ 3).

4) $\implies$ 2) Es similar a 3) $\implies$ 1).

Ejercicio 11. *Suponemos que U_1 y U_2 son regulares. Sean σ una isometría de U_1 en U_2 y W_1 y W_2 los complementos ortogonales de U_1 y U_2 en V, respectivamente, de modo que $V = U_1 \perp W_1$ y $V = U_2 \perp W_2$. Consideremos la isometría de $U_2 \perp W_2$ en $U_1 \perp W_2$, que envía (u, w) en $(\sigma^{-1}(u), w)$. Entonces $U_1 \perp W_1$ es isométrico a $U_1 \perp W_2$. Así, por el teorema de cancelación de Witt, hay una isometría $\tau\colon W_1 \to W_2$. Es inmediato que el morfismo $\sigma'\colon U_1 \perp W_1 \to U_2 \perp W_2$, definido por $\sigma'(u, w) = (\sigma(u), \tau(w))$ es una isometría de V en V que extiende a σ.*

Ejercicio 12. *Suponemos que U es regular. Por el teorema de descomposición de Witt, podemos escribir $U = U_h \perp U_a$ y $U^\perp = V_t \perp V_h \perp V_a$, con V_t totalmente isotrópico, U_h y V_h hiperbólicos y U_a y V_a anisotrópicos. Así, por el item 1) de la Proposición 1.3,*

$$mH = U \perp U^\perp = V_t \perp (U_h \perp V_h) \perp (U_a \perp V_a),$$

de donde $0 = \mathrm{rad}(mH) = V_t$. Además, por el teorema de cancelación de Witt,

$$(m - l_1 - l_2)H = U_a \perp V_a \qquad \text{donde } l_1 = \frac{\dim(U_h)}{2} \text{ y } l_2 = \frac{\dim(V_h)}{2}.$$

Puesto que $\dim(U_a) = m+r-2l_1 = (m-l_1-l_2)+(r+l_2-l_1)$ podemos suponer que tanto U como $U^\perp$ son anisotrópicos. Ahora hacemos la demostración por inducción en m. Si $m = 1$, el resultado es trivial. Supongamos que $m > 1$ y que el resultado vale para espacios hiperbólicos de dimensión menor que $2m$. Sea $v = u+u'$ con $u \in U$ y $u' \in U^\perp$ un vector isotrópico. Dado que u y u' son ortogonales y anisotrópicos, $Fu + Fu'$ es isomorfo a H (item 1) del Teorema 3.5). Sean $V \subseteq U$ y $V' \subseteq U^\perp$ los complementos ortogonales de Fu y Fu' respectivamente. Por el teorema de cancelación de Witt, $(m-1)H = V \perp V'$. Así, dado que $\dim(V) = m + r - 1$, el resultado se deduce inmediatamente de la hipótesis inductiva.

Ejercicio 13. *Es claro que* $1 = 1^2 + a0^2 \in D(\langle 1, a\rangle)$. *Ahora, la ecuación*

$$\begin{aligned}(x_1^2 + ax_2^2)(y_1^2 + ay_2^2) &= (x_1y_1)^2 + a\big((x_1y_2)^2 + (x_2y_1)^2\big) + (ax_2y_2)^2 \\ &= (x_1y_1 + ax_2y_2)^2 + a(x_1y_2 - x_2y_1)^2,\end{aligned}$$

muestra que, si $x_1^2+ax_2^2$ *y* $y_1^2+ay_2^2$ *están en* $D(\langle 1, a\rangle)$, *también* $(x_1^2+ax_2^2)(y_1^2+ay_2^2)$ *está en* $D(\langle 1, a\rangle)$ *y muestra también que* $(\lambda x_1)^2 + a(\lambda x_2)^2$ *con* $\lambda = \frac{1}{x_1^2+ax_2^2}$ *es el inverso multiplicativo de* $x_1^2 + ax_2^2$ *en* $\dot{F}$.

Ejercicio 14. *Dado que* $1 \in D(\varphi)$ *es claro que* $D(\varphi\otimes\sigma) \subseteq D(\varphi)D(\varphi\otimes\sigma)$. *Veamos la otra inclusión. Sean* U *y* V *los espacios vectoriales sobre los que están definidos* φ *y* σ *respectivamente. Si* $x \in D(\varphi)D(\varphi \otimes \sigma)$, *entonces existen* $u \in U$ *y* $\sum_{i\in I} u_i \otimes v_i \in U \otimes V$ *tales que* $x = \varphi(u)\big(\sum_{i\in I} \varphi(u_i)\sigma(v_i)\big) = \sum_{i\in I} \varphi(u)\varphi(u_i)\sigma(v_i)$. *Como* $D(\varphi)$ *es un subgrupo de* $\dot{F}$, *existen* u_i' $(i \in I)$ *tales que* $\varphi(u)\varphi(u_i) = \varphi(u_i')$. *Así,* $x = \sum_{i\in I} \varphi(u_i')\sigma(v_i) \in D(\varphi \otimes \sigma)$.

Ejercicio 15. *Escribamos* $\sigma = \sigma_t \perp mH \perp \sigma_a$ *con* σ_t *totalmente isotrópico y* σ_a *anisotrópico. Como* $\varphi \otimes \sigma = (\varphi \otimes \sigma_t) \perp (\varphi \otimes mH) \perp (\varphi \otimes \sigma_t) = (\varphi \otimes \sigma_t) \perp m\dim(\varphi)H \perp (\varphi\otimes\sigma_a)$ *(Corolario 6.2), el índice de Witt de* $\varphi\otimes\sigma$ *es mayor o igual que* $m\dim(\varphi)$. *Veamos la segunda afirmación. Por el teorema de descomposición de Witt, podemos escribir* $\varphi = \varphi_t \perp lH \perp \varphi_a$ *y* $\sigma = \sigma_t \perp mH \perp \sigma_a$, *con* φ_t *y* σ_t *totalmente isotrópicos y* φ_a *y* σ_a *anisotrópicos. Así,*

$$\varphi \perp \sigma = (\varphi_t \perp \sigma_t) \perp (m + l)H \perp (\varphi_a \perp \sigma_a).$$

Dado que el índice de Witt de $\varphi \perp \sigma$ *es el índice de Witt de* $\varphi_a \perp \sigma_a$ *más* $m+l$ *y que* $\dim(\varphi_a) \leq \dim(\varphi)-2l$, *podemos suponer que tanto* φ *como* σ *son anisotrópicos. En este caso tenemos que probar que el índice de Witt de* $\varphi \perp \sigma$ *es menor o igual que la dimensión de* φ. *Ahora hacemos la demostración por inducción en* $r = \dim(\varphi)$. *Si* $r = 0$, *el resultado es trivial. Supongamos que* $r > 0$ *y que el resultado vale para espacios de dimensión menor que* r. *Sean* U *y* V *los espacios vectoriales sobre los que están definidos* φ *y* σ *respectivamente y sea* $w = u + v$ *con* $u \in U$ *y* $v \in V$ *un vector isotrópico. Como* u *y* v *son ortogonales y anisotrópicos,* $Fu + Fv$ *es isomorfo a* H *(item 1) del Teorema 3.5). Denotemos con* $U' \subseteq U$ *y* $V' \subseteq V$ *a los complementos ortogonales de* Fu *y* Fv *respectivamente. Dado que la dimensión de* U' *es* $r - 1$, *por la hipótesis inductiva el índice de* $U' \perp V'$ *es menor o igual que* $r - 1$. *Usando ahora que* $U \perp V = H \perp (U' \perp V')$ *se deduce inmediatamente el resultado.*

Nota: La misma demostración que la de la segunda parte del Ejercicio 15 muestra que si los índices de Witt de φ y σ son m_1 y m_2 respectivamente, entonces el índice de Witt de $\varphi \perp \sigma$ es menor o igual que $m_1+m_2+\min(\dim(\varphi)-2m_1, \dim(\sigma)-2m_2)$ (y claramente mayor o igual que $m_1 + m_2$).

Ejercicios del Capítulo 2

Ejercicio 1. *Por el teorema de equivalencia de cadena de Witt podemos suponer que* $\langle a_1, a_2\rangle \simeq \langle b_1, b_2\rangle$ *y que* $a_i = b_i$ *para todo* $3 \leq i \leq n$. *Dado que*

$$a_1a_2 = \mathrm{d}(\langle a_1, a_2\rangle) = \mathrm{d}(\langle b_1, b_2\rangle) = b_1b_2 \pmod{\dot{F}^2},$$

en $\widehat{W}(F)$ *tenemos,*

$$\begin{aligned}(\langle a_1\rangle - 1)(\langle a_2\rangle - 1) &= \langle a_1a_2\rangle - \langle a_1\rangle - \langle a_2\rangle + 1\\ &= \langle a_1a_2\rangle - \langle a_1, a_2\rangle + 1\\ &= \langle b_1b_2\rangle - \langle b_1, b_2\rangle + 1\\ &= \langle b_1b_2\rangle - \langle b_1\rangle - \langle b_2\rangle + 1\\ &= (\langle b_1\rangle - 1)(\langle b_2\rangle - 1).\end{aligned}$$

El ejercicio ahora se termina fácilmente usando que $a_i = b_i$ *para* $3 \leq i \leq n$.

Ejercicio 2. *Sea* J *un ideal maximal de* $W(F)$ *que contiene a* $2 = \langle 1, 1\rangle$. *Afirmamos que* $\langle a, b\rangle \in J$, *para todo* $a, b \in \dot{F}$. *Dado que en* $W(F)$

$$\langle a, b\rangle\langle a, -b\rangle = \langle a^2, ab, -ab, -b^2\rangle = 2H = 0,$$

tenemos que $\langle a, b\rangle \in J$ *o* $\langle a, -b\rangle \in J$. *Podemos suponer que* $\langle a, -b\rangle \in J$. *Como* $\langle b, b\rangle = \langle b\rangle\langle 1, 1\rangle$ *también pertenece a* J *y en* $W(F)$

$$\langle a, b\rangle = \langle a, b\rangle + H = \langle a, -b, b, b\rangle = \langle a, -b\rangle + \langle b, b\rangle,$$

resulta que $\langle a, b\rangle \in J$. *Dados que* $a, b \in \dot{F}$ *son arbitrarios, esto muestra que* $IF \subseteq J$, *de donde por maximalidad,* $J = IF$. $\square$

Ejercicio 3

a) La forma bilineal asociada a q_1 *es*

$$B_1((x, y, z), (x', y', z')) = xx' + yy' + zz' + \frac{1}{2}(xy' + yx') + \frac{1}{2}(xz' + zx') + \frac{1}{2}(yz' + zy').$$

Como $B_1((x, y, z), (1, 0, 0)) = x + \frac{1}{2}y + \frac{1}{2}z$, *el vector* $v_1 = (1, 0, 0)$ *es anisotrópico y* $(\mathbb{R}(1, 0, 0))^{\perp} = \mathbb{R}(1, -2, 0) + \mathbb{R}(1, 0, -2)$. *Dado ahora que* $B_1((x, y, z), (1, -2, 0)) = -\frac{3}{2}y - \frac{1}{2}z$, *el vector* $v_2 = (1, -2, 0)$ *es anisotrópico y* $(\mathbb{R}(1, 0, 0) + \mathbb{R}(1, -2, 0))^{\perp} = \mathbb{R}(1, 1, -3)$. *Así, si* $v_3 = (1, 1, -3)$, *entonces* $q_1(xv_1 + yv_2 + zv_3) = x^2 + 3y^2 + 6z^2$, *de donde la signatura de* q_1 *es* 3.

b) La forma bilineal asociada a q_2 *es*

$$B_2((x, y, z), (x', y', z')) = yy' + 2zz' + 2(xy' + yx') + xz' + zx'.$$

Como $B_2((x, y, z), (0, 1, 0)) = 2x + y$, *el vector* $v_1 = (0, 1, 0)$ *es anisotrópico y* $(\mathbb{R}(0, 1, 0))^{\perp} = \mathbb{R}(1, -2, 0) + \mathbb{R}(0, 0, 1)$. *Dado ahora que* $B_1((x, y, z), (0, 0, 1)) = x + 2z$, *el vector* $v_2 = (0, 0, 1)$ *es anisotrópico y* $(\mathbb{R}(0, 1, 0) + \mathbb{R}(0, 0, 1))^{\perp} = \mathbb{R}(2, -4, -1)$. *Así, si* $v_3 = (2, -4, -1)$, *entonces* $q_2(xv_1 + yv_2 + zv_3) = x^2 + 2y^2$, *de donde el radical de* q_2 *tiene dimensión 1 y la signatura de la parte regular de* q_2 *es* 2.

c) Sea $y_2 = x_2 - x_1$. *Entonces*

$$\begin{aligned}\sum_{i=1}^{n-1} x_i x_{i+1} &= x_1(x_1+y_2) + (x_1+y_2)x_3 + \sum_{i=3}^{n-1} x_i x_{i+1} \\ &= x_1^2 + x_1y_2 + x_1x_3 + y_2x_3 + \sum_{i=3}^{n-1} x_i x_{i+1} \\ &= \Big(x_1 + \frac{y_2}{2} + \frac{x_3}{2}\Big)^2 - \frac{y_2^2}{4} - \frac{x_3^2}{4} + \frac{y_2x_3}{2} + \sum_{i=3}^{n-1} x_i x_{i+1} \\ &= z_1^2 - z_2^2 + \sum_{i=3}^{n-1} x_i x_{i+1},\end{aligned}$$

donde $z_1 = x_1 + \frac{1}{2}y_2 + \frac{1}{2}x_3 = \frac{1}{2}(x_1+x_2+x_3)$ *y* $z_2 = \frac{1}{2}(y_2 - x_3) = \frac{1}{2}(-x_1+x_2-x_3)$. *Ahora es fácil ver por inducción que si* $z_{2i-1} = \frac{1}{2}(x_{2i-1} + x_{2i} + x_{2i+1})$ *y* $z_{2i} = \frac{1}{2}(-x_{2i-1} + x_{2i} - x_{2i+1})$ *(*$1 \le i \le [(n-1)/2]$*), entonces*

$$\sum_{i=1}^{n-1} x_i x_{i+1} = \begin{cases} \displaystyle\sum_{i=1}^{(n-1)/2} z_{2i-1}^2 - z_{2i}^2 & \text{si } n \text{ es impar,} \\ \displaystyle\sum_{i=1}^{n/2} z_{2i-1}^2 - z_{2i}^2 & \text{si } n \text{ es par,} \end{cases}$$

donde si n *es par,* $z_{n-1} = \frac{1}{2}(x_{n-1} + x_n)$ *y* $z_n = \frac{1}{2}(-x_{n-1} + x_n)$ *(ver el ejemplo que sigue al método de diagonalización de Lagrange). En consecuencia* q_3 *es regular si y sólo si* n *es par, la dimensión del radical de* q_3 *es menor o igual que* 1 *y la signatura de la parte regular de* q_3 *es* 0.

Ejercicio 4. *Supongamos que* $W(F)$ *es finito. Por el Corolario 2.5 el grupo* $\frac{\dot{F}}{\dot{F}^2}$ *es finito. Además, dado que las formas* $n\langle 1\rangle$ *no son todas anisotrópicas, por el Corolario 3.6 del Capítulo 1, existe* $n \in \mathbb{N}$ *tal que* $-1 \in D(n\langle 1\rangle)$. *Así,* -1 *es una suma de cuadrados. Supongamos ahora que* $\frac{\dot{F}}{\dot{F}^2} = \{s_1, \ldots, s_l\}$ *y que* $-1 = x_1^2 + \cdots + x_r^2$. *Para cada forma* q *existen enteros no negativos* $m_1, \ldots, m_l$ *tales que* $m_1 + \cdots + m_l = \dim(q)$ *y* $q \simeq m_1\langle s_1\rangle \perp \cdots \perp m_l\langle s_l\rangle$. *Así, hay sólo un número finito de formas no isomorfas de cada dimensión. En consecuencia, para terminar el ejercicio es suficiente ver que si* $n > lr$, *no hay ninguna forma anisotrópica de dimensión* n. *Ahora, por el Corolario 3.6 del Capítulo 1 si* $m > r$, *entonces* $m\langle 1\rangle$ *(y por lo tanto* $m\langle s_i\rangle$ *(*$1 \le i \le l$*)) es anisotrópica. La demostración se termina observando que si* $m_1 + \cdots + m_l > lr$, *entonces existe* $1 \le i \le l$ *tal que* $m_i > r$.