UNIVERSIDAD DE VALPARAÍSO

Facultad de Ciencias

Departamento de Matemáticas

Grupo Ortogonal en Espacios de Dimensión Finita sobre Cuerpos Finitos

Tesis presentada por **Jorge Ovalle Ovalle.**
Para optar al grado de Licenciado en Matemáticas.

Profesor Guía Dr. Daniel Jiménez Briones.

Valparaíso, Septiembre de 2008.

Índice general

Tabla de Símbolos

$\mathbb{F}^*$	Grupo multiplicativo del cuerpo $\mathbb{F}$
$(\mathcal{V}, Q)$	Espacio Cuadrático $\mathcal{V}$, con Q la forma cuadrática asociada
$L(\mathcal{V}, \mathcal{W})$	Conjunto de transformaciones lineales de $\mathcal{V}$ en $\mathcal{W}$
$End(\mathcal{V})$	Conjunto de transformaciones lineales de $\mathcal{V}$ en $\mathcal{V}$
$GL_n(\mathcal{V})$	Grupo General Lineal del espacio vectorial $\mathcal{V}$, $\dim \mathcal{V} = n$
$O_n(\mathcal{V})$	Grupo Ortogonal del espacio vectorial $\mathcal{V}$, $\dim \mathcal{V} = n$
$M \equiv N$	M es equivalente con N (pág. 25)
$\mathcal{V} \asymp N$	N es la matriz asociada a $\mathcal{V}$
$\mathcal{V} \cong \mathcal{V}'$	$\sigma : \mathcal{V} \to \mathcal{V}'$, con σ un isomorfismo, $\mathcal{V}$ y $\mathcal{V}'$ son isométricos
$\langle N \rangle$	Espacio vectorial con N como matriz asociada
$d_B(z_1, z_2, \ldots, z_m)$	Discriminante de los vectores $z_1, \ldots, z_m$ (Def. 34)
$\dot{\mathbb{F}}$	Conjunto de los $\alpha \,\varepsilon\, \mathbb{F}$, tal que $\alpha \neq 0$
$\dot{\mathbb{F}}^2$	Conjunto de los $\beta \,\varepsilon\, \dot{\mathbb{F}}$, tal que existe $\alpha \,\varepsilon\, \mathbb{F}$, donde $\beta = \alpha^2$ (cuadrados)
$\mathcal{V} \perp \mathcal{V}'$	Suma ortogonal de $\mathcal{V}$ y $\mathcal{V}'$ (Def. 36)
$\mathcal{U} \oplus \mathcal{W}$	Suma directa entre $\mathcal{U}$ y $\mathcal{W}$
$\mathcal{U}^\perp$	Complemento ortogonal de $\mathcal{U}$ (Def. 38)
$\underset{i=1}{\overset{r}{\times}} \mathcal{V}_i$	Producto interno directo de los espacios $\mathcal{V}_i$
$rad\,\mathcal{U}$	Radical del espacio $\mathcal{U}$ (Def. 38)
$\mathcal{V}_\sigma$	Espacio fijo de σ sobre $\mathcal{V}$

Introducción

La presente tesis estudia el grupo de las transformaciones lineales biyectivas, que preserva o deja invariante una forma cuadrática en espacios vectoriales de dimensión finita sobre cuerpos finitos, llamadas transformaciones Ortogonales. Entre los elementos más característicos del grupo ortogonal, estudiaremos algunos invariantes, un conjunto generador, la posibilidad de levantar isometrías y algunos de los subgrupos notables.

Para finalizar este estudio se obtiene, en la Proposición 68, que un espacio vectorial $\mathcal{V}$ es una representación irreducible de $O_n(\mathcal{V})$ y utilizando los resultados de las proposiciones anteriores, obtendremos algunas representaciones irreducibles del grupo $O_2(\mathcal{V})$ y $O_4(\mathcal{V})$ al descomponer las representaciones naturales.

Para conseguir esto, en el Capítulo 1, entregamos las nociones básicas de álgebra lineal y de representación natural de grupos finitos y de esta manera introducimos las notaciones y la terminología necesaria para el desarrollo de esta tesis.

En el Capítulo 2, definimos los elementos básicos para introducirnos a las formas cuadráticas, entre ellos matriz asociada, suma ortogonal, el complemento ortogonal y el radical en $\mathcal{V}$, los cuales se definen en estos espacios vectoriales. Otros elementos de gran importancia son los vectores isótropos y anisótropos, los vectores isótropos permiten construir los espacios hiperbólicos, necesarios al momento de descomponer un espacio vectorial en suma ortogonal de espacios hiperbólicos, además con ellos construimos el índice; y por otra parte, los anisótropos, que sirven para construir reflexiones, las cuales forman un conjunto generador de nuestro Grupo Ortogonal. Para finalizar este capítulo, enunciamos el Teorema de Witt, de gran utilidad al momento de levantar una isometría a todo el espacio.

Iniciamos el Capítulo 3, destacando en $O_n(\mathcal{V})$ el subgrupo de las rotaciones O^+, para después pasar a estudiar los subgrupos conmutador y el centro, en forma especial entregamos resultados en dimensión 2 y 3. Como resultado adicional obtenemos que un espacio vectorial $\mathcal{V}$ es una representación irreducible del grupo ortogonal.

Para finalizar, en el Capítulo 4, construimos las representaciones naturales de los grupos $O_2(\mathcal{V})$ y $O_4(\mathcal{V})$, en cada uno de ellos descomponemos las órbitas y aplicamos métodos geométricos para encontrar la descomposición explícita de los espacios de representaciones irreducibles.

En el caso de $O_2(\mathcal{V})$, tenemos dos posibles espacios, el hiperbólico o el anisótropo, cuando $\mathcal{V}$ es un espacio isótropo, descomponemos su representación natural en dos naturales, la primera formada por el conjunto de los vectores anisótropos y la otra por el conjunto de los vectores isótropos, trabajando cada una por separado. Así obtenemos una descomposición total en subrepresentaciones irreducibles.

Para el caso de $O_4(\mathcal{V})$, tenemos dos posibles espacios, el formado por una suma de dos planos hiperbólicos y el otro formado por un plano hiperbólico suma ortogonal con un plano anisótropo, en cada uno de estos casos encontramos su descomposición.

Cabe destacar, que para encontrar las subrepresentaciones irreducibles de la representación natural del grupo, hemos usado la estrecha relación que existe entre las órbitas que se obtiene al actuar el grupo sobre el conjunto y los operadores de entrelazamiento.

Capítulo 1

Preliminares

Los resultados expuestos en este capítulo, se pueden encontrar fácilmente en textos relacionados con Algebra Lineal y de Teoría de Representación de Grupos Finitos, en particular utilizaremos [2] y [3].

1.1. Algebra Lineal

En todo lo que sigue, $\mathbb{F}$ denota un cuerpo.

Definición 1 *La traspuesta M^t de una matriz $M = (a_{i\,j}) \,\varepsilon\, M_{n\times m}(\mathbb{F})$ es la matriz de $M_{m\times n}(\mathbb{F})$, la cual posee en la posición (i, j) el coeficiente $a_{j\,i}$.*

Proposición 1 *Sean M y N matrices, tal que el producto MN este bien definido, entonces*

i) $(MN)^t = N^t M^t$

ii) Sea M una matriz de $n \times n$ entonces, $\det(M) = \det(M^t)$

Si $M \,\varepsilon\, GL_n(\mathbb{F})$, entonces

$$(M^{-1})^t = (M^t)^{-1}$$

Definición 2 *Diremos que $\mathcal{V}$ es un $\mathbb{F}$-espacio vectorial, si $(\mathcal{V}, +)$ es un grupo abeliano y además existe una función*

$$\begin{array}{rcl} \cdot : \mathbb{F} \times \mathcal{V} & \rightarrow & \mathcal{V} \\ (\alpha, v) & \rightsquigarrow & \alpha v \end{array}$$

tal que para todo u, $v \,\varepsilon\, \mathcal{V}$ y α, $\beta \,\varepsilon\, \mathbb{F}$, se cumplen los siguientes axiomas:

i) $\alpha(u + v) = \alpha u + \alpha v$

ii) $(\alpha + \beta)v = \alpha v + \beta v$

iii) $(\alpha\beta)v = \alpha(\beta v)$

iv) $1_{\mathbb{F}} v = v$

Ejemplo 1

a) *Sea* $\mathbb{F}^n = \mathbb{F} \times \mathbb{F} \times \cdots \times \mathbb{F}$ *(n veces) un* $\mathbb{F}$*-espacio vectorial, con las operaciones usuales:*

   i) $(x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n) = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$

   ii) $\alpha(x_1, x_2, \ldots, x_n) = (\alpha x_1, \alpha x_2, \ldots, \alpha x_n)$

b) *Sea* $\mathbb{F}^X = \{f : X \to \mathbb{F} \mid f \text{ es una función}\}$*,* $\mathbb{F}^X$ *es un* $\mathbb{F}$*-espacio vectorial con las siguientes operaciones:*

   i)
$$\begin{array}{rll} f+g: & X & \to \mathbb{F} \\ & x & \rightsquigarrow f(x)+g(x) \end{array}$$

   ii)
$$\begin{array}{rll} \alpha f: & X & \to \mathbb{F} \\ & x & \rightsquigarrow \alpha f(x) \end{array}$$

Definición 3 *Sea* $\mathcal{U}$ *un subconjunto no vacío de* $\mathcal{V}$*. Diremos que* $\mathcal{U}$ *es un* $\mathbb{F}$*-subespacio (o simplemente subespacio) vectorial de* $\mathcal{V}$ *si se cumple:*

i) $u + v \,\varepsilon\, \mathcal{U}$*, para todo* $u, v \,\varepsilon\, \mathcal{U}$

ii) $\alpha u \,\varepsilon\, \mathcal{U}$*, para todo* $u \,\varepsilon\, \mathcal{U}$ *y* $\alpha \,\varepsilon\, \mathbb{F}$

Definición 4 *Sean* $v_1, v_2, \ldots, v_m$ *vectores de un* $\mathbb{F}$*-espacio vectorial* $\mathcal{V}$*. Diremos que* v *es una combinación lineal de los vectores* $v_1, v_2, \ldots, v_m$ *si y sólo si existen escalares* $\alpha_1, \alpha_2, \ldots, \alpha_m \,\varepsilon\, \mathbb{F}$*, tal que*

$$v = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_m v_m$$

Sea S un subconjunto no vacío del $\mathbb{F}$-espacio vectorial $\mathcal{V}$. Se define

$$< S >= \left\{ \sum_{i=1}^{n} \alpha_i s_i \mid s_i \,\varepsilon\, S,\ \alpha_i \,\varepsilon\, \mathbb{F},\ n \,\varepsilon\, \mathbb{N} \right\}$$

como el subconjunto de $\mathcal{V}$ formado por todas las combinaciones lineales de los elementos de S.

Proposición 2 *Sea* $S \subseteq \mathcal{V}$*, entonces* $< S >$ *es un subespacio vectorial de* $\mathcal{V}$*.*

Definición 5 *El subespacio vectorial* $< S >$ *de* $\mathcal{V}$ *se llama el espacio generado por* S*.*

Definición 6 *Sea* $S = \{v_1, v_2, \ldots, v_m\}$ *un subconjunto de* $\mathcal{V}$.

i) Diremos que S *es linealmente dependiente si y sólo si, existen escalares no todos nulos* $\alpha_1, \alpha_2, \ldots, \alpha_m \,\varepsilon\, \mathbb{F}$, *tal que*

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_m v_m = 0$$

ii) En otro caso diremos que S *es linealmente independiente, es decir,*

$$\textit{Si } \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_m v_m = 0, \textit{ entonces } \alpha_1 = \alpha_2 = \cdots = \alpha_m = 0$$

Proposición 3 S *es linealmente independiente si y sólo si, no existe* $v \,\varepsilon\, S$ *que es combinación lineal de elementos de* $S - \{v\}$.

Definición 7 *Un subconjunto ordenado* $\mathcal{B}$ *de* $\mathcal{V}$ *se dice una base de* $\mathcal{V}$ *si:*

i) $\mathcal{B}$ *es linealmente independiente*

ii) $\mathcal{B}$ *genera a* $\mathcal{V}$

Proposición 4 *Sea* $\mathcal{V}$ *un* $\mathbb{F}$*-espacio vectorial. Sean* $J \subseteq S$ *subconjuntos no vacíos de* $\mathcal{V}$, *tales que* J *es linealmente independiente y* S *genera a* $\mathcal{V}$. *Entonces existe una base* $\mathcal{B}$ *de* $\mathcal{V}$, *tal que*

$$J \subseteq \mathcal{B} \subseteq S$$

Corolario 1 *Todo conjunto linealmente independiente está contenido en una base.*

Proposición 5 *Sean* $\mathcal{B} = \{v_1, v_2, \ldots, v_n\}$ *y* $\mathcal{B}' = \{w_1, w_2, \ldots, w_m\}$ *dos bases de* $\mathcal{V}$, *entonces* $n = m$.

Definición 8 *Sean* $\mathcal{V}$ *un* $\mathbb{F}$*-espacio vectorial y* $\mathcal{B}$ *una base de* $\mathcal{V}$.

Si $\mathcal{B}$ *es un conjunto finito, entonces se define la dimensión de* $\mathcal{V}$ *como el cardinal de* $\mathcal{B}$, *lo cual denotamos por* $\dim(\mathcal{V})$.

Proposición 6 *Sea* $\mathcal{B} = \{v_1, v_2, \ldots, v_n\}$ *una base del* $\mathbb{F}$*-espacio vectorial* $\mathcal{V}$ *y* $v \,\varepsilon\, \mathcal{V}$, *entonces existen únicos escalares* $\alpha_1, \alpha_2, \ldots, \alpha_n \,\varepsilon\, \mathbb{F}$ *tales que*

$$v = \alpha v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$$

Definición 9 *Conservando las notaciones de la Proposición anterior. Se define las coordenadas de* $v \,\varepsilon\, \mathcal{V}$, *respecto a una base* $\mathcal{B}$, *como la matriz* $[v]_{\mathcal{B}} \,\varepsilon\, M_{n\times 1}(\mathbb{F})$ *definida por:*

$$[v]_{\mathcal{B}} = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix}$$

Definición 10 *Sea* $\mathcal{B} = \{v_1, v_2, \ldots, v_n\}$ *y* $\mathcal{D}$ *dos bases del* $\mathbb{F}$*-espacio vectorial* $\mathcal{V}$*. La matriz cambio de base* $[Id]_{\mathcal{B}}^{\mathcal{D}}$ *es la matriz de* $M_n(\mathbb{F})$ *cuya i-ésima columna es* $[v_i]_{\mathcal{D}}$*.*

Proposición 7 *Sean* $\mathcal{B}$ *y* $\mathcal{D}$ *dos bases de* $\mathcal{V}$ *y* $v \,\varepsilon\, \mathcal{V}$*. Entonces*

i) $[Id]_{\mathcal{B}}^{\mathcal{D}}[v]_{\mathcal{B}} = [v]_{\mathcal{D}}$

ii) $[Id]_{\mathcal{B}}^{\mathcal{D}}$ *es invertible, donde* $([Id]_{\mathcal{B}}^{\mathcal{D}})^{-1} = [Id]_{\mathcal{D}}^{\mathcal{B}}$

Definición 11 *Sean* $\mathcal{U}$, $\mathcal{W}$ *dos subespacios del* $\mathbb{F}$*-espacio vectorial* $\mathcal{V}$*. Se define la suma de* $\mathcal{U}$ *y* $\mathcal{W}$ *como:*

$$\mathcal{U} + \mathcal{W} = \{u + w \mid u \,\varepsilon\, \mathcal{U},\, w \,\varepsilon\, \mathcal{W}\}$$

Definición 12 *Sean* $\mathcal{U}$, $\mathcal{W}$ *dos subespacios del* $\mathbb{F}$*-espacio vectorial* $\mathcal{V}$*. Diremos que* $\mathcal{V}$ *es una suma directa (interna) de los subespacios* $\mathcal{U}$ *y* $\mathcal{W}$ *si:*

i) $\mathcal{V} = \mathcal{U} + \mathcal{W}$

ii) $\mathcal{U} \cap \mathcal{W} = \{0\}$

Denotaremos a esta suma como:

$$\mathcal{V} = \mathcal{U} \oplus \mathcal{W}$$

Proposición 8 *Sean* $\mathcal{U}$, $\mathcal{W}$ *dos subespacios de un espacio vectorial de dimensión finita, entonces*

$$\dim(\mathcal{U} + \mathcal{W}) = \dim(\mathcal{U}) + \dim(\mathcal{W}) - \dim(\mathcal{U} \cap \mathcal{W})$$

En particular

$$\dim(\mathcal{U} \oplus \mathcal{W}) = \dim(\mathcal{U}) + \dim(\mathcal{W})$$

Definición 13 *Sean* $\mathcal{U}_1, \mathcal{U}_2, \ldots, \mathcal{U}_r$ *subespacios del espacio vectorial* $\mathcal{V}$*. Diremos que* $\mathcal{V}$ *es la suma directa de* $\mathcal{U}_1, \mathcal{U}_2, \ldots, \mathcal{U}_r$ *si se tiene:*

i) $\mathcal{V} = \mathcal{U}_1 + \mathcal{U}_2 + \ldots + \mathcal{U}_r$

ii) $\mathcal{U}_i \cap (\mathcal{U}_1 + \mathcal{U}_2 + \ldots + \mathcal{U}_{i-1} + \mathcal{U}_{i+1} + \ldots + \mathcal{U}_r) = \{0\}$ *para todo i*

Definición 14 *Sean* $\mathcal{V}$, $\mathcal{V}'$ *dos espacios vectoriales de dimensión finita sobre* $\mathbb{F}$*. Diremos que la función* $f : \mathcal{V} \to \mathcal{V}'$ *es una transformación lineal (o función lineal) si para todo* $u, v \,\varepsilon\, \mathcal{V}$ *y* $\alpha \,\varepsilon\, \mathbb{F}$*, se tiene:*

i) $f(u + v) = f(u) + f(v)$

ii) $f(\alpha v) = \alpha f(v)$

Sean $\mathcal{V}$, $\mathcal{V}'$ dos espacios vectoriales de dimensión finita. El conjuntos de todas las transformaciones lineales de $\mathcal{V}$ en $\mathcal{V}'$ es un espacio vectorial de dimensión finita sobre $\mathbb{F}$. Este conjunto lo denotamos por:

$$L(\mathcal{V}, \mathcal{V}')$$

Cuando $\mathcal{V} = \mathcal{V}'$, la composición de transformaciones provee una multiplicación en $L(\mathcal{V}, \mathcal{V})$ la cual hace de este, un anillo con identidad; entonces usamos

$$End(\mathcal{V})$$

La multiplicación por escalar y la multiplicación de anillo en $End(\mathcal{V})$ cumple la siguiente propiedad:

$$\alpha(\varphi\psi) = (\alpha\varphi)\psi = \varphi(\alpha\psi)$$

para todo $\alpha \varepsilon \mathbb{F}$ y toda $\varphi, \psi \varepsilon End(\mathcal{V})$, así $End(\mathcal{V})$ tiene estructura de una $\mathbb{F}$-algebra.

Definición 15 *Las transformaciones lineales invertibles en $End(\mathcal{V})$ forman un grupo llamado el Grupo General Lineal y se denota por:*

$$GL_{\mathbb{F}}(\mathcal{V}), \quad GL_n(\mathcal{V}), \quad o \quad GL(\mathcal{V})$$

donde $\dim \mathcal{V} = n$.

Definición 16 *Sean $\mathcal{V}$, $\mathcal{V}'$ dos espacios vectorial sobre $\mathbb{F}$ y sean $\mathcal{B} = \{v_1, v_2, \ldots, v_n\}$, $\mathcal{D}$ bases de $\mathcal{V}$ y $\mathcal{V}'$ respectivamente. La matriz asociada a $\phi \,\varepsilon\, L(\mathcal{V}, \mathcal{V}')$ respecto a las bases $\mathcal{B}$ y $\mathcal{D}$, es la matriz $[\phi]_{\mathcal{B}}^{\mathcal{D}}$ de $M_{m\times n}$ cuya i-ésima columna es $[\phi(v_i)]_{\mathcal{D}}$.*

Proposición 9 *Sean $\phi, \phi' \,\varepsilon\, Hom(\mathcal{V}, \mathcal{V}')$, $\psi \,\varepsilon\, Hom(\mathcal{V}', \mathcal{W})$ y $\mathcal{B}$, $\mathcal{D}$, $\mathcal{C}$ bases de $\mathcal{V}$, $\mathcal{V}'$, $\mathcal{W}$ respectivamente. Entonces*

i) $[\phi]_{\mathcal{B}}^{\mathcal{D}}[v]_{\mathcal{B}} = [\phi(v)]_{\mathcal{D}} \qquad (v \,\varepsilon\, \mathcal{V})$

ii) $[\alpha\phi + \phi']_{\mathcal{B}}^{\mathcal{D}} = \alpha[\phi]_{\mathcal{B}}^{\mathcal{D}} + [\phi']_{\mathcal{B}}^{\mathcal{D}}$ $(\alpha \,\varepsilon\, \mathbb{F})$

iii) $[\psi \circ \phi]_{\mathcal{B}}^{\mathcal{C}} = [\psi]_{\mathcal{D}}^{\mathcal{C}}[\phi]_{\mathcal{B}}^{\mathcal{D}}$

1.1.1. Diagonalización

Proposición 10 *Sean $\phi \,\varepsilon\, End(\mathcal{V})$ y $\mathcal{B}$, $\mathcal{D}$ dos bases del espacio de dimensión finita $\mathcal{V}$, entonces*

$$\det([\phi]_{\mathcal{B}}) = \det([\phi]_{\mathcal{D}})$$

Notación. Sean $\phi \,\varepsilon\, End(\mathcal{V})$ y $\mathcal{B}$ una base de $\mathcal{V}$. Se define el determinante de ϕ como

$$\det \phi = \det([\phi]_{\mathcal{B}})$$

Definición 17 *Sea $\phi \varepsilon End(\mathcal{V})$, donde $\mathcal{V}$ es un $\mathbb{F}$-espacio vectorial de dimensión n y $\mathcal{B}$ una base de $\mathcal{V}$.*

i) Un vector no nulo $v \varepsilon \mathcal{V}$, se dice un vector propio ϕ si existe $\alpha \varepsilon \mathbb{F}$, tal que $\phi(v) = \alpha v$. El escalar α se llama valor propio.

ii) El polinomio $\det([\phi] - xId_n) \varepsilon \mathbb{F}[x]$, se llama polinomio característico. La ecuación $\det([\phi]_{\mathcal{B}} - xId_n) = 0$, se llama ecuación característica de ϕ.

Definición 18 *Si $\alpha \varepsilon \mathbb{F}$ es un valor propio de $\phi \varepsilon End(\mathcal{V})$. Definimos el espacio propio V_α asociado a α, como el Kernel del endomorfismo $\phi - \alpha 1_{\mathcal{V}}$, es decir*

$$\begin{aligned} V_\alpha &= \{v \varepsilon \mathcal{V} \mid (\phi - \alpha 1_{\mathcal{V}})(v) = 0\} \\ &= \{v \varepsilon \mathcal{V} \mid \phi(v) = \alpha v\} \end{aligned}$$

Proposición 11 *Sean $\alpha_1, \alpha_2, \ldots, \alpha_m$ los distintos valores propios de $\phi \varepsilon End(\mathcal{V})$ y $v_1, v_2, \ldots, v_m$ los respectivos vectores propios. Entonces $\{v_1, v_2, \ldots, v_m\}$ es un conjunto linealmente independiente.*

1.2. Representación Natural de Grupos

Sea X un conjunto finito y G un grupo. Sea $\cdot$ una función de $G \times X$ en X, es decir:

$$\begin{aligned} \cdot :\ G \times X &\to X \\ (g, x) &\rightsquigarrow g \cdot x \end{aligned}$$

Se dice que $\cdot$ es una acción si y sólo si

i) $e \cdot x = x$

ii) $g \cdot (h \cdot x) = (gh) \cdot x \qquad \forall\, g, h \,\varepsilon\, G$ y $\forall\, x \,\varepsilon\, X$.

En esta situación, decimos que G actúa sobre X o que X es un G-conjunto.

Si G actúa sobre X, entonces actúa sobre el espacio vectorial

$$\mathbb{C}^X = \{f : X \to \mathbb{C} \mid f \text{ es función}\}$$

del siguiente modo:

$$\begin{aligned} * : G \times \mathbb{C}^X &\to \mathbb{C}^X \\ (g, f) &\rightsquigarrow g * f \end{aligned}$$

donde

$$\begin{aligned} g * f : X &\to \mathbb{C} \\ x &\rightsquigarrow (g * f)(x) = f(g^{-1} \cdot x) \end{aligned}$$

Una base para $\mathbb{C}^X$ es $\{\delta_x \mid x \,\varepsilon\, X\}$, donde

$$\begin{array}{rll} \delta_x : & X & \to \mathbb{C} \\ & y & \rightsquigarrow \begin{cases} 1 & x = y \\ 0 & x \neq y \end{cases} \end{array}$$

Proposición 12 *Sea $g \,\varepsilon\, G$, entonces*

$$\begin{array}{rll} g : & \mathbb{C}^X & \to \mathbb{C}^X \\ & f & \rightsquigarrow g * f \end{array}$$

es un automorfismo.

De esta manera

$$\begin{array}{rll} \rho : & G & \to Aut_{\mathbb{C}}(\mathbb{C}^X) \\ & g & \rightsquigarrow \quad \rho_g : \mathbb{C}^X \to \mathbb{C}^X \\ & & \qquad\qquad f \rightsquigarrow \rho_g(f) : X \to \mathbb{C} \\ & & \qquad\qquad\qquad\qquad x \rightsquigarrow f(g^{-1} \cdot x) \end{array}$$

es llamada la representación natural de G.

En general tenemos lo siguiente:

Definición 19 *Se dice que $(\mathcal{V}, \rho)$ es una representación lineal de G si y sólo si*

$$\rho : G \to Aut_{\mathbb{C}}(\mathcal{V})$$

es un homomorfismo de grupos.

Proposición 13 *Sea X un conjunto finito, entonces*

$$\begin{array}{rll} \psi : & \mathbb{C}^X & \to \mathbb{C}^{|X|} \\ & f & \rightsquigarrow \displaystyle\sum_{x \,\varepsilon\, X} f(x) e_x \end{array}$$

es un isomorfismo.

Observación. Consideremos el producto interno canónico de $\mathbb{C}^n$, definido como:

$$\begin{array}{rll} F : & \mathbb{C}^n \times \mathbb{C}^n & \to \mathbb{C} \\ & (x, y) & \rightsquigarrow F(x, y) = \displaystyle\sum_{i=1}^{n} x_i \overline{y_i} \end{array}$$

donde $x = (x_1, x_2, \ldots, x_n)$ e $y = (y_1, y_2, \ldots, y_n)$.

La Proposición anterior, nos permite definir un producto interno para $\mathbb{C}^X$, dado como:

$$\begin{aligned} <,>: \ \mathbb{C}^X \times \mathbb{C}^X &\to \mathbb{C} \\ (f,h) &\rightsquigarrow \sum_{x\,\varepsilon\,X} f(x)\overline{h(x)} \end{aligned}$$

el cual es invariante bajo G, es decir,

$$< \rho_g(f), \rho_g(h) >=< f, h > \qquad \forall\, g\,\varepsilon\, G$$

Notación. Denotaremos por $L^2(X)$ a $\mathbb{C}^X$.

Definición 20 *Sea G un grupo finito y $(\mathcal{V}, \rho)$ una representación de G.*
Se dice que $(\mathcal{U}, \rho)$ es una subrepresentación de $(\mathcal{V}, \rho)$ si y sólo si

i) $\mathcal{U} \leq \mathcal{V}$ *(subespacio vectorial)*

ii) $(\forall\, g\,\varepsilon\, G)(\rho_g(\mathcal{U}) \subseteq \mathcal{U})$

Definición 21 *Sea $(\mathcal{V}, \rho)$ una representación del grupo finito G. Se dice que $(\mathcal{V}, \rho)$ es una representación irreducible si y sólo si las únicas subrepresentaciones de $\mathcal{V}$ son las triviales, es decir, $(\mathcal{V}, \rho)$ y $(\{e\}, \rho)$ son las únicas subrepresentaciones de $\mathcal{V}$.*

Proposición 14 *Sean $(L^2(X), \rho)$ la representación natural de G, $(\mathcal{U}, \rho)$ una subrepresentación de $L^2(X)$ y $<,>$ un producto interno invariante, entonces $(\mathcal{U}^\perp, \rho)$ es también una subrepresentación de $L^2(X)$, es decir,*

$$L^2(X) = \mathcal{U} \oplus \mathcal{U}^\perp$$

donde

$$\mathcal{U}^\perp = \{f\,\varepsilon\, L^2(X)\, |< f, h >= 0 \quad \forall\, h\,\varepsilon\,\mathcal{U})\}$$

Definición 22 *Sean $(\mathcal{V}, \rho)$, $(\mathcal{W}, \sigma)$ dos representaciones del grupo G y $\phi\,\varepsilon\, Hom(\mathcal{V}, \mathcal{W})$. Diremos que ϕ es un operador de entrelazamiento si $\forall\, g\,\varepsilon\, G$ el siguiente diagrama*

$$\begin{tikzcd} \mathcal{V} \arrow[r, "\phi"] \arrow[d, "\rho_g"'] \arrow[dr, phantom, "\circlearrowright"] & \mathcal{W} \arrow[d, "\sigma_g"] \\ \mathcal{V} \arrow[r, "\phi"'] & \mathcal{W} \end{tikzcd}$$

conmuta, es decir,

$$\rho_g \circ \phi = \phi \circ \sigma_g \qquad \forall\, g\,\varepsilon\, G$$

Notación. Sean $(\mathcal{V},\rho)$, $(\mathcal{W},\sigma)$ dos representaciones del grupo G. Entonces

$$Hom_G(\mathcal{V},\mathcal{W}) = \{\phi : \mathcal{V} \to \mathcal{W} \mid \phi \text{ es un operador de entrelazamiento}\}$$

$$End_G(\mathcal{V}) = \{\phi \mid \phi \,\varepsilon\, Hom_G(\mathcal{V},\mathcal{V})\}$$

Definición 23 *Se dice que las representaciones $(\mathcal{V},\rho)$ y $(\mathcal{W},\sigma)$ son isomorfas si y sólo si existe $\tau : \mathcal{V} \to \mathcal{W}$ un isomorfismo, el cual satisface la siguiente identidad:*

$$\rho_g \circ \tau = \tau \circ \sigma_g \qquad \forall g \,\varepsilon\, G$$

Proposición 15 *Sea $(\mathcal{V},\rho)$ una representación del grupo G. Sea $\phi \,\varepsilon\, End_G(\mathcal{V})$ y α un valor propio de ϕ, entonces*

$$\rho_g(V_\alpha) \subseteq V_\alpha \qquad \forall\, g \,\varepsilon\, G$$

donde V_α es el espacio propio asociado a α.

Proposición 16 *Sea G un grupo, X un conjunto no vacío tal que G actúa sobre X, entonces*

$$\cdot : G \times (X \times X) \to X \times X$$

$$(g,(x,y)) \rightsquigarrow (g\cdot x, g\cdot y)$$

es una acción de G sobre $X \times X$.

Definición 24 *Sea X un G-conjunto. Se define el conjunto de núcleos*

$$N(X,G) = \{K : X \times X \to \mathbb{C} \mid (\forall\, x,y \,\varepsilon\, X)(\forall\, g \,\varepsilon\, G)(K(g\cdot x, g\cdot y) = K(x,y))\}$$

Observación. Sea $K \,\varepsilon\, N(X,G)$, entonces

$$w,z \,\varepsilon\, \mathcal{O}_{(x,y)} \Rightarrow K(w) = K(z)$$

Definición 25 *Sea $\mathcal{O}$ una órbita de la acción de G en $X\times X$. Se define la función característica en la órbita $\mathcal{O}$, como:*

$$\begin{array}{rcl} K: & X \times X & \to \mathbb{C} \\ & (x,y) & \rightsquigarrow \begin{cases} 1 & (x,y) \,\varepsilon\, \mathcal{O} \\ 0 & (x,y) \notin \mathcal{O} \end{cases} \end{array}$$

Definición 26 *Sean $K \varepsilon N(X,G)$ y $\{\delta_x \mid x \varepsilon X\}$ una base de $L^2(X)$, entonces definimos*

$$\begin{array}{rll} \phi_K: & L^2(X) & \to L^2(X) \\ & \delta_x & \rightsquigarrow \sum\limits_{y \,\varepsilon\, X} K(y,x)\delta_y \end{array}$$

un operador de entrelazamiento. En forma general

$$\begin{array}{rll} \phi_K: & L^2(X) & \to L^2(X) \\ & f & \rightsquigarrow \sum\limits_{y \,\varepsilon\, X} K(?,y)f(y) \end{array}$$

Proposición 17 *Sea X un G-conjunto, entonces*

$$\begin{array}{rlll} \psi: & End_G(L^2(X)) & \to N(X,G) \\ & \phi & \to & K_\phi \\ & \phi_K & \leftarrow & K \end{array}$$

es un isomorfismo.

Teorema 1 (Maschke) *Toda representación $(\mathcal{V},\rho)$ de un grupo G es suma directa de representaciones irreducibles*

Corolario 2 *Toda representación $(\mathcal{V},\rho)$ de un grupo G, tiene una descomposición de la forma*

$$\rho = \bigoplus_{i=1}^{r} n_i\rho_i$$

donde $n_i\rho_i$ denota la suma directa de n_i sumandos isomorfismos a ρ_i y ρ_i son todas representaciones irreducibles no isomorfas de G. Esta descomposición es única, salvo orden.

Proposición 18 *Si G es un grupo abeliano, entonces todas las representaciones irreducibles tienen dimensión 1.*

Proposición 19 *Sea $(\mathcal{V},\rho)$ una representación de G. Si*

$$\rho = \bigoplus_{i=1}^{r} n_i\rho_i$$

con ρ_i representaciones irreducibles no isomorfas, entonces

i)

$$\dim_{\mathbb{C}}(End_G(\mathcal{V})) = \sum_{i=1}^{r} n_i^2$$

ii) Sea X un G-conjunto, entonces

$$dim_{\mathbb{C}}(End_G(L^2(X)) = \mid X \times X/G \mid$$

1.2.1. Caracteres

Definición 27 *Sean $\mathcal{V}$ un espacio vectorial de dimensión n, $\mathcal{B}$ una base de $\mathcal{V}$ y f una transformación lineal en $\mathcal{V}$, tal que $[f]_{\mathcal{B}} = (a_{i\,j})$. Se define la traza de f como*

$$Tr(f) = \sum_{i=1}^{n} a_{i\,i}$$

Definición 28 *Sean $(\mathcal{V}, \rho)$ una representación de un grupo G y $\mathcal{B}$ una base de $\mathcal{V}$. Se define el caracter de la representación ρ como*

$$\begin{array}{rll} \chi_\rho : & G & \to \mathbb{C} \\ & g & \rightsquigarrow \chi_\rho(g) = Tr(\rho_g) \end{array}$$

Observación. $\chi_\rho \,\varepsilon\, L^2(G)$.

Proposición 20 *Sea χ el caracter de la representación $(\mathcal{V}, \rho)$ del grupo G, tal que $\dim \mathcal{V} = n$. Entonces*

i) $\chi(e) = n$

ii) $\chi(g^{-1}) = \overline{\chi(g)}$ *para* $g \,\varepsilon\, G$

iii) $\chi(ghg^{-1}) = \chi(h)$ *para todo* $g, h \,\varepsilon\, G$

donde $\overline{\chi(g)}$ *corresponde al conjugado de* $\chi(g)$.

Proposición 21 (Lema de Schur) *Sean $(\mathcal{V}, \rho)$, $(\mathcal{W}, \sigma)$ dos representaciones de un grupo G y sea $\phi \,\varepsilon\, Hom_G(\mathcal{V}, \mathcal{W})$.*

i) *Si $(\mathcal{V}, \rho)$ y $(\mathcal{W}, \sigma)$ son irreducibles no isomorfos, entonces $\phi = 0$.*

ii) *Si $(\mathcal{V}, \rho)$ y $(\mathcal{W}, \sigma)$ son isomorfas, entonces ϕ es una homotecia, es decir, una multiplicación por escalar de la identidad.*

Proposición 22 *Sean $(\mathcal{V}, \rho)$, $(\mathcal{W}, \sigma)$ dos representaciones de un grupo G.*

$$(\mathcal{V}, \rho) \text{ y } (\mathcal{W}, \sigma) \text{ son isomorfas si y sólo si } \chi_\rho = \chi_\sigma$$

Proposición 23 *Sean $(\mathcal{V}, \rho)$, $(\mathcal{W}, \sigma)$ dos representaciones de G, entonces*

$$< \chi_\rho, \chi_\sigma >= \dim_{\mathbb{C}}(Hom_G(\rho, \sigma))$$

Capítulo 2

Formas Cuadráticas y Grupo Ortogonal

Nuestro propósito es estudiar las formas cuadráticas y la geometría ortogonal en un espacio vectorial $\mathcal{V}$ de dimensión finita n.

Para ello estudiaremos ciertos grupos de transformaciones lineales que deja la forma cuadrática invariante. Debemos hacer la suposición desde ahora que el cuerpo de escalares $\mathbb{F}$ es de característica distinta de 2 y $\mathcal{V}$ es no nulo.

2.1. Espacios Cuadráticos

Sea $\mathcal{V}$ un espacio vectorial de dimensión n sobre el cuerpo $\mathbb{F}$ de característica distinta de 2 y sea B una forma bilineal simétrica de $\mathcal{V} \times \mathcal{V}$, es decir una función

$$B : \mathcal{V} \times \mathcal{V} \to \mathbb{F}$$

con las siguientes propiedades:

$$\begin{array}{rcl} B(x+y,z) & = & B(x,z)+B(y,z) \\ B(x,y+z) & = & B(x,y)+B(x,z) \\ B(\alpha x,y) & = & \alpha B(x,y) \\ B(x,y) & = & B(y,x) \end{array}$$

para todo $x, y, z \,\varepsilon\, \mathcal{V}$ y todo $\alpha \,\varepsilon\, \mathbb{F}$.

Si definimos $Q(x) = B(x,x)$, obtenemos una función

$$Q : \mathcal{V} \to \mathbb{F}$$

que satisface las siguientes propiedades

$$Q(\alpha x) = \alpha^2 Q(x)$$

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

A esta función la llamamos **forma cuadrática**. Una forma de escribir ambas condiciones es:

$$Q\left(\sum_i \alpha_i x_i\right) = \sum_i \alpha_i^2 Q(x_i) + 2\sum_{i<j} \alpha_i\alpha_j B(x_i, x_j)$$

La segunda identidad muestra que la forma bilineal simétrica B asociada con la forma cuadrática Q es única.

$$B(x,y) = \frac{1}{2}\left(Q(x+y) - Q(x) - Q(y)\right)$$

Definición 29 *Un espacio cuadrático es un par $(\mathcal{V}, Q)$ tal que $\mathcal{V}$ es un espacio vectorial y Q es una forma cuadrática la cual tiene a B como forma bilineal simétrica asociada a Q.*

Ejemplo 2

1) *Sea $\mathcal{V} = \mathbb{F} \times \mathbb{F}$. Definimos*

$$\begin{array}{rcl} Q: & \mathcal{V} & \to \mathbb{F} \\ & (x,y) & \rightsquigarrow xy \end{array}$$

una forma cuadrática. Entonces $(\mathcal{V}, Q)$ es un espacio cuadrático.

2) *Sea $\mathbb{F}_q$, el cuerpo finito de q elementos. Entonces*

$$\mathbb{F}_{q^2} = \{\alpha + \epsilon\beta \mid \alpha, \beta \,\varepsilon\, \mathbb{F}_q\} = \mathbb{F}_q[x]/ < x^2 - \delta >$$

es la extensión cuadrática de $\mathbb{F}_q$, donde δ es un no cuadrado de $\mathbb{F}_q$.

De esta forma $\mathbb{F}_{q^2}$, es un espacio vectorial de dimensión dos sobre $\mathbb{F}_q$. Se define

$$\begin{array}{rcl} N: & \mathbb{F}_{q^2} & \to \mathbb{F}_q \\ & a + \epsilon b & \rightsquigarrow a^2 - \delta b^2 \end{array}$$

que es una forma cuadrática, con $\epsilon^2 = \delta$. De esta manera tenemos que $(\mathbb{F}_{q^2}, N)$ es un espacio cuadrático.

Podemos describir N a través del conjugado, es decir, si $\alpha + \epsilon\beta \,\varepsilon\, \mathbb{F}_{q^2}$, se define

$$\overline{(\alpha + \epsilon\beta)} = (\alpha - \epsilon\beta)$$

el conjugado de $\alpha + \epsilon\beta$. Luego

$$\begin{array}{rcl} N: & \mathbb{F}_{q^2} & \to \mathbb{F}_q \\ & a + \epsilon b & \rightsquigarrow (\alpha + \epsilon\beta)\overline{(\alpha + \epsilon\beta)} \end{array}$$

Definición 30 *Sea $(\mathcal{V}, Q)$ un espacio cuadrático.*

i) Se dice que Q representa a un elemento α del cuerpo, si existe un vector x en $\mathcal{V}$ tal que $Q(x) = \alpha$, en otras palabras si $\alpha \,\varepsilon\, Q(\mathcal{V})$.

ii) Decimos que Q es universal si $Q(\mathcal{V}) = \mathbb{F}$.

Sea $\alpha \,\varepsilon\, \mathbb{F}$ fijo, definimos

$$B^\alpha(x, y) = \alpha B(x, y) \qquad \forall\, x, y \,\varepsilon\, \mathcal{V},$$

o de otra forma; sea $\mathcal{C} = \{B : \mathcal{V} \times \mathcal{V} \to \mathbb{F} \mid B \text{ es una forma bilineal simétrica}\}$ y consideremos la acción

$$\begin{array}{rccl} \cdot : & \mathbb{F}^* \times \mathcal{C} & \longrightarrow & \mathcal{C} \\ & (\alpha, B) & \rightsquigarrow & B^\alpha \end{array}$$

donde

$$\begin{array}{rccl} B^\alpha : & \mathcal{V} \times \mathcal{V} & \longrightarrow & \mathbb{F} \\ & (x, y) & \rightsquigarrow & B^\alpha(x, y) = \alpha B(x, y) \end{array}$$

Esto provee a $\mathcal{V}$ con una nueva forma bilineal simétrica B^α y una nueva función cuadrática Q^α asociada con B^α. De esta forma $(\mathcal{V}, Q^\alpha)$ es un espacio cuadrático. Al espacio vectorial lo denotamos por $\mathcal{V}^\alpha$.

Cuando hacemos esto, decimos que hemos multiplicado por α el espacio cuadrático.

No debemos confundir la multiplicación por escalar del espacio cuadrático $(\mathcal{V}, Q)$ con la multiplicación por escalar de un vector $x \,\varepsilon\, \mathcal{V}$, es decir, sea $x \,\varepsilon\, \mathcal{V}$ y $\alpha \,\varepsilon\, \mathbb{F}$ entonces

$$Q^\alpha(x) = \alpha\, Q(x), \quad \text{mientras } Q(\alpha x) = \alpha^2 Q(x).$$

Proposición 24 *Sean $B : \mathcal{V} \times \mathcal{V} \to \mathbb{F}$ una forma bilineal simétrica y $\alpha \,\varepsilon\, \mathbb{F}^*$. Entonces*

$$Q^\alpha(\mathcal{V}) = \alpha Q(\mathcal{V})$$

donde Q es la forma cuadrática asociada a B y Q^α la forma cuadrática asociada a B^α.

Demostración. Sea $\alpha \,\varepsilon\, \mathbb{F}^*$. Como $\alpha^{-1} \,\varepsilon\, \mathbb{F}^*$, basta demostrar una sola inclusión.

$\subseteq$) Sea $\beta \,\varepsilon\, Q^\alpha(\mathcal{V})$, entonces $\exists\, y \,\varepsilon\, \mathcal{V}$ tal que $Q^\alpha(y) = \beta$ pero

$$\begin{aligned} \beta &= Q^\alpha(y) \\ &= B^\alpha(y, y) \\ &= \alpha B(y, y) \\ &= \alpha Q(y) \end{aligned}$$

así

$$\beta \ \varepsilon \ \alpha Q(\mathcal{V})$$

Por lo tanto

$$Q^{\alpha}(\mathcal{V}) = \alpha Q(\mathcal{V})$$

■

Proposición 25 *Sean* $(\mathcal{V}', Q')$ *un espacio cuadrático y* $\sigma \ \varepsilon \ L(\mathcal{V}, \mathcal{V}')$. *Se define*

$$\begin{array}{rll} Q: & \mathcal{V} & \to \mathbb{F} \\ & x & \rightsquigarrow Q'(\sigma(x)) \end{array}$$

Entonces $(\mathcal{V}, Q)$ *es un espacio cuadrático, en tal caso decimos que* σ *traslada la forma cuadrática* Q' *a* Q.

Demostración. Basta demostrar que Q es una forma cuadrática. Sean $x, y \ \varepsilon \ \mathcal{V}$ y $\alpha \ \varepsilon \ \mathbb{F}$, entonces

1)

$$\begin{aligned} Q(\alpha x) &= Q'(\sigma(\alpha x)) \\ &= Q'(\alpha\sigma(x)) \\ &= \alpha^2 Q'(\sigma(x)) \\ &= \alpha^2 Q(x) \end{aligned}$$

2)

$$\begin{aligned} Q(x+y) &= Q'(\sigma(x+y)) \\ &= Q'(\sigma(x)+\sigma(y)) \\ &= Q'(\sigma(x)) + Q'(\sigma(y)) + 2B'(\sigma(x), \sigma(y)) \\ &= Q(x) + Q(y) + 2B(x, y) \end{aligned}$$

■

Observación. Si $\sigma \ \varepsilon \ L(\mathcal{V}, \mathcal{V}')$ traslada la forma cuadrática Q' a Q, usando la propiedad

$$Q'(x+y) = Q'(x) + Q'(y) + 2B'(x, y)$$

obtenemos que:

$$Q'(\sigma(x)) = Q(x) \quad \text{y} \quad B'(\sigma(x), \sigma(y)) = B(x, y) \qquad \forall\, x, y \ \varepsilon \ \mathcal{V}$$

luego σ traslada la forma cuadrática Q' y la forma bilineal B'.

Definición 31 *Sean* $(\mathcal{V}, Q)$, $(\mathcal{V}', Q')$ *dos espacios cuadráticos y* $\sigma \; \varepsilon \; L(\mathcal{V}, \mathcal{V}')$. *Se dice que* σ *es una isometría de* $\mathcal{V}$ *en* $\mathcal{V}'$ *si y sólo si*

$$\sigma \text{ es inyectiva y traslada la forma cuadrática } Q' \text{ a } Q$$

Notación.

i) El conjunto de todas las isometrías de $\mathcal{V}$ en $\mathcal{V}'$ se denotará por

$$O(\mathcal{V}, \mathcal{V}')$$

ii) Si $\mathcal{V} \cong \mathcal{V}'$ y la $\dim \mathcal{V} = n$, entonces

$$O(\mathcal{V}, \mathcal{V}') = O_n(\mathcal{V})$$

en este caso diremos que $\mathcal{V}$ y $\mathcal{V}'$ son isométricos.

Proposición 26 $O_n(\mathcal{V})$ *es un subgrupo de* $GL_n(\mathcal{V})$.

Demostración. Como $\mathcal{V} \cong \mathcal{V}'$, toda isometría es invertible, así

$$O_n(\mathcal{V}) \subseteq GL_n(\mathcal{V})$$

más aún, la composición de dos isometrías es una isometría, también lo es la inversa de una isometría.

De esta forma $O_n(\mathcal{V}) \leq GL_n(\mathcal{V})$ (subgrupo).

■

Definición 32 *Este grupo* $O_n(\mathcal{V})$, *es llamado el grupo ortogonal de* $\mathcal{V}$, *con respecto a la forma cuadrática* Q.

Proposición 27 *Sea* α *un escalar no nulo, entonces*

$$O_n(\mathcal{V}) = O_n(\mathcal{V}^\alpha)$$

Demostración. Sea $\sigma \; \varepsilon \; O_n(\mathcal{V}) \Rightarrow Q(\sigma(x)) = Q(x) \; \forall \; x \; \varepsilon \; \mathcal{V}$, entonces

$$\begin{aligned} Q^\alpha(\sigma(x)) &= B^\alpha(\sigma(x), \sigma(x)) \\ &= \alpha B(\sigma(x), \sigma(x)) \\ &= \alpha B(x, x) \\ &= B^\alpha(x, x) \\ &= Q^\alpha(x) \end{aligned}$$

así

$$\sigma \; \varepsilon \; O_n(\mathcal{V}^\alpha)$$

Por lo tanto

$$O_n(\mathcal{V}) \subseteq O_n(\mathcal{V}^\alpha)$$

Recíprocamente, sea $\sigma \,\varepsilon\, O_n(\mathcal{V}^\alpha) \Rightarrow Q^\alpha(\sigma(x)) = Q^\alpha(x)\ \forall\ x \,\varepsilon\, \mathcal{V}$
pero

$$\begin{array}{rll} & Q^\alpha(\sigma(x)) & = Q^\alpha(x) \\ \Leftrightarrow & \alpha B(\sigma(x),\sigma(x)) & = \alpha B(x,x) \text{ como } \alpha \neq 0 \\ \Leftrightarrow & B(\sigma(x),\sigma(x)) & = B(x,x) \\ \Leftrightarrow & Q(\sigma(x)) & = Q(x) \end{array}$$

así

$$\sigma \,\varepsilon\, O_n(\mathcal{V})$$

Por lo tanto

$$O_n(\mathcal{V}^\alpha) \subseteq O_n(\mathcal{V})$$

Finalmente obtenemos que

$$O_n(\mathcal{V}) = O_n(\mathcal{V}^\alpha)$$

■

Proposición 28 *Sean $(\mathcal{V}, Q)$ y $(\mathcal{V}', Q')$ dos espacios cuadráticos, $\sigma \,\varepsilon\, L(\mathcal{V}, \mathcal{V}')$ y sea $\mathcal{B} = \{x_1, x_2, \ldots, x_n\}$ una base para $\mathcal{V}$, tal que*

$$B'(\sigma(x_i), \sigma(x_j)) = B(x_i, x_j) \quad 1 \leq i, j \leq n$$

Entonces σ traslada la forma bilineal.

Demostración. Sea $x \,\varepsilon\, \mathcal{V}$, entonces $x = \sum_i \alpha_i x_i$. Así

$$\begin{aligned} Q'(\sigma(x)) &= Q'\left(\sum_i \alpha_i \sigma(x_i)\right) \\ &= \sum_i \alpha_i^2 Q'(\sigma(x_i)) + 2\sum_{i<j} \alpha_i \alpha_j B'(\sigma(x_i), \sigma(x_j)) \\ &= \sum_i \alpha_i^2 Q(x_i) + 2\sum_{i<j} \alpha_i \alpha_j B(x_i, x_j) \\ &= Q(x) \end{aligned}$$

■

2.2. Matriz Asociada

Sea $(\mathcal{V}, Q)$ un espacio cuadrático de dimensión n y $\mathcal{B} = \{x_1, \ldots, x_n\}$ una base de $\mathcal{V}$. Podemos asociar al espacio cuadrático y a la forma bilineal B asociada a Q, una matriz simétrica N de $n \times n$, la cual en la entrada i, j el coeficiente es $B(x_i, x_j)$.

Llamaremos a $N = (B(x_i, x_j))$, la matriz asociada al espacio cuadrático $(\mathcal{V}, Q)$ o también, la matriz asociada a la forma bilineal B, en la base $\{x_1, \ldots, x_n\}$ y lo denotamos por

$$\mathcal{V} \asymp N \quad \text{en} \quad \mathcal{B}$$

Recíprocamente si $\mathcal{V}$ es un espacio vectorial con base $\mathcal{B} = \{x_1, \ldots, x_n\}$ y si $N = (n_{i\,j})$ es una matriz simétrica de $n \times n$, entonces existe una forma bilineal B con respecto a la cual $\mathcal{V}$ tiene a la matriz N como su matriz asociada en $\mathcal{B}$, la cual se define como

$$B\left(\sum_i \alpha_i\, x_i, \sum_j \beta_j\, x_j\right) = \sum_{i,\,j} \alpha_i \beta_j n_{i\,j}$$

para vectores $\sum\limits_i \alpha_i\, x_i$ y $\sum\limits_j \beta_j\, x_j$ de $\mathcal{V}$.

Si $\mathcal{V} \asymp N'$ en la base $\mathcal{B}' = \{x'_1, \ldots, x'_n\}$ y sea $T = [Id]^{\mathcal{B}}_{\mathcal{B}'}$ la matriz cambio de base, es decir

$$x'_j = \sum_k t_{k\,j}\, x_k$$

Entonces

$$B(x'_i, x'_j) = B\left(\sum_l t_{l\,i}\, x_l, \sum_k t_{k\,j}\, x_k\right) = \sum_{l,\,k} t_{li} B(x_l, x_k) t_{k\,j}$$

Así

$$N' = T^t N T$$

como T es invertible, decimos que N' y N son equivalentes sobre $\mathbb{F}$, lo cual lo denotamos por $N' \equiv N$.

Definición 33 *Dada una matriz simétrica N de $n \times n$, $\langle N \rangle$ denota el espacio cuadrático de dimensión n el cual tiene como matriz asociada a N.*

Observación. Si $\alpha \;\varepsilon\; \mathbb{F}^*$, entonces $\langle \alpha \rangle$ denota la recta, la cual contiene un vector no nulo x para el cual $Q(x) = \alpha$.

Proposición 29 *Sean $(\mathcal{V}, Q)$ y $(\mathcal{V}', Q')$ dos espacios cuadráticos con matrices asociadas M y N respectivamente. Entonces*

$$\mathcal{V} \cong \mathcal{V}' \textit{ si y sólo si } M \equiv N$$

Demostración. Sean $\mathcal{B} = \{x_1, \ldots, x_m\}$, $\mathcal{B}' = \{y_1, \ldots, y_n\}$ bases de $\mathcal{V}$ y $\mathcal{V}'$ respectivamente.

Definamos $M = (a_{ij})$ y $N = (b_{ij})$, donde $B(x_i, x_j) = a_{ij}$ y $B'(y_i, y_j) = b_{ij}$.

Sea $\sigma : \mathcal{V} \to \mathcal{V}'$ una isometría, tal que $\mathcal{V} \cong \mathcal{V}'$, entonces

$$B'(z_i, z_j) = B'(\sigma(x_i), \sigma(x_j)) = B(x_i, x_j) = a_{ij}$$

escribiendo

$$z_i = \sum_k t_{k\,i}\, y_k$$

obtenemos $T = (t_{k\,i}) = [\sigma]_{\mathcal{B}}^{\mathcal{B}'}$ una matriz invertible, entonces

$$a_{ij} = B'(z_i, z_j) = B'\left(\sum_k t_{k\,i}\, y_k, \sum_l t_{l\,j}\, y_l\right) = \sum_{k,\,l} t_{k\,i}\, b_{k\,l}\, t_{l\,j}$$

Así $M = T^t N T$ y por lo tanto $M \equiv N$.

El recíproco es análogo. ∎

Definición 34 *Sean $z_1, \ldots, z_m$ vectores en el espacio cuadrático $(\mathcal{V}, Q)$. El determinante de la matriz $(B(z_i, z_j))$ de $m \times m$ es llamado el discriminante de los vectores $z_1, \ldots, z_m$ y lo denotaremos por*

$$d_B(z_1, \ldots, z_m)$$

De otro modo, tenemos que d_B es una función, dada por

$$\begin{array}{rccl} d_B : & \mathcal{V}^m & \to & \mathbb{F} \\ & (z_1, z_2, \ldots, z_m) & \rightsquigarrow & d_B(z_1, \ldots, z_m) \end{array}$$

Proposición 30 *Sea $\mathcal{B} = \{x_1, \ldots, x_n\}$ una base de $\mathcal{V}$, tal que N es la matriz asociada a $\mathcal{V}$ en esta base, entonces*

$$d_B(x_1, \ldots, x_n) = \det N$$

Demostración. Como N es la matriz asociada de $\mathcal{V}$, es decir, $N = (B(x_i, x_j))$ para $1 \leq i, j \leq n$. Entonces

$$\begin{aligned} d_B(x_1, x_2, \ldots, x_n) &= \det((B(x_i, x_j))) \\ &= \det N \end{aligned}$$

∎

Si consideramos otra base $\{x_1', \ldots, x_n'\}$ de $\mathcal{V}$ y la relación $N' = T^t N T$ obtenemos que

$$\begin{aligned} d_B(x_1', \ldots, x_n') &= \det N' \\ &= \det(T^t N T) \\ &= \alpha^2 d_B(x_1, \ldots, x_n) \end{aligned}$$

para algún $\alpha \,\varepsilon\, \dot{\mathbb{F}} = \{\alpha \,\varepsilon\, \mathbb{F} \mid \alpha \neq 0\}$.

Sea $\dot{\mathbb{F}}^2 = \{\beta \,\varepsilon\, \dot{\mathbb{F}} \mid (\exists \alpha \,\varepsilon\, \dot{\mathbb{F}})(\beta = \alpha^2)\}$ y considerando la función

$$\begin{array}{rcl} \pi: & \mathbb{F} & \to 0 \cup (\dot{\mathbb{F}}/\dot{\mathbb{F}}^2) \\ & \alpha & \rightsquigarrow \quad \overline{\alpha} \end{array}$$

luego

$$\begin{array}{cccccc} d_B: & \mathcal{V}^n & \to & \mathbb{F} & \xrightarrow{\pi} & 0 \cup (\dot{\mathbb{F}}/\dot{\mathbb{F}}^2) \\ & (x'_1, x'_2, \ldots, x'_n) & \rightsquigarrow & \alpha^2 d_B(x_1, x_2, \ldots, x_n) & \rightsquigarrow & \overline{d_B(x_1, x_2, \ldots, x_n)} \end{array}$$

Por lo tanto la proyección de $d_B(x_1, \ldots, x_n)$ en $0 \cup (\dot{\mathbb{F}}/\dot{\mathbb{F}}^2)$ es independiente de la base, esto es llamado el discriminante del espacio cuadrático $(\mathcal{V}, Q)$ y se denota como:

$$d_B\mathcal{V} \quad \text{o} \quad d\mathcal{V}$$

Si $d\mathcal{V} = \alpha$ con $\alpha \,\varepsilon\, \dot{\mathbb{F}}$; esto significa que $d\mathcal{V}$ es la proyección de α en $0 \cup (\dot{\mathbb{F}}/\dot{\mathbb{F}}^2)$. Es equivalente a decir que $\mathcal{V}$ tiene una base $\{x_1, x_2, \ldots, x_n\}$ en la cual

$$d_B(x_1, \ldots, x_n) = \alpha$$

Proposición 31 *Sea N la matriz asociada al espacio cuadrático $(\mathcal{V}, Q)$ y $\alpha \,\varepsilon\, \mathbb{F}$, entonces*

$$\mathcal{V}^\alpha \asymp \alpha N$$

de lo cual obtenemos que $d\mathcal{V}^\alpha = \alpha^n d\mathcal{V}$.

Demostración. Sea $\mathcal{B} = \{x_1, x_2, \ldots, x_n\}$ una base de $\mathcal{V}$, entonces

$$N = (B(x_i, x_j))$$

para $1 \leq i, j \leq n$, donde B es la forma bilineal simétrica asociada al espacio cuadrático $(\mathcal{V}, Q)$. B^α es la forma bilineal simétrica asociada a $\mathcal{V}^\alpha$, entonces

$$B^\alpha(x_i, x_j) = \alpha B(x_i, x_j)$$

así

$$(B^\alpha(x_i, x_j))_{i,j} = (\alpha B(x_i, x_j))_{i,j}$$

de esta forma, αN es la matriz asociada a $\mathcal{V}^\alpha$, además

$$\begin{aligned} d\mathcal{V}^\alpha &= \det(\alpha(B(x_i, x_j))) \\ &= \alpha^n \det((B(x_i, x_j))) \\ &= \alpha^n N \end{aligned}$$

■

Ejemplo 3 *Sean $\{x_1, \ldots, x_m\}$ vectores del espacio cuadrático $(\mathcal{V}, Q)$, si $d_B(x_1, \ldots, x_m) \neq 0$, entonces $\{x_1, \ldots, x_m\}$ son independientes.*

Demostración. Consideremos una combinación lineal a cero, es decir,

$$\sum_{i=1}^{m} \alpha_i x_i = 0$$

entonces

$$0 = B\left(\sum_{i=1}^{m} \alpha_i x_i, x_j\right) = \sum_{i=1}^{m} \alpha_i B(x_i, x_j) \qquad 1 \leq j \leq m$$

Esto es una dependencia entre las filas de la matriz $(B(x_i, x_j))$; tal dependencia es imposible ya que $d_B(x_1, \ldots, x_m) \neq 0$. ■

2.3. Suma Ortogonal

Consideremos el espacio cuadrático $(\mathcal{V}, Q)$ y la asociada forma bilineal simétrica B.

Definición 35 *Sean X e Y dos subconjuntos de $\mathcal{V}$.*

i) Se define

$$B(X, Y) = \{B(x, y) \mid x \,\varepsilon\, X \,, y \,\varepsilon\, Y\}$$

ii) Diremos que X e Y son ortogonales si

$$B(X, Y) = \{0\}$$

Análogamente si $x, y \,\varepsilon\, \mathcal{V}$, se dice que son ortogonales si y sólo si

$$B(x, y) = 0$$

Notación.

1) $B(x, \mathcal{W}) = \{B(x, z) \mid z \,\varepsilon\, \mathcal{W}\}$

2) $B(x, \mathcal{W}) = \{0\}$, entonces $B(x, \mathcal{W}) = 0$

Definición 36 *Decimos que $\mathcal{V}$ tiene una suma ortogonal en subespacios $\mathcal{V}_1, \ldots, \mathcal{V}_r$, si cumple lo siguiente:*

1) $\mathcal{V} = \mathcal{V}_1 \oplus \cdots \oplus \mathcal{V}_r$

2) Los $\mathcal{V}_i$ son ortogonales dos a dos, es decir,

$$B(\mathcal{V}_i, \mathcal{V}_j) = 0 \quad \textit{para} \quad 1 \leq i < j \leq r$$

Esta suma ortogonal la denotaremos como:

$$\mathcal{V} = \mathcal{V}_1 \perp \cdots \perp \mathcal{V}_r$$

Llamaremos a los $\mathcal{V}_i$ los componentes de la suma ortogonal o simplemente, sumandos ortogonales. Formalmente definiremos

$$\underset{\phi}{\perp} \mathcal{V}_i = 0$$

donde ϕ denota el conjunto vacío.

Proposición 32 *Sea $(\mathcal{V}, Q)$ un espacio cuadrático, tal que $\mathcal{V} = \mathcal{U} \perp \mathcal{W}$, entonces*

$$\dim \mathcal{V} = \dim \mathcal{U} + \dim \mathcal{W}$$

Proposición 33 *Sea $(\mathcal{V}, Q)$ un espacio cuadrático, tal que $\mathcal{V} = \mathcal{V}_1 \perp \mathcal{V}_2 \perp \cdots \perp \mathcal{V}_r$, entonces*

$$d_B(\mathcal{V}) = d\mathcal{V}_1 d\mathcal{V}_2 \cdots d\mathcal{V}_r$$

Demostración. Sean $\mathcal{C}_1, \ldots, \mathcal{C}_r$ bases de $\mathcal{V}_1, \ldots, \mathcal{V}_r$ respectivamente, entonces $\mathcal{C} = \mathcal{C}_1 \cup \cdots \cup \mathcal{C}_r$ es una base de $\mathcal{V}$, la cual consideramos ordenada, luego

$$d_B(\mathcal{V}) = det((B(x_i, x_j))) \qquad \text{con } x_i, x_j \,\varepsilon\, \mathcal{C}$$

como los $\mathcal{V}_i$ son ortogonales dos a dos, la matriz $(B(x_i, x_j))$ tiene la siguiente forma:

$$\left(\begin{array}{c|c|c|c} (B(x_i^1, x_j^1)) & 0 & 0 & 0 \\ \hline 0 & (B(x_i^2, x_j^2)) & 0 & 0 \\ \hline 0 & 0 & \ddots & 0 \\ \hline 0 & 0 & 0 & (B(x_i^r, x_j^r)) \end{array}\right)$$

donde los elementos $x_k^i \,\varepsilon\, \mathcal{C}_i$. Por lo tanto

$$\begin{aligned} det((B(x_i, x_j))) &= det(B(x_i^1, x_j^1)) det(B(x_i^2, x_j^2)) \cdots det(B(x_i^r, x_j^r)) \\ &= d\mathcal{V}_1 d\mathcal{V}_2 \cdots d\mathcal{V}_r \end{aligned}$$

■

la multiplicación esta dada por supuesto en $0 \cup (\dot{\mathbb{F}}/\dot{\mathbb{F}}^2)$.

Proposición 34 *Sean $(\mathcal{V}_1, Q_1), (\mathcal{V}_2, Q_2), \ldots, (\mathcal{V}_r, Q_r)$ espacios cuadráticos, entonces existe un espacio cuadrático $(\mathcal{V}, Q)$, tal que*

$$\mathcal{V} = \mathcal{V}_1 \perp \mathcal{V}_2 \perp \cdots \perp \mathcal{V}_r$$

Demostración. Consideremos $\mathcal{V} = \overset{r}{\underset{i=1}{\times}} \mathcal{V}_i$ y definamos una forma bilineal para $\mathcal{V}$ de la siguiente forma:

$$\begin{aligned} B: \ \mathcal{V} \times \mathcal{V} &\to \mathbb{F} \\ (x,y) &\rightsquigarrow \sum_{i=1}^{r} B_i(x_i, y_i) \end{aligned}$$

donde $x = (x_1, x_2, \ldots, x_r), y = (y_1, y_2, \ldots, y_r)$, con $x_i, y_i \ \varepsilon \ \mathcal{V}_i$ y $1 \leq i \leq r$, además sean $B_1, B_2, \ldots, B_r$ las respectivas formas bilineales de $\mathcal{V}_1, \mathcal{V}_2, \ldots, \mathcal{V}_r$ respectivamente. Probemos que B es una forma bilineal de $\mathcal{V}$, para esto, sean $x, y, z \ \varepsilon \ \mathcal{V}$ y $\alpha \ \varepsilon \ \mathbb{F}$, entonces

a)

$$\begin{aligned} B(x+y,z) &= B\left((x_1, x_2, \ldots, x_r) + (y_1, y_2, \ldots, y_r), (z_1, z_2, \ldots, z_r)\right) \\ &= B\left((x_1 + y_1, x_2 + y_2, \ldots, x_r + y_r), (z_1, z_2, \ldots, z_r)\right) \\ &= \sum_{i=1}^{r} B_i(x_i + y_i, z_i) \\ &= \sum_{i=1}^{r} B_i(x_i, z_i) + B_i(y_i, z_i) \\ &= B(x,z) + B(y,z) \end{aligned}$$

b)

$$\begin{aligned} B(x,y+z) &= B\left((x_1, x_2, \ldots, x_r), (y_1, y_2, \ldots, y_r) + (z_1, z_2, \ldots, z_r)\right) \\ &= B\left((x_1, x_2, \ldots, x_r), (y_1 + z_1, y_2 + z_2, \ldots, y_r + z_r)\right) \\ &= \sum_{i=1}^{r} B_i(x_i, y_i + z_i) \\ &= \sum_{i=1}^{r} B_i(x_i, y_i) + B_i(x_i, z_i) \\ &= B(x,y) + B(x,z) \end{aligned}$$

c)

$$\begin{aligned} B(\alpha x, y) &= B\left(\alpha(x_1, x_2, \ldots, x_r), (y_1, y_2, \ldots, y_r)\right) \\ &= B\left((\alpha x_1, \alpha x_2, \ldots, \alpha x_r), (y_1, y_2, \ldots, y_r)\right) \\ &= \sum_{i=1}^{r} B_i(\alpha x_i, y_i) \\ &= \alpha \sum_{i=1}^{r} B_i(x_i, y_i) \\ &= \alpha B(x,y) \end{aligned}$$

d)

$$\begin{aligned} B(x,y) &= B\left((x_1,x_2,\ldots,x_r),(y_1,y_2,\ldots,y_r)\right)\\ &= \sum_{i=1}^{r} B_i(x_i,y_i)\\ &= \sum_{i=1}^{r} B_i(y_i,x_i)\\ &= B\left((y_1,y_2,\ldots,y_r),(x_1,x_2,\ldots,x_r)\right)\\ &= B(y,x) \end{aligned}$$

por lo tanto B es una forma bilineal.

Por la definición de B, tenemos que $B(x_i,x_j)=0$ para $1\le i<j\le r$.

Como $\mathop{\times}\limits_{i=1}^{r}\mathcal{V}_i \cong \bigoplus\limits_{i=1}^{r}\mathcal{V}_i$, cuando r es finito, entonces

$$\mathcal{V}=\mathcal{V}_1\perp\mathcal{V}_2\perp\cdots\perp\mathcal{V}_r$$

Con

$$\begin{array}{rcl} Q: & \mathcal{V} & \to \mathbb{F}\\ & (x_1,x_2,\ldots,x_r) & \rightsquigarrow \displaystyle\sum_{i=1}^{r} Q_i(x_i) \end{array}$$

la respectiva forma cuadrática asociada a $\mathcal{V}$. ■

Ejemplo 4 *Sean M y N dos matrices simétricas sobre $\mathbb{F}$ y definamos*

$$\mathcal{V}=\langle M\rangle\perp\langle N\rangle$$

luego, $\mathcal{V}$ es un espacio cuadrático con una base en la cual

$$\mathcal{V}\asymp\left(\begin{array}{c|c} M & 0\\ \hline 0 & N\end{array}\right)$$

Similarmente

$$\mathcal{V}\asymp\langle\alpha_1\rangle\perp\cdots\perp\langle\alpha_n\rangle$$

con todos los α_i en $\mathbb{F}$, de manera que $\mathcal{V}$ tiene una base $\{x_1,\ldots,x_n\}$ en la cual $Q(x_i)=\alpha_i$ para $1\le i\le n$ y $B(x_i,x_j)=0$ para $1\le i<j\le n$ y su matriz asociada es:

$$\left(\begin{array}{c|c|c|c|c|c} \alpha_1 & 0 & 0 & 0 & \cdots & 0\\ \hline 0 & \alpha_2 & 0 & 0 & \cdots & 0\\ \hline 0 & 0 & \alpha_3 & 0 & \cdots & 0\\ \hline \vdots & \vdots & \vdots & \ddots & \cdots & \vdots\\ \hline \vdots & \vdots & \vdots & \vdots & \ddots & \vdots\\ \hline 0 & 0 & 0 & 0 & 0 & \alpha_n \end{array}\right)$$

Definición 37 *Sea $\mathcal{B} = \{x_1, \ldots, x_n\}$ una base del espacio cuadrático $(\mathcal{V}, Q)$.*
Se dice que $\mathcal{B}$ es una base ortogonal si y sólo si

$$B(x_i, x_j) = 0 \qquad para \qquad 1 \leq i < j \leq n$$

Ejemplo 5 *Sea $(\mathcal{V}, Q)$ un espacio cuadrático y $\mathcal{B} = \{x_1, x_2, \ldots, x_n\}$ una base de $\mathcal{V}$, tal que $Q(\mathcal{V}) = 0$, es decir, $Q(x) = 0$ para todo $x \,\varepsilon\, \mathcal{V}$, entonces*

$$\begin{aligned} B(x_i, x_j) &= \frac{1}{2}(Q(x_i + x_j) - Q(x_i) - Q(x_j)) \\ &= 0 \end{aligned}$$

de aquí obtenemos que $B(x_i, x_j) = 0$ para $1 \leq i < j \leq n$. Por lo tanto $\mathcal{B}$ es una base ortogonal de $\mathcal{V}$.

Proposición 35 *Todo espacio cuadrático tiene una base ortogonal.*

Demostración. La demostración se hará por inducción en la dimensión de $\mathcal{V}$.

1) Si $Q(\mathcal{V}) = 0$, es el ejemplo anterior.

2) Sea $Q(\mathcal{V}) \neq 0$, podemos escoger $x \,\varepsilon\, \mathcal{V}$ con $Q(x) \neq 0$ y completamos $\{x, x_2, \ldots, x_n\}$ a una base de $\mathcal{V}$. Así tenemos que

$$\left\{x, x_2 - \frac{B(x, x_2)}{Q(x)}x, \ldots, x_n - \frac{B(x, x_n)}{Q(x)}x\right\}$$

es también una base de $\mathcal{V}$.
Sea $\mathcal{W} = \left\langle x_2 - \frac{B(x, x_2)}{Q(x)}x, \ldots, x_n - \frac{B(x, x_n)}{Q(x)}x \right\rangle$ un subespacio de $\mathcal{V}$ de dimensión $n-1$, de donde obtenemos que $B(x, \mathcal{W}) = 0$, en efecto

$$\begin{aligned} B(x, \mathcal{W}) &= B\left(x, \alpha_1\left(x_2 - \frac{B(x, x_2)}{Q(x)}x\right) + \ldots + \alpha_{n-1}\left(x_n - \frac{B(x, x_n)}{Q(x)}x\right)\right) \\ &= \alpha_1 B\left(x, x_2 - \frac{B(x, x_2)}{Q(x)}x\right) + \cdots + \alpha_{n-1} B\left(x, x_n - \frac{B(x, x_n)}{Q(x)}x\right) \\ &= \alpha_1(B(x, x_2) - B(x, x_2)) + \cdots + \alpha_{n-1}(B(x, x_n) - B(x, x_n)) \\ &= 0 \end{aligned}$$

Por hipótesis de inducción en $\mathcal{W}$, obtenemos que esta base es una base ortogonal.

■

Observación.

1) Sean $(\mathcal{V}, Q) = \overset{r}{\underset{i=1}{\perp}} \mathcal{V}_i$ y $(\mathcal{V}', Q')$ dos espacios cuadráticos, con
$$\sigma : \mathcal{V} \to \mathcal{V}'$$
una transformación lineal, entonces se define σ_i como la restricción de σ a $\mathcal{V}_i$, es decir
$$\sigma\mid_{\mathcal{V}_i} = \sigma_i : \mathcal{V}_i \to \sigma(\mathcal{V}_i)$$

2) Sea $(\mathcal{V}, Q) = \overset{r}{\underset{i=1}{\perp}} \mathcal{V}_i$ un espacio cuadrático, entonces $(\mathcal{V}_i, Q_i)$ es un espacio cuadrático para $1 \leq i \leq r$, donde
$$Q_i = Q\mid_{\mathcal{V}_i} : \mathcal{V}_i \to \mathbb{F}$$

Proposición 36 *Sean $(\mathcal{V}, Q) = \mathcal{V}_1 \perp \cdots \perp \mathcal{V}_r$ y $(\mathcal{V}', Q') = \mathcal{V}_1' + \cdots + \mathcal{V}_r'$ dos espacios cuadráticos, con los subespacios $\mathcal{V}_i'$ ortogonales dos a dos, (no necesariamente asumimos que los $\mathcal{V}_i'$ son una suma ortogonal de $\mathcal{V}'$).*

Si $\sigma_i : \mathcal{V}_i \to \mathcal{V}_i'$ traslada la forma cuadrática. Entonces existe una única $\sigma : \mathcal{V} \to \mathcal{V}'$ que traslada la forma cuadrática, la cual concuerda con cada σ_i.

Demostración. Sea $\mathcal{B}_i = \{x_1^i, x_2^i, \ldots, x_{s^i}^i\}$ una base de $\mathcal{V}_i$, así
$$\mathcal{B} = \{x_1^1, x_2^1, \ldots, x_{s^1}^1, x_1^2, x_2^2, \ldots, x_{s^2}^2, \ldots, x_1^r, x_2^r, \ldots, x_{s^r}^r\}$$
es una base de $\mathcal{V}$ y
$$\begin{array}{rccl} \sigma : & \mathcal{V} & \to & \mathcal{V}' \\ & \sum_{i=1}^{r} x_i & \rightsquigarrow & \sum_{i=1}^{r} \sigma_i(x_i) \end{array}$$
es una función. Notemos que σ está bien definida, ya que basta definirla en los elementos de la base, dada por
$$\begin{array}{ccc} \mathcal{V} & \to & \mathcal{V}' \\ x_j^i & \rightsquigarrow & \sigma_i(x_j^i) \end{array}$$
y se extiende de manera única, linealmente. Además
$$\begin{aligned} Q'(\sigma(x)) &= Q'(\sigma\left(\sum x_i\right)) \\ &= Q'(\sum \sigma(x_i)) \\ &= Q'(\sum \sigma_i(x_i)) \\ &= \sum Q'(\sigma_i(x_i)) \\ &= \sum Q(x) \\ &= Q(x) \end{aligned}$$

■

Notación. La función construida en la Proposición anterior, se denotará por

$$\sigma = \sigma_1 \perp \cdots \perp \sigma_r$$

El caso importante es donde $\mathcal{V} = \mathcal{V}'$, $\mathcal{V}_i = \mathcal{V}_i'$ y todas las σ_i están en $O(\mathcal{V}_i)$, en este caso

$$\sigma_1 \perp \cdots \perp \sigma_r \,\varepsilon\, O(\mathcal{V})$$

Proposición 37 *Sean* $\sigma = \sigma_1 \perp \sigma_2 \perp \cdots \perp \sigma_r, \tau = \tau_1 \perp \tau_2 \perp \cdots \perp \tau_r \,\varepsilon\, O(\mathcal{V})$, *entonces*

$$\begin{aligned} \sigma \circ \tau &= (\sigma_1 \circ \tau_1) \perp \cdots \perp (\sigma_r \circ \tau_r) \\ \sigma^{-1} &= \sigma_1^{-1} \perp \cdots \perp \sigma_r^{-1} \\ \det \sigma &= \det \sigma_1 \det \sigma_2 \cdots \det \sigma_r \end{aligned}$$

2.4. Complementos Ortogonales

Definición 38 *Sea* $\mathcal{U}$ *un subespacio del espacio cuadrático* $(\mathcal{V}, Q)$. *Se define el complemento ortogonal de* $\mathcal{U}$ *como el subespacio*

$$\mathcal{U}^{\perp} = \{x \,\varepsilon\, \mathcal{V} \mid \forall\, y \,\varepsilon\, \mathcal{U},\ B(x,y) = 0\}$$

El radical de $\mathcal{V}$ *es el subespacio*

$$rad\,\mathcal{V} = \{x \,\varepsilon\, \mathcal{V} \mid \forall\, z \,\varepsilon\, \mathcal{V},\ B(x,z) = 0\}$$

Así el $rad\,\mathcal{V} = \mathcal{V}^{\perp}$.

Ejemplo 6 *Sea*

$$\begin{array}{rcl} Q: & \mathbb{F}^2 & \to \mathbb{F} \\ & (x,y) & \rightsquigarrow x^2 \end{array}$$

una forma cuadrática de $\mathbb{F}^2$. *Entonces*

$$\begin{array}{rcl} B: & \mathbb{F}^2 \times \mathbb{F}^2 & \to \mathbb{F} \\ & ((x,y),(a,b)) & \rightsquigarrow xa \end{array}$$

es la forma bilineal asociada a Q. *Así*

$$\begin{aligned} rad\,\mathcal{V} &= \{(x,y) \,\varepsilon\, \mathbb{F}^2 \mid B((x,y),(a,b)) = 0, \forall (a,b) \,\varepsilon\, \mathbb{F}^2\} \\ &= \{(x,y) \,\varepsilon\, \mathbb{F}^2 \mid xa = 0, \forall a \,\varepsilon\, \mathbb{F}\} \\ &= <(0,1)> \end{aligned}$$

Definición 39 *Diremos que* $(\mathcal{V}, Q)$ *es un espacio cuadrático regular si* $rad\,\mathcal{V} = \{0\}$.

Proposición 38 *Sea $(\mathcal{V}, Q)$ un espacio cuadrático, que es una suma de subespacios ortogonales dos a dos, es decir, $\mathcal{V} = \mathcal{V}_1 + \cdots + \mathcal{V}_r$ con $B(\mathcal{V}_i, \mathcal{V}_j) = 0$ para $1 \leq i < j \leq r$. Entonces*

$$rad\,\mathcal{V} = rad\,\mathcal{V}_1 + \cdots + rad\,\mathcal{V}_r$$

Demostración. Sea $x \,\varepsilon\, rad\,\mathcal{V}$ y lo escribimos como $x = \sum x_i$ con cada $x_i \,\varepsilon\, \mathcal{V}_i$. Entonces para $(1 \leq i \leq r)$ tenemos

$$B(x_i, \mathcal{V}_i) = B(\Sigma\, x_j, \mathcal{V}_i) \subseteq B(x, \mathcal{V}) = 0$$

así $x_i \,\varepsilon\, rad\,\mathcal{V}_i$, por lo tanto $x \,\varepsilon\, \sum rad\,\mathcal{V}_i$.

En el otro sentido, si tomamos $x = \sum x_i$ con cada $x_i \,\varepsilon\, rad\,\mathcal{V}_i$ tenemos

$$B(x, \mathcal{V}) \subseteq B(x_1, \mathcal{V}_1) + \cdots + B(x_r, \mathcal{V}_r) = 0$$

de manera que $x \,\varepsilon\, rad\,\mathcal{V}$. ■

Corolario 3 *$\mathcal{V}$ es regular si y sólo si todos los $\mathcal{V}_i$ son regulares.*

Corolario 4 *Si $\mathcal{V}$ es regular, entonces $\mathcal{V} = \mathcal{V}_1 \perp \cdots \perp \mathcal{V}_r$.*

Demostración. Sólo es necesario mostrar que la suma es directa. Así que tomemos $x_1 + \cdots + x_r = 0$ con $x_i \,\varepsilon\, \mathcal{V}_i$ para $1 \leq i \leq r$. Entonces

$$0 = B(x_1 + \cdots + x_r, \mathcal{V}_i) = B(x_i, \mathcal{V}_i)$$

Por lo tanto $x_i \,\varepsilon\, rad\,\mathcal{V}_i = 0$, así $x_i = 0$. ■

Proposición 39 *Sea $(\mathcal{V}, Q)$ un espacio cuadrático. $\mathcal{V}$ es regular si y sólo si $d\mathcal{V} \neq 0$.*

Demostración. Sea $\mathcal{B} = \{x_1, x_2, \ldots, x_n\}$ una base ortogonal de $\mathcal{V}$ y consideremos

$$\mathcal{V} = < x_1 > \perp \cdots \perp < x_n >$$

Entonces

$$\begin{aligned} d\mathcal{V} &= d(< x_1 > \perp < x_2 > \perp \cdots \perp < x_n >) \\ &= d(< x_1 >) d(< x_2 >) \cdots d(< x_n >) \\ &= Q(x_1) Q(x_2) \cdots Q(x_n) \\ &\neq 0 \end{aligned}$$

ya que $Q(x_i) \neq 0$ para $1 \leq i \leq n$.

En el otro sentido, si $d\mathcal{V} \neq 0$, entonces $rad < x_i >= 0$ para $1 \leq i \leq n$. De esta manera

$$\begin{aligned} rad\,\mathcal{V} &= rad < x_1 > + rad < x_2 > + \cdots + rad < x_n > \\ &= 0 \end{aligned}$$

por lo tanto $\mathcal{V}$ es regular. ■

Proposición 40 *Sea $\mathcal{U}$ un subespacio regular del espacio cuadrático $(\mathcal{V}, Q)$. Entonces $\mathcal{U}$ es un sumando ortogonal de $\mathcal{V}$, es decir, $\mathcal{V} = \mathcal{U} \perp \mathcal{U}^{\perp}$. Además si $\mathcal{V} = \mathcal{U} \perp \mathcal{W}$ es cualquier otra suma ortogonal, entonces $\mathcal{W} = \mathcal{U}^{\perp}$.*

Demostración. Sea $\mathcal{B} = \{x_1, x_2, \ldots, x_r\}$ una base ortogonal de $\mathcal{U}$, entonces

$$\mathcal{U} =< x_1 >\perp \cdots \perp< x_r >$$

Ya que $\mathcal{U}$ es regular, todos los $Q(x_i) \neq 0$. Sea $z \,\varepsilon\, \mathcal{V}$.

Se define

$$y = \frac{B(z, x_1)}{Q(x_1)} x_1 + \cdots + \frac{B(z, x_r)}{Q(x_r)} x_r, \ \varepsilon\, \mathcal{U}$$

y consideramos

$$w = z - y$$

veamos que $w \,\varepsilon\, \mathcal{U}^{\perp}$, para ello calculemos $B(w, x_i)$ para $1 \leq i \leq r$, así

$$\begin{aligned} B(w, x_i) &= B(z - y, x_i) \\ &= B(z, x_i) - B\left(\frac{B(z, x_1)}{Q(x_1)} x_1 + \cdots + \frac{B(z, x_r)}{Q(x_r)} x_r, x_i\right) \\ &= B(z, x_i) - B(\frac{B(z, x_i)}{Q(x_i)} x_i, x_i) \\ &= B(z, x_i) - \frac{B(z, x_i)}{Q(x_i)} B(x_i, x_i) \\ &= 0 \end{aligned}$$

de aquí que $w \,\varepsilon\, \mathcal{U}^{\perp}$.

Por lo tanto $z = y - w$, así $V = \mathcal{U} + \mathcal{U}^{\perp}$.

Ahora $\mathcal{U} \cap \mathcal{U}^{\perp} = rad\, \mathcal{U} = 0$. De esta manera $\mathcal{V} = \mathcal{U} \oplus \mathcal{U}^{\perp}$. Por lo tanto $\mathcal{V} = \mathcal{U} \perp \mathcal{U}^{\perp}$.

Si $\mathcal{V} = \mathcal{U} \perp \mathcal{W}$, entonces $\mathcal{W} \subseteq \mathcal{U}^{\perp}$. Pero tenemos que $\mathcal{V} = \mathcal{U} \perp \mathcal{U}^{\perp}$. De aquí que $\dim \mathcal{W} = \dim \mathcal{U}^{\perp}$. Por lo tanto $\mathcal{W} = \mathcal{U}^{\perp}$. ■

Lema 1 *Sea $\mathcal{U}$ un subespacio de un espacio cuadrático regular $(\mathcal{V}, Q)$. Entonces*

$$(\mathcal{U}^{\perp})^{\perp} = \mathcal{U}$$

Demostración. Sea $\mathcal{W}$ un subespacio de $\mathcal{V}$, tal que $\mathcal{V} = \mathcal{U} \perp \mathcal{W}$. Como $\mathcal{V}$ es regular entonces $\mathcal{U}$ y $\mathcal{W}$ también lo son. Así $\mathcal{W} = \mathcal{U}^{\perp}$, de esta manera

$$\mathcal{V} = \mathcal{U} \perp \mathcal{U}^{\perp}$$

lo mismo sucede para $\mathcal{W}$, es decir $\mathcal{V} = \mathcal{W} \perp \mathcal{W}^{\perp}$ y como $\mathcal{W} = \mathcal{U}^{\perp}$, por lo tanto

$$(\mathcal{U}^{\perp})^{\perp} = \mathcal{U}$$

■

Proposición 41 *Sean* $(\mathcal{V}, Q)$ *un espacio cuadrático y* $\mathcal{U}, \mathcal{W}$ *subespacios de* $\mathcal{V}$*, tal que* $\mathcal{U} \subset \mathcal{W}$*. Entonces* $\mathcal{W}^{\perp} \subset \mathcal{U}^{\perp}$*.*

Demostración. Sea $w \,\varepsilon\, \mathcal{W}^{\perp}$, entonces $B(w, z) = 0$ para todo $z \,\varepsilon\, \mathcal{W}$. En particular para $z \,\varepsilon\, \mathcal{U}$, por lo tanto

$$B(w, z) = 0 \qquad \forall\, z \,\varepsilon\, \mathcal{U}$$

así $w \,\varepsilon\, \mathcal{U}^{\perp}$. ■

Proposición 42 *Sea* B *la forma bilineal del espacio cuadrático regular* $(\mathcal{V}, Q)$ *y sea* $\mathcal{V}^* = L(\mathcal{V}, \mathbb{F})$ *el espacio dual de* $\mathcal{V}$*, entonces existe un isomorfismo* φ *de* $\mathcal{V}$ *en* $\mathcal{V}^*$*.*

Demostración. Sea $x \,\varepsilon\, \mathcal{V}$, entonces

$$\varphi_x(y) = B(x, y)$$

define una forma lineal $\varphi_x : \mathcal{V} \to \mathbb{F}$. Así φ_x está en el espacio dual $\mathcal{V}^*$. Por lo tanto

$$\begin{array}{rccl} \varphi : & \mathcal{V} & \longrightarrow & \mathcal{V}^* \\ & x & \rightsquigarrow & \varphi_x \end{array}$$

es un isomorfismo. ■

Sea $\{x_1, \ldots, x_n\}$ una base de $\mathcal{V}$, entonces $\{x_1^*, x_2^*, \ldots, x_n^*\}$ es la base dual de $\{x_1, x_2, \ldots, x_n\}$ en $\mathcal{V}^*$, dada por:

$$\begin{array}{rcl} x_j^* : & \mathcal{V} & \to \mathbb{F} \\ & x_i & \rightsquigarrow x_j^*(x_i) = \left\{ \begin{array}{ll} 1 & i = j \\ 0 & i \neq j \end{array} \right. \end{array}$$

Si aplicamos φ^{-1} a esta base dual obtenemos una base $\{y_1, \ldots, y_n\}$ para $\mathcal{V}$ con la propiedad que

$$B(x_i, y_j) = \delta_{ij} \qquad \text{(Delta de Kronecker)}$$

en efecto, como $y_j = \varphi^{-1}(x_j^*)$, entonces

$$\begin{array}{rcll} y_j & = & \varphi^{-1}(x_j^*) & /\varphi \\ \varphi_{y_j} & = & x_j^* & /x_i \\ \varphi_{y_j}(x_i) & = & x_j^*(x_i) & \\ B(y_j, x_i) & = & \delta_{i\,j} & \\ B(x_i, y_j) & = & \delta_{i\,j} & \end{array}$$

Más aún, esta base es única.

Corolario 5 *Sea* $\mathcal{W}$ *un subespacio de un espacio cuadrático regular* $(\mathcal{V}, Q)$*, entonces*

$$\dim \mathcal{V} = \dim \mathcal{W} + \dim \mathcal{W}^{\perp}$$

Demostración. Sea $\mathcal{B} = \{x_1, x_2, \ldots, x_r\}$ una base de $\mathcal{W}$, luego $\mathcal{C} = \{x_1, x_2, \ldots, x_n\}$ es una base de $\mathcal{V}$, por lo tanto existe $\{y_1, y_2, \ldots, y_n\}$ tal que

$$B(x_i, y_j) = \delta_{ij}$$

entonces $\mathcal{W}^{\perp} =< y_{r+1}, \ldots, y_n >$, en efecto

sea $z = \sum_{i=1}^{n} \alpha_i y_i$, entonces

$$\begin{aligned} 0 &= B(x_i, z) \\ &= \alpha_j \qquad\qquad 1 \leq j \leq r \end{aligned}$$

por lo tanto $z\, \varepsilon\ < y_{r+1}, \ldots, y_n >$. ■

Ejemplo 7 *Sean $(\mathcal{V}, Q)$ un espacio cuadrático regular, N la matriz de $\mathcal{V}$ en la base $\mathcal{B} = \{x_1, \ldots, x_n\}$ y M la matriz de $\mathcal{V}$ en la base $\mathcal{C} = \{y_1, \ldots, y_n\}$, tal que $B(x_i, y_j) = \delta_{i\,j}$. Entonces $M = N^{-1}$.*

Demostración. Por 2.2 tenemos que $M = T^t N T$ donde $T = (t_{ij})$ con $1 \leq i, j \leq n$, es la matriz cambio base, es decir $y_i = \sum_j t_{j\,i} x_j$. Si $NT = (c_{i\,j})$ con $1 \leq i, j \leq n$, entonces

$$\begin{aligned} c_{i\,j} &= \sum_{k=1}^{n} n_{i\,k} t_{k_j} \\ &= \sum_{k=1}^{n} B(x_i, x_k) t_{k\,j} \\ &= \sum_{k=1}^{n} B(x_i, t_{k\,j} x_k) \\ &= B\left(x_i, \sum_{k=1}^{n} t_{k\,j} x_k\right) \\ &= B(x_i, y_j) \\ &= \delta_{i\,j} \end{aligned}$$

de esta manera, NT es la matriz identidad. De aquí $M = T^t$. Por lo tanto $M = MNM$. Así $M = N^{-1}$. ■

2.5. Suma Radical

Sea $(\mathcal{V}, Q)$ un espacio cuadrático y $\mathcal{U}$ un subespacio de $\mathcal{V}$.

Lema 2 *Si $\mathcal{V} = \mathcal{U} \oplus rad\mathcal{V}$, entonces $\mathcal{V} = \mathcal{U} \perp rad\mathcal{V}$.*

Demostración. Basta demostrar que $\mathcal{U}$ y $rad\mathcal{V}$ son ortogonales, para esto, sea $y \,\varepsilon\, rad\mathcal{V}$, entonces

$$B(y,x)=0 \quad \forall x \,\varepsilon\, \mathcal{V}$$

en particular para $x \,\varepsilon\, \mathcal{U}$. Por lo tanto $\mathcal{V}=\mathcal{U}\perp rad\mathcal{V}$. ■

Definición 40 *A la suma ortogonal anterior la llamaremos suma radical de $\mathcal{V}$.*

Además, $\mathcal{U}$ no es único a menos que $\mathcal{V}$ sea regular, pero veremos en la Proposición 45 que es siempre único bajo una isometría.

Ejemplo 8 *Sea*

$$\begin{array}{rcl} Q: & \mathbb{R}^2 & \to \mathbb{R} \\ & (x,y) & \rightsquigarrow x^2 \end{array}$$

una forma cuadrática de $\mathbb{R}^2$ y la forma bilineal simétrica asociada es:

$$\begin{array}{rcl} B: & \mathbb{R}^2\times\mathbb{R}^2 & \to \mathbb{R} \\ & ((x,y),(a,b)) & \rightsquigarrow xa \end{array}$$

Es fácil obtener que rad $\mathbb{R}^2 =<(0,1)>$. Por lo tanto $\mathbb{R}^2 =<(1,\alpha)>\oplus<(0,1)>$ con $\alpha \,\varepsilon\, \mathbb{R}$. Con lo cual, $\mathcal{U}$ de la Proposición siguiente, no es único.

Proposición 43 *Sea $(\mathcal{V},Q)$ un espacio cuadrático y $\mathcal{U}$ un subespacio de $\mathcal{V}$, tal que $\mathcal{V}=\mathcal{U}\perp rad\,\mathcal{V}$, entonces $\mathcal{U}$ es regular.*

Demostración. Como $\mathcal{V}=\mathcal{U}\perp rad\,\mathcal{V}$, entonces

$$\begin{aligned} rad\,\mathcal{V} &= rad\,\mathcal{U}+rad\,(rad\,\mathcal{V}) \\ rad\,\mathcal{V} &= rad\,\mathcal{U}+rad\,\mathcal{V} \\ 0 &= rad\,\mathcal{U} \end{aligned}$$

por lo tanto $\mathcal{U}$ es regular. ■

Proposición 44 *Sean $(\mathcal{V},Q)$, $(\mathcal{V}',Q')$ dos espacios cuadráticos, tal que $\sigma \,\varepsilon\, L(\mathcal{V},\mathcal{V}')$ traslada la forma cuadrática. Si $\mathcal{V}$ es regular, entonces σ es una isometría.*

Demostración. Tomemos x en el kernel de σ. Entonces

$$B(x,\mathcal{V})=B'(\sigma(x),\sigma(\mathcal{V}))=0$$

Así $x \,\varepsilon\, rad\,\mathcal{V}$. Por lo tanto $x=0$. ■

Proposición 45 *Sea $\mathcal{V}=\mathcal{U}\perp rad\,\mathcal{V}$ y $\mathcal{V}'=\mathcal{U}'\perp rad\,\mathcal{V}'$ la suma radical de los espacios cuadráticos $(\mathcal{V},Q)$ y $(\mathcal{V}',Q')$. Entonces*

$$\mathcal{V}\cong\mathcal{V}' \text{ si y sólo si } \mathcal{U}\cong\mathcal{U}' \text{ con } rad\,\mathcal{V}\cong rad\,\mathcal{V}'$$

Demostración. Sean $\sigma:\mathcal{V}\to\mathcal{V}'$ una isometría, $x \,\varepsilon\, rad\,\mathcal{V}$ y $y \,\varepsilon\, \mathcal{V}$, entonces

$$\begin{aligned} 0 &= B(x,y) \\ &= B(\sigma(x),\sigma(y)) \end{aligned}$$

por lo tanto $\sigma(x) \,\varepsilon\, rad\,\mathcal{V}'$, de esta manera $rad\,\mathcal{V}\cong rad\,\mathcal{V}'$.

Como $\mathcal{V}\cong\mathcal{V}'$ y $rad\,\mathcal{V}\cong rad\,\mathcal{V}'$, entonces $\mathcal{U}\cong\mathcal{U}'$. ■

2.6. Isotropías

Sea $(\mathcal{V}, Q)$ un espacio cuadrático tal que $\mathcal{V} \neq \{0\}$.

Definición 41 *Sea $x \,\varepsilon\, \mathcal{V}$ no nulo,*

a) x es isótropo si y sólo si $Q(x) = 0$

b) x es anisótropo si y sólo si $Q(x) \neq 0$

c) $\mathcal{V}$ es isótropo si y sólo si este contiene un vector isótropo

d) $\mathcal{V}$ es anisótropo si y sólo si no contiene vectores isótropos

e) $\mathcal{V}$ es totalmente isótropo si y sólo si cada uno de los vectores no nulos son isótropos.

Observación. Tenemos que $\mathcal{V}$ es totalmente isótropo si y sólo si $\mathcal{V}$ es no nulo con $Q(\mathcal{V}) = 0$.

Para cualquier espacio cuadrático $(\mathcal{V}, Q)$ con un forma cuadrática, tal que $Q(\mathcal{V}) = 0$, obtenemos lo siguiente:

$$Q(\mathcal{V}) = 0 \Leftrightarrow B(\mathcal{V}, \mathcal{V}) = 0$$

debido a la identidad $B(x, y) = \frac{1}{2}\left(Q(x + y) - Q(x) - Q(y)\right)$.

Un ejemplo de espacios isótropos es cualquier espacio que tiene en la matriz asociada un cero en la diagonal. El más simple y más importante ejemplo de un espacio regular isótropo es el plano hiperbólico.

Definición 42 *Un espacio $\mathcal{V}$ es llamado un plano hiperbólico si la matriz asociada a la forma bilineal es*

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

en alguna base de $\mathcal{V}$.

Ejemplo 9 *Supongamos que el plano hiperbólico $\mathcal{V}$ esta escrito como $\mathcal{V} = < x, y >$, con $Q(x) = Q(y) = 0$. Entonces las rectas $< x >$, $< y >$ son isótropas y la ecuación*

$$Q(\alpha x + \beta y) = 2\alpha\beta B(x, y)$$

muestra que estas son solamente las rectas isótropas en $\mathcal{V}$. Esta ecuación muestra que $Q(\mathcal{V}) = \mathbb{F}$, en otras palabras, todos los planos hiperbólicos son universales.

Proposición 46 *Las siguientes afirmaciones son equivalentes para un espacio cuadrático $(\mathcal{V}, Q)$ de dimensión 2:*

1) $\mathcal{V}$ es un plano hiperbólico

2) $\mathcal{V}$ es isótropo y regular

3) $d\mathcal{V} = -1$

Demostración.

1) $\Rightarrow$ 2) a) Sea $\{x_1, x_2\}$ una base de $\mathcal{V}$, como

$$\mathcal{V} \asymp \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

entonces $Q(x_1) = Q(x_2) = 0$, de esta manera x_1 y x_2 son isótropos. Por lo tanto $\mathcal{V}$ es isótropo.

b) $d\mathcal{V} = det \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = -1$. Por lo tanto $\mathcal{V}$ es regular.

2) $\Rightarrow$ 3) Sea $x \,\varepsilon\, \mathcal{V}$ tal que $Q(x) = 0$ y sea $x_1 \,\varepsilon\, \mathcal{V}$ tal que $\{x, x_1\}$ forman una base de $\mathcal{V}$. Así $\mathcal{V}$ en esta base tiene la matriz

$$\begin{pmatrix} 0 & \beta \\ \beta & \gamma \end{pmatrix}$$

entonces $d\mathcal{V} = \det \begin{pmatrix} 0 & \beta \\ \beta & \gamma \end{pmatrix} = -\beta^2$, como $\mathcal{V}$ es regular, entonces $\beta \,\varepsilon\, \dot{\mathbb{F}}$. Pero $-\beta^2$ es equivalente a -1 en $\dot{\mathbb{F}}/\dot{\mathbb{F}}^2$. Así $d\mathcal{V} = -1$.

3) $\Rightarrow$ 1) Como $\mathcal{V}$ es regular entonces $Q(\mathcal{V}) \neq 0$. Tomando $\alpha \,\varepsilon\, \mathbb{F}$, tal que $\alpha \,\varepsilon\, Q(\mathcal{V})$, es decir, $\exists\ x \,\varepsilon\, \mathcal{V}$ tal que $Q(x) = \alpha$. Así $< x >$ es un sumando ortogonal de $\mathcal{V}$ y además regular, de esta manera $\mathcal{V} =< x >\perp< y >$ para algún $y \,\varepsilon\, \mathcal{V}$.

Como $d\mathcal{V} = -1$, entonces $-Q(x)Q(y)$ es un cuadrado no nulo, de esta manera podemos asumir que $Q(y) = -\alpha$. Entonces

$$\mathcal{V} = \left\langle \frac{1}{2}(x+y), \frac{1}{\alpha}(x-y) \right\rangle$$

en esta base ortogonal tiene como matriz $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, en efecto

$$\begin{aligned} Q\left(\frac{1}{2}(x+y)\right) &= \frac{1}{4}\left(Q(x) + Q(y) + 2B(x,y)\right) \\ &= \frac{1}{4}(\alpha - \alpha + 2B(x,y)) \\ &= 0 \end{aligned}$$

$$
\begin{aligned}
B\left(\frac{1}{2}(x+y), \frac{1}{\alpha}(x-y)\right) &= \frac{1}{2\alpha}(Q(x) - B(x,y) + B(x,y) - Q(y)) \\
&= \frac{1}{2\alpha}(\alpha + 0 - (-\alpha)) \\
&= 1
\end{aligned}
$$

por lo tanto $\mathcal{V}$ es un plano hiperbólico.

■

Proposición 47 *Todo espacio regular isótropo tiene como sumando ortogonal un plano hiperbólico. Así este es universal.*

Demostración. Sea x un vector isótropo en $\mathcal{V}$. Como $\mathcal{V}$ es regular, $\exists\ y \ \varepsilon\ \mathcal{V}$ con $B(x,y) \neq 0$ entonces $\mathcal{H} =< x, y >$ es un espacio regular isótropo de dimensión 2 entonces es un plano hiperbólico, además como $\mathcal{H}$ es regular, entonces

$$\mathcal{V} = \mathcal{H} \perp \mathcal{H}^{\perp}$$

Como $Q\mid_{\mathcal{H}}$ es universal, entonces $\mathcal{V}$ es universal ya que

$$
\begin{aligned}
Q(\mathcal{V}) &= Q(\mathcal{H} \perp \mathcal{H}^{\perp}) \\
&= Q(\mathcal{H}) + Q(\mathcal{H}^{\perp}) \\
&= \mathbb{F} + Q(\mathcal{H}^{\perp}) \\
&= \mathbb{F}
\end{aligned}
$$

■

Proposición 48 *Sea $(\mathcal{V}, Q)$ un espacio cuadrático regular, sea $\alpha\ \varepsilon\ \mathbb{F}$. Entonces se cumple:*

$$\alpha\ \varepsilon\ Q(\mathcal{V}) \textit{ si y sólo si } \langle -\alpha \rangle \perp \mathcal{V} \textit{ es isótropo}$$

Demostración. Consideremos $\mathcal{W} = \langle -\alpha \rangle \perp \mathcal{V}$ con $Q(z) = -\alpha$, para algún $z\ \varepsilon\ \mathcal{W}$.

$\Rightarrow$) Sea $x\ \varepsilon\ \mathcal{V}$ tal que $Q(x) = \alpha$ entonces

$$
\begin{aligned}
Q(z+x) &= Q(z) + Q(x) + 2B(z,x) \\
&= -\alpha + \alpha + 0 \\
&= 0
\end{aligned}
$$

entonces $\mathcal{W}$ es isótropo.

$\Leftarrow$) Supongamos que $\mathcal{W}$ es isótropo. Si $\mathcal{V}$ es isótropo este es universal por Proposición 47, así $\alpha \,\varepsilon\, Q(\mathcal{V})$.

Si $\mathcal{V}$ no es isótropo, entonces existe $x \,\varepsilon\, \mathcal{W}$ tal que $Q(x) = 0$, donde $x = \beta z + y$, con $\beta \,\varepsilon\, \dot{\mathbb{F}}$, $y \,\varepsilon\, \mathcal{V}$. Así

$$\begin{aligned} Q(\beta z + y) &= 0 \\ -\beta^2\alpha + Q(y) &= 0 \\ \alpha &= Q(y)/\beta^2 = Q\left(\frac{1}{\beta}\, y\right) \qquad \varepsilon\, Q(\mathcal{V}) \end{aligned}$$

■

Proposición 49 *Sea* $\mathcal{U}$ *un subespacio regular de un espacio cuadrático* $(\mathcal{V}, Q)$*, tal que la* $\dim \mathcal{U} = 3$ *y la* $\dim \mathcal{V} = 4$*. Si el discriminante de* $\mathcal{V}$ *es 1, entonces*

$$\mathcal{V} \text{ es isótropo si y sólo si } \mathcal{U} \text{ es isótropo}$$

Demostración.

$\Leftarrow$) La demostración es clara.

$\Rightarrow$) Sea $\mathcal{V}$ isótropo y escribamos $\mathcal{V} = \mathcal{U} \perp \mathcal{U}^\perp$, por Proposición 40.
Como $\dim \mathcal{U}^\perp = 1$, entonces $\mathcal{U}^\perp = \langle \alpha \rangle$, con $\alpha \,\varepsilon\, \dot{\mathbb{F}}$ y $Q(x) = \alpha$, con $x \,\varepsilon\, \mathcal{V}$. Así

$$\mathcal{V} = \mathcal{U} \perp < \alpha > \text{ es isótropo}$$

entonces $-\alpha \,\varepsilon\, Q(\mathcal{U})$ por proposición 48. De esta manera $\mathcal{U} = \langle -\alpha \rangle \perp \mathcal{P}$, por Proposición 38, con $\mathcal{P}$ un plano.

De esta manera

$$\mathcal{V} = \langle -\alpha \rangle \perp \mathcal{P} \perp \langle \alpha \rangle$$

como

$$\begin{aligned} 1 = d\mathcal{V} &= d\langle -\alpha \rangle \cdot d\mathcal{P} \cdot d\langle \alpha \rangle \\ &= -\alpha^2 d\mathcal{P} \\ &= -d\mathcal{P} \\ d\mathcal{P} &= -1 \end{aligned}$$

así $\mathcal{P}$ es un plano hiperbólico. Por lo tanto $\mathcal{U}$ es isótropo.

■

Proposición 50 *Sea* $(\mathcal{V}, Q)$ *un espacio cuadrático regular,* $\mathcal{U}$ *un subespacio de* $\mathcal{V}$ *con* $Q(\mathcal{U}) = 0$ *y* $\{x_1, x_2, \ldots, x_r\}$ *una base de* $\mathcal{U}$*. Entonces existe un subespacio* $\mathcal{H}_1 \perp \mathcal{H}_2 \perp \cdots \perp \mathcal{H}_r$ *de* $\mathcal{V}$ *en el cual cada* $\mathcal{H}_i$ *es un plano hiperbólico, con* $x_i \,\varepsilon\, \mathcal{H}_i$*.*

Demostración.

a) Si $r = 1$ tomamos $y_1 \,\varepsilon\, \mathcal{V}$ con $B(x_1, y_1) \neq 0$ y haciendo $\mathcal{H}_1 =< x_1, y_1 >$ obtenemos que $\mathcal{H}_1$ es un plano hiperbólico con las propiedades deseadas.

b) $r > 1$ definimos lo siguiente:
sea
$$\mathcal{U}_{r-1} =< x_1, \ldots, x_{r-1} > \quad \text{y} \quad \mathcal{U}_r = \mathcal{U}$$
entonces $\mathcal{U}_{r-1} \subset \mathcal{U}_r$ de esta manera $\mathcal{U}_r^\perp \subset \mathcal{U}_{r-1}^\perp$.
Sea $y_r \,\varepsilon\, \mathcal{U}_{r-1}^\perp - \mathcal{U}_r^\perp$ y escribiendo $\mathcal{H}_r =< x_r, y_r >$, obtenemos que
$$B(y_r, w) = 0 \qquad \forall w \,\varepsilon\, \mathcal{U}_{r-1}$$
en particular para x_i, con $1 \leq i \leq r-1$. Como $B(x_r, y_r) \neq 0$, así $\mathcal{H}_r$ es un plano hiperbólico que contiene a x_r.
Escribiendo $\mathcal{V} = \mathcal{H}_r \perp \mathcal{H}_r^\perp$, entonces
$$\mathcal{H}_r \subseteq \mathcal{U}_{r-1}^\perp$$
ya que $y_r \,\varepsilon\, \mathcal{U}_{r-1}^\perp$ y $x_r \,\varepsilon\, \mathcal{U}_r^\perp \subseteq \mathcal{U}_{r-1}^\perp$. Así
$$\mathcal{U}_{r-1} \subseteq \mathcal{H}_r^\perp$$
Aplicando la inductividad a $\mathcal{U}_{r-1}$ como subespacio de $\mathcal{H}_r^\perp$ obtenemos que
$$\mathcal{H}_1 \perp \mathcal{H}_2 \perp \cdots \perp \mathcal{H}_{r-1} \subseteq \mathcal{H}_r^\perp$$
con $x_i \,\varepsilon\, \mathcal{H}_i$ para $1 \leq i \leq r-1$. De esta manera $\mathcal{H}_1 \perp \mathcal{H}_2 \perp \cdots \perp \mathcal{H}_r$ es el subespacio con las propiedades deseadas.

■

2.7. Involuciones y Reflexiones

Sea $1_\mathcal{V} \,\varepsilon\, End(\mathcal{V})$ la transformación lineal identidad, es decir
$$\begin{aligned} 1_\mathcal{V} : \ \mathcal{V} &\to \mathcal{V} \\ x &\rightsquigarrow x \end{aligned}$$
y su inversa aditiva $-1_\mathcal{V}$, la cual da el opuesto a todo vector de $\mathcal{V}$, es decir,
$$\begin{aligned} -1_\mathcal{V} : \ \mathcal{V} &\to \mathcal{V} \\ x &\rightsquigarrow -x \end{aligned}$$
Claramente $\pm 1_\mathcal{V} \,\varepsilon\, O_n(\mathcal{V})$ ya que $Q(\pm 1_\mathcal{V}(x)) = Q(x) \;\forall\, x \,\varepsilon\, \mathcal{V}$.

Definición 43 *Sea $\sigma \,\varepsilon\, End(\mathcal{V})$, tal que $\sigma \neq 1_\mathcal{V}$, diremos que σ es una involución si $\sigma^2 = 1_\mathcal{V}$.*

Proposición 51 *Sea $(\mathcal{V}, Q)$ un espacio cuadrático y $\sigma \,\varepsilon\, O_n(\mathcal{V})$. σ es una involución si y sólo si existe una suma ortogonal de $\mathcal{V} = \mathcal{U} \perp \mathcal{W}$ para la cual $\sigma = -1_\mathcal{U} \perp 1_\mathcal{W}$.*

Demostración.

$\Leftarrow$) Si $\sigma = -1_{\mathcal{U}} \perp 1_{\mathcal{W}}$, entonces

$$\begin{aligned} \sigma^2 &= -1_{\mathcal{U}} - 1_{\mathcal{U}} \perp 1_{\mathcal{W}} 1_{\mathcal{W}} \\ &= 1_{\mathcal{U}} \perp 1_{\mathcal{W}} \\ &= 1_{\mathcal{V}} \end{aligned}$$

por lo tanto es una involución. Donde $1_{\mathcal{U}} = 1_{\mathcal{V}}|_{\mathcal{U}}$ y $1_{\mathcal{W}} = 1_{\mathcal{V}}|_{\mathcal{W}}$.

$\Rightarrow$) Supongamos que σ es una involución, entonces $\sigma^2 = 1_{\mathcal{V}}$. Consideremos las transformaciones lineales $\sigma - 1_{\mathcal{V}}$ y $\sigma + 1_{\mathcal{V}}$ definidas de la siguiente forma:

$$\begin{aligned} \sigma - 1_{\mathcal{V}} : \ & \mathcal{V} \to \mathcal{V} \\ & x \rightsquigarrow (\sigma - 1_{\mathcal{V}})(x) = \sigma(x) - x \end{aligned}$$

$$\begin{aligned} \sigma + 1_{\mathcal{V}} : \ & \mathcal{V} \to \mathcal{V} \\ & x \rightsquigarrow (\sigma + 1_{\mathcal{V}})(x) = \sigma(x) + x \end{aligned}$$

haciendo $\mathcal{U} = (\sigma - 1_{\mathcal{V}})(\mathcal{V})$ y $\mathcal{W} = (\sigma + 1_{\mathcal{V}})(\mathcal{V})$, para $x \,\varepsilon\, \mathcal{V}$ tenemos que

$$x = -\frac{1}{2}(\sigma - 1_{\mathcal{V}})(x) + \frac{1}{2}(\sigma + 1_{\mathcal{V}})(x) \ \ \varepsilon\, \mathcal{U} + \mathcal{W}$$

en efecto,

$$\begin{aligned} -\frac{1}{2}(\sigma - 1_{\mathcal{V}})(x) + \frac{1}{2}(\sigma + 1_{\mathcal{V}})(x) &= -\frac{1}{2}(\sigma(x) - x) + \frac{1}{2}(\sigma(x) + x) \\ &= x \end{aligned}$$

de esta manera $\mathcal{V} = \mathcal{U} + \mathcal{W}$.

Sea $y \,\varepsilon\, \mathcal{U}$, entonces $y = (\sigma - 1_{\mathcal{V}})(x)$, así

$$\begin{aligned} \sigma(y) &= \sigma((\sigma - 1_{\mathcal{V}})(x)) \\ &= \sigma^2(x) - \sigma(x) \\ &= x - \sigma(x) \\ &= -(\sigma - 1_{\mathcal{V}})(x) \\ &= -y \end{aligned}$$

para todo $y \,\varepsilon\, \mathcal{U}$. Similarmente para $z \,\varepsilon\, \mathcal{W}$ tenemos que $z = (\sigma + 1_{\mathcal{V}})(x)$, entonces

$$\begin{aligned} \sigma(z) &= \sigma^2(x) + \sigma(x) \\ &= x + \sigma(x) \\ &= (\sigma + 1_{\mathcal{V}})(x) \\ &= z \end{aligned}$$

para todo $z \,\varepsilon\, \mathcal{W}$. Si $v \,\varepsilon\, \mathcal{U} \cap \mathcal{W}$ tenemos que

$$\begin{array}{rcl} \sigma(v) &=& \sigma(v) \\ -v &=& v \\ 2v &=& 0 \\ v &=& 0 \end{array}$$

por lo tanto $\mathcal{U} \cap \mathcal{W} = 0$. Así $\mathcal{V} = \mathcal{U} \oplus \mathcal{W}$. Además para $y \,\varepsilon\, \mathcal{U}$ y $z \,\varepsilon\, \mathcal{W}$ tenemos que

$$\begin{array}{rcl} B(y,z) &=& B(\sigma(y), \sigma(z)) \\ &=& B(-y, z) \\ 2B(y,z) &=& 0 \\ B(y,z) &=& 0 \end{array}$$

Así $B(\mathcal{U}, \mathcal{W}) = 0$. Por lo tanto $\mathcal{V} = \mathcal{U} \perp \mathcal{W}$.

De esta manera σ es $-1_{\mathcal{U}}$ en $\mathcal{U}$ y $1_{\mathcal{W}}$ en $\mathcal{W}$, por lo tanto

$$\sigma = -1_{\mathcal{U}} \perp 1_{\mathcal{W}}$$

■

Observación. $\mathcal{U}$ es el conjunto de vectores opuestos de σ y $\mathcal{W}$ es el conjunto de vectores fijos de σ.

Definición 44 *Sea $y \,\varepsilon\, \mathcal{V}$ fijo, tal que y es anisótropo, entonces se define*

$$\begin{array}{rcl} \tau_y : & \mathcal{V} & \to \mathcal{V} \\ & x & \rightsquigarrow x - \dfrac{2B(x,y)}{Q(y)} y \end{array}$$

una reflexión de $\mathcal{V}$ en $\mathcal{V}$.

Proposición 52 *Sea $y \,\varepsilon\, \mathcal{V}$, tal que y es anisótropo y $\sigma \,\varepsilon\, O_n(\mathcal{V})$, entonces tenemos las siguientes propiedades:*

a) τ_y *es una transformación lineal*

b) τ_y *es una involución*

c) $\tau_y \,\varepsilon\, O_n(\mathcal{V})$

d) $\sigma \tau_y \sigma^{-1} = \tau_{\sigma(y)}$

e) $\tau_y^{-1} = \tau_y$

Demostración. Sean $x, z \,\varepsilon\, \mathcal{V}$ y $\alpha \,\varepsilon\, \mathbb{F}$ entonces

a)

$$\begin{aligned}
\tau_y(\alpha x + z) &= (\alpha x + z) - \frac{2B(\alpha x + z, y)}{Q(y)} y \\
&= (\alpha x + z) - \frac{2(B(\alpha x, y) + B(z, y))}{Q(y)} y \\
&= \alpha \left(x - \frac{2B(x, y)}{Q(y)} y \right) + z - \frac{2B(z, y)}{Q(y)} y \\
&= \alpha \tau_y(x) + \tau_y(z)
\end{aligned}$$

por lo tanto τ_y es una transformación lineal.

b)

$$\begin{aligned}
\tau_y^2(x) &= \tau_y(\tau_y(x)) \\
&= \tau_y \left(x - \frac{2B(x, y)}{Q(y)} y \right) \\
&= \tau_y(x) - \frac{2B(x, y)}{Q(y)} \tau_y(y) \qquad \text{pero } \tau_y(y) = -y \\
&= \left(x - \frac{2B(x, y)}{Q(y)} y \right) + \frac{2B(x, y)}{Q(y)} y \\
&= x
\end{aligned}$$

Por lo tanto $\tau_y^2(x) = x$, de esta manera $\tau_y^2 = 1_{\mathcal{V}}$. Así τ_y es una involución.

c) 1)

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

Por lo tanto τ_y traslada la forma cuadrática.

2) Sea $x \,\varepsilon\, \ker \tau_y$

$$\tau_y(x) = 0_{\mathcal{V}}$$

como τ_y es una involución, entonces

$$\begin{aligned}
\tau_y^2(x) &= \tau_y(0_{\mathcal{V}}) = 0_{\mathcal{V}} \\
x &= 0_{\mathcal{V}}
\end{aligned}$$

así τ_y es una isometría y por lo tanto $\tau_y \,\varepsilon\, O_n(\mathcal{V})$.

d)

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

e) Como τ_y es una involución, entonces

$$
\begin{aligned}
\tau_y \circ \tau_y &= 1_{\mathcal{V}} \\
\tau_y &= \tau_y^{-1}
\end{aligned}
$$

■

Llamaremos a τ_y la reflexión con respecto al vector y o con respecto a la recta $< y >$. Además sea $x \,\varepsilon\, \mathcal{V}$, entonces

$$
\begin{aligned}
\tau_y(x) &= \tau_{y'}(x) \\
\Leftrightarrow \quad x - \frac{2B(x,y)}{Q(y)}y &= x - \frac{2B(x,y')}{Q(y')}y' \\
\Leftrightarrow \quad \frac{B(x,y')}{Q(y')}y' &= \frac{B(x,y)}{Q(y)}y
\end{aligned}
$$

pero $\frac{B(x,y')}{Q(y')}, \frac{B(x,y)}{Q(y)} \,\varepsilon\, \mathbb{F}$, por lo tanto

$$
< y' > \;=\; < y >
$$

así $\tau_y(x) = \tau_{y'}(x)$ si y sólo si $\alpha y \,\varepsilon\, < y' >$ o viceversa.

En particular hay exactamente tantas reflexiones como vectores anisótropos en $\mathcal{V}$.

Ejemplo 10 *Sea $\sigma \,\varepsilon\, O_2(\mathcal{H})$, con $\mathcal{H}$ un plano hiperbólico. Entonces,*

σ es una reflexión si y sólo si σ intercambia las dos rectas isótropas.

a) *Sea* $\mathcal{H} =< x, y >$ *un plano hiperbólico con* $Q(x) = Q(y) = 0$. *Consideremos un vector* $z = x - \alpha y$ *para algún* $\alpha \neq 0$. *Luego*

$$\begin{aligned} B(z,z) &= B(x-\alpha y, x-\alpha y) \\ &= 2\alpha B(x,y) \end{aligned}$$

por lo tanto z *es anisótropo. De esta manera podemos formar la reflexión* τ_z, *donde*

$$\begin{aligned} \tau_z(x) &= x - \frac{2B(x, x-\alpha y)}{Q(x-\alpha y)}(x-\alpha y) \\ &= x - \frac{2(B(x,x) - \alpha B(x,y))}{-2\alpha B(x,y)}(x-\alpha y) \\ &= x - x + \alpha y \\ &= \alpha y \end{aligned}$$

$$\begin{aligned} \tau_z(y) &= y - \frac{2B(y, x-\alpha y)}{-2\alpha B(x,y)}(x-\alpha y) \\ &= y - \frac{2B(x,y)}{-2\alpha B(x,y)}(x-\alpha y) \\ &= y + \alpha^{-1}x - y \\ &= \alpha^{-1}x \end{aligned}$$

Así toda reflexión en un plano hiperbólico intercambia las dos rectas isótropas.

b) *Sea* $\sigma \,\varepsilon\, O_2(\mathcal{V})$, *tal que intercambia las dos rectas isótropas, entonces debe ser una reflexión:* $\sigma(x) = \alpha y$ *con* $\alpha \,\varepsilon\, \dot{\mathbb{F}}$, *de aquí la ecuación*

$$\begin{aligned} B(x,y) &= B(\sigma(x), \sigma(y)) \\ &= B(\alpha y, \sigma(y)) \end{aligned}$$

lleva a que $\sigma(y) = \alpha^{-1}x$, *por lo tanto* $\sigma = \tau_{x-\alpha y}$.

Finalmente notemos que la acción de $\sigma' \,\varepsilon\, O_2(\mathcal{V})$ *la cual no es una reflexión esta descrita por*

$$\sigma'(x) = \alpha x, \quad \sigma'(y) = \alpha^{-1}y$$

por lo tanto, toda σ' *es de la forma*

$$\sigma' = \tau_{x-y}\tau_{x-\alpha y}$$

2.8. Teorema de Witt

Teorema 2 *Sea* $\mathcal{U}$ *y* $\mathcal{W}$ *subespacios regulares de un espacio cuadrático* $(\mathcal{V}, Q)$. *Si* $\mathcal{U} \cong \mathcal{W}$, *entonces* $\mathcal{U}^\perp \cong \mathcal{W}^\perp$.

Demostración. Probaremos el resultado por inducción en la dimensión de $\mathcal{U}$.

i) $\dim \mathcal{U} = 1$. Sean $\mathcal{U}$ y $\mathcal{W}$ rectas, es decir $\mathcal{U} =< x >$ y $\mathcal{W} =< y >$ con $Q(x) = Q(y) \neq 0$. Entonces

$$Q(x+y) + Q(x-y) = 2Q(x) + 2Q(y) = 4Q(x)$$

por lo tanto $Q(x+y)$ o $Q(x-y)$ es no nulo. Como $\mathcal{W} =< y >$, podemos intercambiar y por $-y$, es decir, $\mathcal{W} =< -y >$, lo cual nos permite asumir que $Q(x-y) \neq 0$. Por consiguiente podemos considerar la reflexión τ_{x-y}. Así tenemos que

$$\tau_{x-y}(x) = x - \frac{2B(x, x-y)}{Q(x-y)}(x-y)$$

pero

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

así

$$\tau_{x-y}(x) = x - \frac{Q(x-y)}{Q(x-y)}(x-y) = y$$

de aquí que τ_{x-y} es la respectiva isometría de la hipótesis, es decir, $\tau_{x-y}(\mathcal{U}) = \mathcal{W}$. Sea $u \,\varepsilon\, \mathcal{U}^{\perp}$, tenemos que

$$B(u,x) = 0 \qquad \forall\, x \,\varepsilon\, \mathcal{U}$$

luego

$$\begin{aligned} 0 &= B(u,x) \\ &= B(\tau_{x-y}(u), \tau_{x-y}(x)) \\ &= B(\tau_{x-y}(u), y) \end{aligned}$$

por lo tanto $\tau_{x-y}(u) \;\varepsilon\; \mathcal{W}^{\perp}$. Así $\tau_{x-y}\left(\mathcal{U}^{\perp}\right) \subseteq \mathcal{W}^{\perp}$. Como $\dim \mathcal{U}^{\perp} = \dim \mathcal{W}^{\perp}$, entonces $\mathcal{U}^{\perp} \cong \mathcal{W}^{\perp}$.

ii) $\dim \mathcal{U} > 1$. Como $\mathcal{U} \cong \mathcal{W}$ y son regulares, podemos considerar

$$\mathcal{U} = \mathcal{U}_1 \perp \mathcal{U}_1^{\perp} \quad \text{y} \quad \mathcal{W} = \mathcal{W}_1 \perp \mathcal{W}_1^{\perp}$$

donde $\mathcal{U}_1 \cong \mathcal{W}_1$ y $\mathcal{U}_1^{\perp} \cong \mathcal{W}_1^{\perp}$, además $\dim \mathcal{U}_1 = 1$.

Como $\mathcal{V} = \mathcal{U} \perp \mathcal{U}^{\perp}$ y $\mathcal{U}_1 \cong \mathcal{W}_1$, por la primera parte resulta que

$$\mathcal{U}_1^{\perp} \perp \mathcal{U}^{\perp} \cong \mathcal{W}_1^{\perp} \perp \mathcal{W}^{\perp}$$

Tenemos $\mathcal{U}_1^{\perp} \cong \mathcal{W}_1^{\perp}$ y $\dim \mathcal{U}_1 < \dim \mathcal{U}$, luego por hipótesis de inducción

$$\mathcal{U}^{\perp} \cong \mathcal{W}^{\perp}$$

■

Teorema 3 (Witt) *Sean $(\mathcal{V}, Q)$ y $(\mathcal{V}', Q')$ dos espacios cuadráticos regulares e isométricos. Sea $\mathcal{U}$ un subespacio de $\mathcal{V}$ y σ una isometría de $\mathcal{U}$ en $\mathcal{V}'$. Entonces existe una prolongación de σ a una isometría de $\mathcal{V}$ sobre $\mathcal{V}'$.*

Demostración. Consideremos $\mathcal{U} = \mathcal{W} \perp rad\mathcal{U}$ y sea $\{x_1, x_2, \ldots, x_r\}$ una base para $rad\mathcal{U}$. La Proposición 43 nos dice que $\mathcal{W}$ es regular y por la Proposición 50 existe un subespacio

$$\mathcal{H} = \mathcal{H}_1 \perp \mathcal{H}_2 \perp \cdots \perp \mathcal{H}_r$$

del espacio $\mathcal{W}^{\perp}$ en el cual cada $\mathcal{H}_i$ es un plano hiperbólico tal que $x_i \,\varepsilon\, \mathcal{H}_i$. Como $\mathcal{H}$ es regular, este es un sumando ortogonal de $\mathcal{W}^{\perp}$, así

$$\mathcal{V} = \mathcal{W} \perp \mathcal{H} \perp \mathcal{H}^{\perp}$$

donde $\mathcal{H}^{\perp} = \{z \,\varepsilon\, \mathcal{W}^{\perp} \mid \forall\, y \,\varepsilon\, \mathcal{H},\ B(y,z) = 0\}$. Colocando $\sigma(\mathcal{U}) = \mathcal{U}'$, $\sigma(\mathcal{W}) = \mathcal{W}'$ y $\sigma(x_i) = x_i'$ para $1 \leq i \leq r$, tenemos que

$$rad\,\mathcal{U}' = \sigma(rad\,\mathcal{U}) =< x_1', x_2', \ldots, x_r' >$$

y

$$\mathcal{U}' = \mathcal{W}' \perp rad\,\mathcal{U}'$$

Repitiendo el proceso anterior obtenemos una suma ortogonal

$$\mathcal{V}' = \mathcal{W}' \perp \mathcal{H}' \perp (\mathcal{H}')^{\perp}$$

en la cual

$$\mathcal{H}' = \mathcal{H}_1' \perp \mathcal{H}_2' \perp \cdots \mathcal{H}_r'$$

donde los $\mathcal{H}_i'$ son planos hiperbólicos con $x_i' \,\varepsilon\, \mathcal{H}_i'$.

De esta manera existe una isometría

$$\tau : \mathcal{H} \to \mathcal{H}'$$

la cual coincide con σ en cada x_i y por lo tanto en $rad\,\mathcal{U}$, además σ lleva $\mathcal{W}$ en $\mathcal{W}'$, por lo tanto existe una prolongación de σ a una isometría $\sigma' = \sigma \perp \tau$ de $\mathcal{W} \perp \mathcal{H}$ sobre $\mathcal{W}' \perp \mathcal{H}'$.

Como $\mathcal{H}$ y $\mathcal{H}'$ son isométricos por τ, el teorema anterior nos dice que $\mathcal{H}^{\perp}$ y $(\mathcal{H}')^{\perp}$ son isométricos. Por lo tanto hay una prolongación de σ a una isometría de $\mathcal{V}$ sobre $\mathcal{V}'$.

■

Uno puede usar los dos últimos teoremas para definir un invariante llamado índice a un espacio regular cuadrático $(\mathcal{V}, Q)$.

Proposición 53 *Sea $(\mathcal{V}, Q)$ un espacio cuadrático regular, entonces todos los subespacios $\mathcal{M}$ maximales de $\mathcal{V}$, tal que $Q(\mathcal{M}) = 0$, tienen la misma dimensión.*

Demostración. Sea $\mathcal{M}$ un subespacio maximal de $\mathcal{V}$ tal que $Q(\mathcal{M}) = 0$ y sea $\mathcal{M}'$ otro subespacio maximal, tal que $Q(\mathcal{M}') = 0$, y supongamos que $\dim \mathcal{M} \leq \dim \mathcal{M}'$.

Existe una isometría σ de $\mathcal{M}$ en $\mathcal{M}'$, donde $Q(\mathcal{M}) = Q(\mathcal{M}') = 0$, así hay una prolongación de σ a una isometría τ de $\mathcal{V}$ sobre $\mathcal{V}$ por teorema anterior. Entonces

$$\mathcal{M} \subseteq \tau^{-1}(\mathcal{M}')$$

pero $Q(\tau^{-1}(\mathcal{M}')) = 0$ y $\mathcal{M}$ es maximal, entonces $\mathcal{M} = \tau^{-1}(\mathcal{M}')$ luego $\dim \mathcal{M} = \dim \mathcal{M}'$. ■

Definición 45 *Sea $(\mathcal{V}, Q)$un espacio cuadrático regular y $\mathcal{M}$ un subespacio maximal totalmente isótropo. Se define el índice de $\mathcal{V}$ como la dimensión de $\mathcal{M}$ y lo denotaremos por ind $\mathcal{V}$.*

Existe otra forma de mirar el índice. Si descomponemos $\mathcal{V}$ completamente en planos hiperbólicos obtenemos una suma ortogonal

$$\mathcal{V} = \mathcal{H}_1 \perp \cdots \perp \mathcal{H}_r \perp \mathcal{V}_0$$

con $0 \leq 2r \leq \dim \mathcal{V}$ y $\mathcal{V}_0$ es 0 o anisótropo. Por Teorema 2 vemos que r no depende de la suma ortogonal realizada y entonces $\mathcal{V}_0$ es único bajo una isometría. La Proposición 50 muestra que r es realmente el índice de $\mathcal{V}$. En particular esto prueba que $r = \mathrm{ind}\mathcal{V}$ satisface la inecuación

$$0 \leq 2\,\mathrm{ind}\mathcal{V} \leq \dim \mathcal{V}$$

Definición 46 *Sea $(\mathcal{V}, Q)$ un espacio cuadrático tal que ind $\mathcal{V} = r$. Diremos que $\mathcal{V}$ es un espacio hiperbólico si* $\dim \mathcal{V} = 2r$.

Así $(\mathcal{V}, Q)$ es un espacio hiperbólico si y sólo si este tiene una suma ortogonal

$$\mathcal{V} = \mathcal{H}_1 \perp \cdots \perp \mathcal{H}_r$$

en la cual $1 \leq r$ con todos los $\mathcal{H}_i$ planos hiperbólicos.

Capítulo 3

Subgrupos Distinguidos del Grupo Ortogonal

Consideremos un espacio cuadrático regular $(\mathcal{V}, Q)$. Mostraremos que las reflexiones de $\mathcal{V}$ generan a $O_n(\mathcal{V})$ y haremos un estudio preliminar de ciertos subgrupos de $O_n(\mathcal{V})$, estos son:

i) O_n^+, el subgrupo de rotaciones.

ii) Ω_n, el subgrupo conmutador.

iii) Z_n, el centro.

3.1. Rotaciones y Simetrías

Consideremos el grupo ortogonal $O_n(\mathcal{V})$ del espacio cuadrático regular no nulo $(\mathcal{V}, Q)$ y la forma bilineal B asociada a Q.

Fijemos una base $\mathcal{B} = \{x_1, x_2, \ldots, x_n\}$ para $\mathcal{V}$ y sea M la matriz asociada a B. Consideremos $\sigma \,\varepsilon\, O_n(\mathcal{V})$ y sea $T = [\sigma]_{\mathcal{B}}$ la matriz de σ en esta base, es decir,

$$\sigma(x_j) = \sum_{i=1}^{n} t_{ij}\, x_i$$

entonces $\{\sigma(x_1), \sigma(x_2), \ldots, \sigma(x_n)\}$ es también una base de $\mathcal{V}$ y la matriz asociada a B en esta base es M, en efecto

$$\begin{aligned} (B(\sigma(x_i), \sigma(x_j))) &= (B(x_i, x_j)) \qquad 1 \leq i, j \leq n \\ &= M \end{aligned}$$

Proposición 54 *Sean $\sigma \,\varepsilon\, End(\mathcal{V})$, $\mathcal{B}$ una base de $\mathcal{V}$ y M la matriz asociada a B en esta base.*

$$\sigma \,\varepsilon\, O_n(\mathcal{V}) \text{ si y sólo si } [\sigma]_{\mathcal{B}}^t M [\sigma]_{\mathcal{B}} = M$$

Demostración. Sea $T = [\sigma]_{\mathcal{B}}$, por 2.2 tenemos que $M = T^tMT$, entonces

$$\begin{aligned}
\sigma \,\varepsilon\, O_n(\mathcal{V}) &\Leftrightarrow B(\sigma(x),\sigma(y)) = B(x,y) \qquad \forall\, x,y\,\varepsilon\,\mathcal{V}\\
&\Leftrightarrow [\sigma(x)]_{\mathcal{B}}^t\,(B(x_i,x_j))\,[\sigma(y)]_{\mathcal{B}} = [x]_{\mathcal{B}}^t\,(B(x_i,x_j))\,[y]_{\mathcal{B}} \qquad \forall\, x,y\,\varepsilon\,\mathcal{V}\\
&\Leftrightarrow ([\sigma]_{\mathcal{B}}[x]_{\mathcal{B}})^t\; M\,[\sigma]_{\mathcal{B}}[y]_{\mathcal{B}} = [x]_{\mathcal{B}}^t\,M\,[y]_{\mathcal{B}} \qquad \forall\, x,y\,\varepsilon\,\mathcal{V}\\
&\Leftrightarrow [x]_{\mathcal{B}}^tT^tMT[y]_{\mathcal{B}} = [x]_{\mathcal{B}}^tM[y]_{\mathcal{B}} \qquad \forall\, x,y\,\varepsilon\,\mathcal{V}\\
&\Leftrightarrow T^tMT = M
\end{aligned}$$

■

Corolario 6 *Con las hipótesis de la Proposición anterior.*

$$\begin{array}{rcl}
\phi: \; O_n(\mathcal{V}) & \rightarrow & \{T\,\varepsilon\, GL_n(\mathcal{V}) \mid M = T^tMT\}\\
\sigma & \rightsquigarrow & [\sigma]_{\mathcal{B}}
\end{array}$$

es un isomorfismo de grupos.

Corolario 7 *Sea $\sigma\,\varepsilon\,O_n(\mathcal{V})$, entonces*

$$det(\phi(\sigma)) = \pm 1$$

Demostración. Por la Proposición anterior, si $\sigma\,\varepsilon\,O_n(\mathcal{V})$, entonces $M = T^tMT$, donde $M = (B(x_i,x_j))$ y $T = [\sigma]_{\mathcal{B}}$, entonces

$$\begin{aligned}
\det M &= \det(T^tMT)\\
\det M &= \det(T^t)\det M \det T\\
\det M &= \det M(\det(T))^2\\
1 &= (\det(T))^2\\
\pm 1 &= \det(\phi(\sigma))
\end{aligned}$$

cuando $\mathcal{V}$ es regular.

Denotamos por $\det(\phi(\sigma)) = \det(\sigma)$. ■

Si consideramos ahora el determinante como una función, es decir,

$$\det : O_n(\mathcal{V}) \rightarrow \{\pm 1\}$$

entonces det es un epimorfismo de grupos y con núcleo $\ker(\det) = \{\sigma\,\varepsilon\,O_n(\mathcal{V}) \mid \det\sigma = 1\}$, de esta manera $\ker(\det) \trianglelefteq O_n(\mathcal{V})$, con

$$[O_n(\mathcal{V}) : \ker(\det)] = 2$$

Definición 47 *Sea $\sigma \varepsilon O_n(\mathcal{V})$.*

1) *Diremos que σ es una rotación si $\det \sigma = 1$ y sea*

$$O_n^+(\mathcal{V}) = \{\sigma \varepsilon O_n(\mathcal{V}) \mid \det \sigma = 1\}$$

el conjunto de rotaciones de $\mathcal{V}$.

2) *Diremos que σ es una simetría si $\det \sigma = -1$ y sea*

$$O_n^-(\mathcal{V}) = \{\sigma \varepsilon O_n(\mathcal{V}) \mid \det \sigma = -1\}$$

el conjunto de simetrías de $\mathcal{V}$.

Por Corolario anterior, tenemos que $O_n^+(\mathcal{V})$ es un subgrupo normal de $O_n(\mathcal{V})$, además $O_n^+(\mathcal{V})$,$O_n^-(\mathcal{V})$ corresponden a las clases laterales, así tenemos que

$$O_n(\mathcal{V}) = O_n^+(\mathcal{V}) \cup O_n^-(\mathcal{V}), \qquad O_n^+(\mathcal{V}) \cap O_n^-(\mathcal{V}) = \phi$$

Observación. *Como hay tantas reflexiones como rectas anisótropas, entonces el número de reflexiones es al menos igual al número de rectas anisótropas. Como hay tantas rotaciones como reflexiones, entonces el número de rotaciones es al menos igual al número de rectas anisótropas.*

Proposición 55 *Sea $(\mathcal{V}, Q)$ un espacio hiperbólico y $\sigma \varepsilon O_n(\mathcal{V})$ la cual es la identidad en un subespacio maximal totalmente isótropo de $\mathcal{V}$. Entonces σ es una rotación.*

Demostración. Sea $\mathcal{M}$ un subespacio maximal tal que $Q(\mathcal{M}) = 0$ y sea r la dimensión de $\mathcal{M}$, por lo tanto la dimensión de $\mathcal{V}$ es $2r$. Por la Proposición 50 existe otro subespacio maximal totalmente isótropo $\mathcal{N}$ de $\mathcal{V}$ tal que $\mathcal{V} = \mathcal{M} \oplus \mathcal{N}$.

Para cualquier $x \varepsilon \mathcal{M}$ e $y \varepsilon \mathcal{N}$, donde $\sigma(x) = x$ se cumple que

$$\begin{aligned} B(x, \sigma(y) - y) &= B(x, \sigma(y)) - B(x, y) \\ &= B(x, \sigma(y)) - B(\sigma(x), \sigma(y)) \\ &= 0 \end{aligned}$$

por lo tanto $\sigma(y) - y \varepsilon \mathcal{M}^\perp$.

Como $\mathcal{M} \subseteq \mathcal{M}^\perp$ y la $\dim \mathcal{M} = \dim \mathcal{V}/2$, entonces $\dim \mathcal{M} = \dim \mathcal{M}^\perp$, por lo tanto $\mathcal{M} = \mathcal{M}^\perp$, así $\sigma(y) - y \varepsilon \mathcal{M}$.

Tomando una base $\{x_1, x_2, \ldots, x_r\}$ de $\mathcal{M}$ y una base $\{y_1, y_2, \ldots, y_r\}$ de $\mathcal{N}$, construimos $\mathcal{B} = \{x_1, x_2, \ldots, x_r, y_1, y_2, \ldots, y_r\}$ una base para $\mathcal{V}$, entonces la matriz asociada a σ en esta base, la obtenemos de:

i) $\sigma(x_i) = x_i \quad 1 \leq i \leq r$

ii)

$$\sigma(y_k) - y_k = \sum_{i=1}^{r} \alpha_i^k\, x_i + \sum_{j=1}^{r} \beta_j^k\, y_j \qquad \varepsilon\ \mathcal{M}$$

de esta manera $\beta_j^k = 0,$ para $1 \leq j \neq k \leq r$. Así

$$\sigma(y_k) = \sum_{i=1}^{r} \alpha_i^k\, x_i + y_k$$

de esta forma

$$[\sigma]_{\mathcal{B}} = \begin{pmatrix} 1 & 0 & \cdots & 0 & \alpha_1^1 & \alpha_1^2 & \cdots & \alpha_1^r \\ 0 & 1 & \cdots & 0 & \alpha_2^1 & \alpha_2^2 & \cdots & \alpha_2^r \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 1 & \alpha_r^1 & \alpha_r^2 & \cdots & \alpha_r^r \\ 0 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

y por lo tanto

$$\det \sigma = \det([\sigma]_{\mathcal{B}}) = 1$$

■

Proposición 56 *Sea $\mathcal{U}$ un hiperplano del espacio cuadrático regular $(\mathcal{V}, Q)$ y sea σ una isometría de $\mathcal{U}$ en $\mathcal{V}$. Si $\mathcal{U}$ es regular hay exactamente dos prolongaciones de σ a $\mathcal{V}$ y una es una reflexión compuesta con la otra. Si $\mathcal{U}$ no es regular hay exactamente una prolongación de σ a $\mathcal{V}$.*

Demostración. El Teorema de Witt nos asegura que existe una prolongación σ_1 de σ. Consideremos $\sigma_2\ \varepsilon\ O_n(\mathcal{V})$. σ_2 es una prolongación de σ si y sólo si $\sigma_2^{-1} \circ \sigma_1 = 1_{\mathcal{U}}$ en $\mathcal{U}$, en efecto, como $\sigma_1 \mid_{\mathcal{U}} = \sigma$, entonces

$$\begin{aligned} \sigma_1 \mid_{\mathcal{U}} &= \sigma_2 \mid_{\mathcal{U}} \\ \sigma_2^{-1} \circ \sigma_1 \mid_{\mathcal{U}} &= 1_{\mathcal{U}} \end{aligned}$$

Sea $\rho = \sigma_2^{-1} \circ \sigma_1$, entonces

1) $\mathcal{U}$ es regular. Sea $\mathcal{U}^{\perp} =< y >$ con $Q(y) \neq 0$, entonces para todo $x\ \varepsilon\ \mathcal{U}$

$$\begin{aligned} 0 &= B(x, y) \\ &= B(\rho(x), \rho(y)) \\ &= B(x, \rho(y)) \end{aligned}$$

entonces $\rho(y)\,\varepsilon\,\mathcal{U}^{\perp}$, de esta manera $\rho(y) = \alpha y$. Así

$$\begin{aligned} Q(y) &= Q(\rho(y)) \\ &= Q(\alpha y) \\ &= \alpha^2 Q(y) \end{aligned}$$

por lo tanto $\alpha^2 = 1$. De esta forma $\rho\,|_{\mathcal{U}^{\perp}} = \pm 1_{\mathcal{U}^{\perp}}$. Por lo tanto

$$\sigma_2 = \sigma \perp \sigma_1 \quad \text{o} \quad \sigma_2 = \sigma \perp -\sigma_1$$

y sólo existen 2 prolongaciones.

Si consideramos τ_y la reflexión con respecto a la recta $< y >$, donde $< y >$ es ortogonal a $\mathcal{U}$, entonces para $u\,\varepsilon\,\mathcal{U}$ tenemos que

$$\begin{aligned} \sigma_1 \circ \tau_y(u) &= \sigma_1\left(u - \frac{2B(u,y)}{Q(y)}y\right) \\ &= \sigma_1(u+0) \\ &= \sigma(u) \end{aligned}$$

así, $\sigma_1 \circ \tau_y$ es la otra prolongación de σ.

2) $\mathcal{U}$ no es regular. Demostraremos que $\rho = 1_{\mathcal{V}}$. Sea $rad(\mathcal{U}) = \mathcal{U} \cap \mathcal{U}^{\perp} =< x >$ con $Q(x) = 0$. Por Lema 2 tenemos que $\mathcal{U} = \mathcal{W} \perp rad\ (\mathcal{U})$, donde $\mathcal{W}$ es regular y $\dim \mathcal{W} = n-2$. Por lo tanto

$$\mathcal{V} = \mathcal{W} \perp \mathcal{W}^{\perp} = \mathcal{W} \perp < x, z > \qquad Q(x) = Q(z) = 0$$

Como $\rho\,(\mathcal{W}) = \mathcal{W}$ y además $\rho(x) = x$ y $\rho(z) = \alpha z$ con $\alpha\,\varepsilon\,\mathbb{F}$, de esta manera

$$\begin{aligned} B(x,z) &= B(\rho(x), \rho(z)) \\ &= B(x, \alpha z) \\ &= \alpha B(x,z) \end{aligned}$$

así $\alpha = 1$ y $\rho = 1_{\mathcal{V}}$ en $\mathcal{V}$. De donde $\sigma_2 = \sigma_1$ y así σ tiene sólo una prolongación.

■

3.2. Conjunto Generador de $O_n(\mathcal{V})$

En esta sección mostraremos que las reflexiones forman un conjunto generador de $O_n(\mathcal{V})$.

Lema 3 *Sea $(\mathcal{V}, Q)$ un espacio cuadrático de dimensión n y $\sigma\,\varepsilon\,O_n(\mathcal{V})$ con la siguiente condición:*

$$\forall\, x \text{ anisótropo en } \mathcal{V} \Rightarrow \sigma(x) - x \text{ es isótropo en } \mathcal{V} \qquad (*)$$

entonces $n \geq 4$, par, y σ es una rotación.

Demostración. Sea $n \geq 3$ y $\sigma \,\varepsilon\, O_n(\mathcal{V})$, tal que cumple la condición $(*)$. Afirmamos que $Q(\sigma(x) - x) = 0$ para todo $x \,\varepsilon\, \mathcal{V}$, y no sólo para vectores anisótropos.

Para esto consideremos un vector isótropo $y \,\varepsilon\, \mathcal{V}$, tal que $\sigma(y) \neq y$, de esta manera existe un plano hiperbólico $\mathcal{H} =< y, z >$ con $Q(z) \neq 0$. Por lo tanto

$$\begin{aligned} Q(y + \beta z) &= Q(y) + 2\beta B(y, z) + \beta^2 Q(z) \\ &\neq 0 \end{aligned}$$

para ciertos $\beta \,\varepsilon\, \dot{\mathbb{F}}$. Así

$$Q(\sigma(y + \beta z) - (y + \beta z)) = 0, \qquad Q(\sigma(z) - z) = 0$$

por la condición $(*)$, luego

$$\begin{aligned} 0 &= Q(\sigma(y + \beta z) - (y + \beta z)) \\ &= Q(\sigma(y) - y + \sigma(\beta z) - \beta z) \\ &= Q(\sigma(y) - y) + 2\beta B(\sigma(y) - y, \sigma(z) - z) + \beta Q(\sigma(z) - z) \\ &= Q(\sigma(y) - y) + 2\beta B(\sigma(y) - y, \sigma(z) - z) \end{aligned}$$

entonces usando dos de estos valores obtenemos que $Q(\sigma(y) - y) = 0$ como afirmamos.

De esta forma, existe un subespacio $\mathcal{W} = (\sigma - 1_{\mathcal{V}})(\mathcal{V})$ de $\mathcal{V}$, el cual satisface que $Q(\mathcal{W}) = 0$.

Si consideramos $x \,\varepsilon\, \mathcal{V}$ y $w \,\varepsilon\, \mathcal{W}^{\perp}$, entonces obtenemos

$$\begin{aligned} B(x, \sigma(w) - w) &= B(\sigma(x) - \sigma(x) + x, \sigma(w) - w) \\ &= B(\sigma(x), \sigma(w) - w) - B(\sigma(x) - x, \sigma(w) - w) \\ &= B(\sigma(x), \sigma(w) - w) \\ &= B(\sigma(x), \sigma(w)) - B(\sigma(x), w) \\ &= B(x - \sigma(x), w) \\ &= -B((\sigma - 1)(x), w) \\ &= 0 \end{aligned}$$

Así $\sigma(w) - w \,\varepsilon\, rad\,\mathcal{V}$, pero $\mathcal{V}$ es regular, por lo tanto

$$\sigma(w) = w, \quad \forall\, w \,\varepsilon\, \mathcal{W}^{\perp}$$

Sea $w \,\varepsilon\, \mathcal{W}^{\perp}$ anisótropo, por la condición $(*)$ tenemos que $\sigma(w) - w$ es isótropo, pero esto es una contradicción ya que $\sigma(w) - w = 0$.

Por lo tanto $\forall\, w \,\varepsilon\, \mathcal{W}^{\perp}$, w es isótropo, es decir, $Q(\mathcal{W}^{\perp}) = 0$. Así

$$\mathcal{W} \subseteq \mathcal{W}^{\perp} \subseteq (\mathcal{W}^{\perp})^{\perp} = \mathcal{W}$$

Por lo tanto $\mathcal{W} = \mathcal{W}^{\perp}$. De esta manera n es par y la $\dim \mathcal{W} = \frac{n}{2}$, por el Corolario 5, lo que implica que $\mathcal{V}$ es un espacio hiperbólico y además $\mathcal{W}$ es un espacio totalmente isótropo. Como σ es la identidad en $\mathcal{W}^{\perp} = \mathcal{W}$, por la Proposición 55, σ es una rotación. ■

Teorema 4 *Sea $(\mathcal{V}, Q)$ un espacio cuadrático regular de dimensión n. Entonces $\forall\, \sigma\ \varepsilon\ O_n(\mathcal{V})$, σ es un producto de a lo más n reflexiones.*

Demostración. La demostración se realiza por inducción en n.

$n = 1$ Es fácil al considerar los elementos de $O_1(\mathcal{V})$.

$n > 1$ a) Sea x anisótropo en $\mathcal{V}$ tal que $\sigma(x) = x$.
La restricción de σ al hiperplano $\mathcal{U}$ ortogonal a $< x >$ es un elemento de $O_{n-1}(\mathcal{U})$.
En efecto, sea $y\ \varepsilon\ \mathcal{U}$, entonces

$$\begin{aligned} B(\sigma(y), x) &= B(\sigma(y), \sigma(x)) \\ &= B(y, x) \\ &= 0 \end{aligned}$$

así $\sigma(y)\ \varepsilon\ < x >^{\perp} = \mathcal{U}$. Por hipótesis inductiva, $\sigma \mid_{\mathcal{U}}$ es producto de a lo más $n-1$ reflexiones tomadas con respecto a las rectas de $\mathcal{U}$, es decir

$$\sigma \mid_{\mathcal{U}} = \tau_{x_1}\tau_{x_2}\cdots\tau_{x_{n-1}}$$

con τ_{x_i} reflexiones en $O_{n-1}(\mathcal{U})$, $1 \leq i \leq n-1$.
Cada τ_{x_i} tiene una prolongación natural τ'_{x_i} en $\mathcal{V}$ dada con respecto a su recta de origen $< x_i >$. Esta prolongación está dada de la siguiente forma:
Consideremos $\mathcal{V} = < x > \perp \mathcal{U}$, entonces $v = \alpha x + u\ \varepsilon\ \mathcal{V}$, con $u\ \varepsilon\ \mathcal{U}$, así

$$\begin{aligned} \tau'_{x_i}(\alpha x + u) &= \alpha x + u - \frac{2B(\alpha x + u, x_i)}{Q(x_i)} x_i \\ &= \alpha x + u - \frac{2B(u, x_i)}{Q(x_i)} x_i \\ &= \alpha x + \tau_{x_i}(u) \end{aligned}$$

es la prolongación de τ_{x_i} a $\mathcal{V}$.
Por lo tanto el producto de las τ'_{x_i} con $1 \leq i \leq n$ concuerda con σ tanto en $\mathcal{U}$ como en $< x >$, así

$$\sigma = \tau'_{x_1}\tau'_{x_2}\cdots\tau'_{x_{n-1}} \quad \text{sobre } \mathcal{V}$$

Así σ es producto de a lo más $n-1$ reflexiones cuando deja un vector fijo.

b) Sea $x\ \varepsilon\ \mathcal{V}$ anisótropo tal que $Q(\sigma(x) - x) \neq 0$
De esta manera existe una reflexión $\tau_{\sigma(x)-x}$. Formando $\tau_{\sigma(x)-x}\sigma$, entonces $\tau_{\sigma(x)-x}\sigma$ deja fijo a x, en efecto

$$\begin{aligned} (\tau_{\sigma(x)-x}\sigma)(x) &= \tau_{\sigma(x)-x}(\sigma(x)) \\ &= \sigma(x) - \frac{2B(\sigma(x), \sigma(x) - x)}{Q(\sigma(x) - x)}(\sigma(x) - x) \end{aligned}$$

$$
\begin{aligned}
&= \frac{Q(\sigma(x)-x)\sigma(x) - 2B(\sigma(x),\sigma(x)-x)(\sigma(x)-x)}{Q(\sigma(x)-x)} \\
&= \frac{2B(\sigma(x),\sigma(x))x - 2B(\sigma(x),x)x}{Q(\sigma(x)-x)} \\
&= \frac{2Q(\sigma(x)) - 2B(\sigma(x),x)}{Q(\sigma(x)-x)}x \\
&= x.
\end{aligned}
$$

Por lo anterior tenemos que $\tau_{\sigma(x)-x}\sigma$ es producto de a lo más $n-1$ reflexiones. Por lo tanto σ es producto de a lo más n reflexiones.

c) Sea $x \,\varepsilon\, \mathcal{V}$ anisótropo tal que $Q(\sigma(x)-x)=0$, es decir, que satisface la condición $(*)$, entonces n es par y σ es una rotación. Si fijamos una reflexión τ en $\mathcal{V}$, entonces $\tau\sigma$ es una reflexión, por lo tanto no satisface la condición $(*)$, así $\tau\sigma$ es producto de a lo más n reflexiones, por lo tanto σ es producto de a lo más $n+1$ reflexiones, pero σ no puede ser producto de $n+1$ reflexiones ya que σ es una rotación y $n+1$ es impar.

Por lo tanto σ es producto de a lo mas n reflexiones.

■

Definición 48 *Sea $(\mathcal{V},Q)$ un espacio cuadrático y $\sigma \,\varepsilon\, O_n(\mathcal{V})$. El conjunto*

$$\mathcal{V}_\sigma = \{x \,\varepsilon\, \mathcal{V} \mid \sigma(x) = x\}$$

es el espacio fijo de σ.

Ejemplo 11 *Sea $\sigma \,\varepsilon\, O_n(\mathcal{V})$.*

a) Si $\sigma = -1_{\mathcal{V}}$, entonces $\mathcal{V}_\sigma = \{0\}$

b) Si $\sigma = 1_{\mathcal{V}}$, entonces $\mathcal{V}_\sigma = \mathcal{V}$

c) Sea $(\mathcal{V},Q)$ un espacio cuadrático. Sea $y \,\varepsilon\, \mathcal{V}$ tal que $Q(y) \neq 0$, por lo tanto existe la reflexión τ_y en $\mathcal{V}$, así

$$
\begin{aligned}
\mathcal{V}_{\tau_y} &= \{x \,\varepsilon\, \mathcal{V} \mid \tau_y(x) = x\} \\
&= \{x \,\varepsilon\, \mathcal{V} \mid x - \frac{2B(x,y)}{Q(y)}y = x\} \\
&= \{x \,\varepsilon\, \mathcal{V} \mid B(x,y)y = 0\} \\
&= \{x \,\varepsilon\, \mathcal{V} \mid B(x,y) = 0)\} \\
&= < y >^{\perp}
\end{aligned}
$$

Por lo tanto el espacio fijo de una reflexión es el hiperplano ortogonal a la recta de la definición de la reflexión.

d) *Consideremos el espacio vectorial* $(\mathbb{R}^2, Q)$, *con*

$$\begin{array}{rll} Q: & \mathbb{R}^2 & \to \mathbb{R} \\ & (x,y) & \rightsquigarrow x^2+y^2 \end{array}$$

obtenemos que

$$O_2(\mathbb{R}^2) = \left\{ \begin{pmatrix} \cos(\alpha) & \sin(\alpha) \\ -\sin(\alpha) & \cos(\alpha) \end{pmatrix}, \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix} \mid \alpha \,\varepsilon\, \mathbb{R} \right\}$$

de esta forma

$$\mathbb{R}^2_{\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}} = \{(0,0)\}$$

Corolario 8 *Sea* $(\mathcal{V}, Q)$ *un espacio cuadrático y* $\sigma \,\varepsilon\, O_n(\mathcal{V})$. *Si* σ *es producto de* r *reflexiones, entonces la dimensión de su espacio fijo es al menos* $n-r$.

Demostración. Expresando σ como un producto $\sigma = \tau_1\tau_2\cdots\tau_r$ de reflexiones y sea $\mathcal{U}_i$ el espacio fijo de τ_i para $1 \leq i \leq r$, entonces

$$\mathcal{U}_1 \cap \mathcal{U}_2 \cap \cdots \cap \mathcal{U}_r \subset \mathcal{V}_\sigma$$

por lo tanto basta probar que si $\mathcal{U}_1, \ldots, \mathcal{U}_r$ son hiperplanos de $\mathcal{V}$, entonces

$$\dim(\mathcal{U}_1 \cap \mathcal{U}_2 \cap \cdots \cap \mathcal{U}_r) \geq n-r$$

Hagamos inducción en r

a) $r=1$, por Ejemplo $c)$ anterior, es un hiperplano.

b) $r>1$,

$$\begin{aligned} \dim(\mathcal{U}_1 \cap \mathcal{U}_2 \cap \cdots \cap \mathcal{U}_r) &= \dim(\mathcal{U}_1 \cap \cdots \cap \mathcal{U}_{r-1}) + \dim(\mathcal{U}_r) - \dim((\mathcal{U}_1 \cap \cdots \cap \mathcal{U}_{r-1}) + \mathcal{U}_r) \\ &\geq (n-(r-1)) + (n-1) - (n) = n-r \end{aligned}$$

■

Corolario 9 *Sea* $(\mathcal{V}, Q)$ *un espacio cuadrático y* $\sigma \,\varepsilon\, O_n(\mathcal{V})$, *tal que* σ *es producto de* n *reflexiones. Entonces puede ser expresado como producto de* n *reflexiones con la primera (o la última) escogida arbitrariamente.*

Demostración. Escribamos σ como un producto de n reflexiones, $\sigma = \tau_1\tau_2\cdots\tau_n$. Sea τ una reflexión cualquiera, entonces por el Teorema anterior $\tau\sigma$ puede ser escrito como producto de a lo más n reflexiones

$$\sigma = \tau\tau_2'\tau_3'\cdots\tau_r'$$

donde $r-1 \leq n \Leftrightarrow r \leq n+1$. Aquí el $\det \sigma = (-1)^r$ y por la hipótesis $\det \sigma = (-1)^n$. Por lo tanto r y n tienen la misma paridad. En particular $r \leq n$. Si $r < n$, podemos poner un número par de τ's al final de la expresión anterior para σ y obtener

$$\sigma = \tau\tau_2'\cdots\tau_n'$$

Así podemos elegir la primera reflexión en forma arbitraria. Para el caso de la última elegida arbitrariamente, se procede en forma similar. ■

3.3. Peculiaridades en Dimensión 2 y 3

El grupo ortogonal de espacios de dimensión dos y tres tienen ciertas propiedades especiales que pueden ser usadas en la teoría general. Incidentalmente la teoría del grupo ortogonal en dimensión dos es muy diferente de la teoría en grandes dimensiones.

Proposición 57 *Sea $(\mathcal{V}, Q)$ un espacio cuadrático de dimensión 2, entonces $O_2^+(\mathcal{V})$ es conmutativo.*

Demostración.

a) Sean $\tau, \sigma \; \varepsilon \; O_2(\mathcal{V})$, tal que τ es una reflexión y σ una rotación, entonces

$$\tau\sigma = \tau_1$$

es una reflexión, de esta manera

$$\begin{aligned} \tau\sigma\tau &= \tau_1\tau \\ &= \sigma^{-1} \end{aligned}$$

b) Sean $\sigma, \varrho \; \varepsilon \; O_2^+(\mathcal{V})$, entonces

$$\begin{aligned} \sigma\varrho\sigma^{-1} &= \tau\tau_1\varrho\tau_1\tau \qquad \text{por a)} \\ &= \tau\varrho^{-1}\tau \\ &= \varrho \end{aligned}$$

Por lo tanto $O_2^+(\mathcal{V})$ es conmutativo. ■

Proposición 58 *Sea $(\mathcal{V}, Q)$ un espacio cuadrático regular, con $1 \leq \dim \mathcal{V} \leq 3$ y $\sigma \; \varepsilon \; O_n(\mathcal{V})$ tal que $\dim \mathcal{V}_\sigma = d$, entonces σ es un producto de $n - d$ reflexiones de $\mathcal{V}$.*

Demostración.

I) Supongamos que σ es producto de r reflexiones, con $r < n - d$, entonces

$$d = \dim(\mathcal{V}_\sigma) \geq n - r > d$$

lo cual no es posible.

II) Probemos que σ tiene al menos una expresión como producto de $n - d$ reflexiones.

1) $n = 1$

a) $d = 0$, entonces $\sigma = -1_\mathcal{V}$, así σ es una reflexión.

b) $d = 1$, entonces $\sigma = 1_\mathcal{V}$.

2) $n = 2$

a) $d = 0$, supongamos que existe $y \,\varepsilon\, \mathcal{V}$ tal que $Q(y) \neq 0$ y $\sigma = \tau_y$, entonces

$$\{0\} = \mathcal{V}_{\tau_y} =< y >^{\perp}$$

lo cual no puede ser ya que $\dim < y >^{\perp} = 1$, entonces $1_{\mathcal{V}} \neq \sigma \neq \tau_y$.

Por lo tanto σ es una rotación.

b) $d = 1$, como $\mathcal{V}_\sigma \leq \mathcal{V}$ de dimensión 1, entonces $\mathcal{V}_\sigma$ es regular, entonces $\mathcal{V} = \mathcal{V}_\sigma \perp \mathcal{V}_\sigma^{\perp}$. Así σ es una reflexión con respecto a la recta ortogonal a $\mathcal{V}_\sigma$.

c) $d = 2$, $\sigma = 1_{\mathcal{V}}$.

3) $n = 3$

a) $d = 0$

- Si σ es producto de 1 reflexión, entonces $\dim \mathcal{V}_\sigma = 2$, lo cual es una contradicción.

- Supongamos que $\sigma = \tau_y \tau_x$, con $x, y \,\varepsilon\, \mathcal{V}$ y $Q(y) = Q(x) \neq 0$, así

$$\begin{aligned}
\mathcal{V}_\sigma &= \{z \,\varepsilon\, \mathcal{V} \mid \tau_y(\tau_x(z)) = z\} \\
&= \{z \,\varepsilon\, \mathcal{V} \mid \tau_y\left(z - \frac{2B(x,z)}{Q(x)}x\right) = z\} \\
&= \{z \,\varepsilon\, \mathcal{V} \mid \tau_y(z) - \frac{2B(x,z)}{Q(x)}\tau_y(x) = z\} \\
&= \{z \,\varepsilon\, \mathcal{V} \mid z - \frac{2B(y,z)}{Q(y)}y - \frac{2B(x,z)}{Q(x)}\left(x - \frac{2B(y,x)}{Q(y)}y\right) = z\} \\
&= \{z \,\varepsilon\, \mathcal{V} \mid \left(\frac{4B(x,z)B(y,x)}{Q(y)Q(x)} - \frac{2B(y,z)}{Q(y)}\right)y = \frac{2B(x,z)}{Q(x)}x\}
\end{aligned}$$

Así la $\dim \mathcal{V}_\sigma$ es al menos 1, lo cual es una contradicción. Por lo tanto σ es producto de tres reflexiones.

b) $d = 1$, entonces $\mathcal{V}_\sigma =< x >$ con $x \,\varepsilon\, \mathcal{V}$. Luego es necesario mostrar que σ es una rotación.

Supongamos que σ es una reflexión, entonces $-\sigma$ es una rotación, por lo tanto $-\sigma$ deja fijo un vector, es decir $-\sigma(y) = y$ y σ invierte otro, $\sigma(z) = -z$. Estos dos vectores son independientes, en efecto, sean $y, z \,\varepsilon\, \mathcal{V}$ no nulos y $\alpha, \beta \,\varepsilon\, \mathbb{F}$, tal que $\sigma(z) = -z$ y $-\sigma(y) = y$. Supongamos que $\alpha y + \beta z = 0$, así

$$\begin{aligned}
\sigma(\alpha y + \beta z) &= 0 \\
\alpha\sigma(y) + \beta\sigma(z) &= 0 \\
\beta\sigma(z) &= \alpha - \sigma(y) \\
\beta z = \alpha y &
\end{aligned}$$

de esta manera, $2\alpha y = 0$, entonces $\alpha = 0$ y a su vez $\beta = 0$, por lo tanto $\{y, z\}$ es linealmente independiente.

De esta forma $\sigma^2(w) = w$, para todo $w \varepsilon\ < y, z >$. A su vez σ^2 es una rotación; de esta manera $\sigma^2 = 1_{\mathcal{V}}$ por la Proposición 56. Así σ es una reflexión y una involución, entonces por la Proposición 51, $\sigma = -1_{\mathcal{V}}$ o una reflexión, lo cual es imposible, ya que $\dim \mathcal{V}_\sigma = 1$. Por lo tanto σ es una rotación.

c) $d = 2$, entonces $\mathcal{V}_\sigma = \mathcal{P}$, donde $\mathcal{P}$ es un plano, el cual es regular, así σ es una reflexión con respecto a la recta ortogonal $\mathcal{P}$.

d) $d = 3$, entonces σ es la identidad.

■

La ultima Proposición muestra que para espacios de dimensión 3 el espacio fijo de cualquier rotación, distinta de la identidad, es una recta. A esta recta la llamaremos el eje de rotación. El conjunto de todas las rotaciones con un eje dado es un subgrupo de $O_3^+(\mathcal{V})$.

Proposición 59 *Sea L una recta anisótropa y O_L el grupo de rotación que tienen como eje a L, entonces existe un isomorfismo natural de O_L sobre el grupo $O_2^+(L^\perp)$.*

Proposición 60 *Sea L una recta isótropa en un espacio cuadrático regular $(\mathcal{V}, Q)$ de dimensión 3, entonces existe un isomorfismo de grupos entre $(O_L, \cdot)$ y $(\mathbb{F}, +)$.*

Demostración. Sea $L =< x >$ con $x \varepsilon \mathcal{V}$. Podemos obtener la suma ortogonal

$$\mathcal{V} =< x, y > \perp < z >$$

donde $Q(x) = Q(y) = 0$, $B(x, y) = 1$. Sea $\mathcal{U}$ un plano, tal que $\mathcal{U} =< x > \perp < z >$, donde $rad\mathcal{U} =< x >$.

Consideremos $\alpha \varepsilon \mathbb{F}$ y definamos una función

$$\begin{aligned} \rho : \ \mathcal{U} &\to \mathcal{V} \\ x &\rightsquigarrow x \\ z &\rightsquigarrow \alpha x + z \end{aligned}$$

la cual es una isometría, en efecto

$$\begin{aligned} B(\rho(x), \rho(z)) &= B(x, \alpha x + z) \\ &= B(x, \alpha x) + B(x, z) \\ &= B(x, z) \end{aligned}$$

El Teorema de Witt nos dice que existe una prolongación de ρ a una isometría de $\mathcal{V}$ sobre $\mathcal{V}$, esta prolongación es única ya que $\mathcal{U}$ no es regular. De esta forma asociamos esta única isometría de $\mathcal{V}$ sobre $\mathcal{V}$ con α. Esta isometría la escribimos como ρ_α y se define de la siguiente forma:

$$\begin{aligned} \rho_\alpha : \ \mathcal{V} &\to \mathcal{V} \\ x &\rightsquigarrow x \\ z &\rightsquigarrow \alpha x + z \end{aligned}$$

donde $\rho_{\alpha+\beta} = \rho_\alpha \rho_\beta$ y, en particular $\rho_\alpha = \rho^2_{\alpha/2}$, de esta manera ρ_α es siempre una rotación, con $< x >$ como el eje de rotación. Así obtenemos el homomorfismo definido por:

$$\begin{aligned} \phi : \ \mathbb{F} &\to O_{<x>} \\ \alpha &\rightsquigarrow \rho_\alpha \end{aligned}$$

Además,

i) Sea $\alpha \ \varepsilon \ \ker \phi$, entonces

$$\begin{array}{rcll} \phi(\alpha) &=& 1_{\mathcal{V}} & \\ \rho_\alpha &=& 1_{\mathcal{V}} & /z \\ \rho_\alpha(z) &=& z & \\ \alpha x + z &=& z & \\ \alpha x &=& 0 & \\ \alpha = 0 &\vee& x = 0 & \end{array}$$

como $x \neq 0$, entonces ϕ es inyectiva.

ii) Epiyectividad. Sea $\sigma \ \varepsilon \ O_3^+(\mathcal{V})$ con $\mathcal{V}_\sigma =< x >$ y escribiendo

$$\begin{array}{rcl} \sigma(x) &=& x \\ \sigma(y) &=& ax + by + cz \\ \sigma(z) &=& dx + ey + fz \end{array}$$

como $< x, y >$ es un plano hiperbólico, entonces $B(\sigma(x), \sigma(y)) = 1$, así $b = 1$.
Además $\mathcal{U} =< x > \perp < z >$, entonces $e = 0$. Si consideramos $\mathcal{B} = \{x, y, z\}$ una base para $\mathcal{V}$, entonces

$$[\sigma]_{\mathcal{B}} = \begin{pmatrix} 1 & a & d \\ 0 & b & e \\ 0 & c & f \end{pmatrix} = \begin{pmatrix} 1 & a & d \\ 0 & 1 & 0 \\ 0 & c & f \end{pmatrix}$$

como el $\det \sigma = 1$, entonces $f = 1$, así σ queda como

$$\begin{array}{rcl} \sigma(x) &=& x \\ \sigma(y) &=& ax + y + cz \\ \sigma(z) &=& dx + z \end{array}$$

por lo tanto σ en $\mathcal{U}$ esta dada como

$$\sigma(x) = x \qquad \sigma(z) = dx + z$$

así σ y ρ_d coinciden en $\mathcal{U}$ y como $\mathcal{U}$ no es regular, entonces $\sigma = \rho_d$. Así ϕ es epiyectiva y por lo tanto un isomorfismo

■

Corolario 10 *Toda rotación en un eje isótropo es el cuadrado de una rotación en el mismo eje. Hay al menos una rotación en este eje la cual no es la identidad.*

3.4. El subgrupo conmutador de $O_n(\mathcal{V})$

Denotaremos por Ω_n al subgrupo conmutador del grupo ortogonal $O_n(\mathcal{V})$ de un espacio cuadrático regular $(\mathcal{V}, Q)$.

Proposición 61 *El conmutador Ω_n está generado por elementos de la forma $[\tau_x, \tau_y] = \tau_x\tau_y\tau_x^{-1}\tau_y^{-1}$. Además contiene los cuadrados de todos los elementos de $O_n(\mathcal{V})$ y en particular esta generado por los cuadrados de los elementos de $O_n^+(\mathcal{V})$.*

Demostración. Sea G un subgrupo de $O_n(\mathcal{V})$ que está generado por el conmutador $[\tau_x, \tau_y] = \tau_x\tau_y\tau_x^{-1}\tau_y^{-1} = (\tau_x\tau_y)^2$. Para cualquier $\sigma \,\varepsilon\, O_n(\mathcal{V})$ tenemos que $\sigma\tau_x\sigma^{-1} = \tau_{\sigma(x)}$, entonces

$$\sigma[\tau_x, \tau_y]\sigma^{-1} = [\tau_{\sigma(x)}, \tau_{\sigma(y)}]$$

por lo tanto G es un subgrupo normal de $O_n(\mathcal{V})$. Así podemos definir la proyección canónica

$$\begin{array}{rll} ^{-}: & O_n(\mathcal{V}) & \to O_n(\mathcal{V})/G \\ & \tau_x & \rightsquigarrow \overline{\tau_x} \end{array}$$

y tenemos que $\overline{[\tau_x, \tau_y]} = 1$, es decir, $\overline{\tau_x\tau_y} = \overline{\tau_y\tau_x}$.

De esta manera, si consideramos $\sigma, \varrho \,\varepsilon\, O_n(\mathcal{V})$ y las escribimos en términos de reflexiones, resulta que

$$\sigma = \tau_1\tau_2\cdots\tau_m \quad \text{y} \quad \varrho = \tau_{m+1}\tau_{m+2}\cdots\tau_r$$

tenemos

$$\overline{\sigma}\,\overline{\varrho} = \overline{\tau_1}\cdots\overline{\tau_m}\;\overline{\tau_{m+1}}\cdots\overline{\tau_r} = \overline{\tau_{m+1}}\cdots\overline{\tau_r\tau_1}\;\cdots\overline{\tau_m} = \overline{\varrho}\,\overline{\sigma}$$

por lo tanto $O_n(\mathcal{V})/G$ es conmutativo. Luego

$$\begin{array}{rcl} \overline{\sigma\rho} & = & \overline{\rho\sigma} \\ \overline{\sigma\rho\sigma^{-1}\rho^{-1}} & = & 1 \end{array}$$

de esta manera $\sigma\rho\sigma^{-1}\rho^{-1} \,\varepsilon\, G$, por lo tanto así $\Omega_n \subseteq G$, pero $G \subseteq \Omega_n$ por definición. Por lo tanto $G = \Omega_n$.

Finalmente, sea $\sigma \,\varepsilon\, O_n(\mathcal{V})$, entonces tenemos

$$\overline{\sigma}^2 = \overline{\tau_1}\cdots\overline{\tau_m}\;\overline{\tau_1}\cdots\overline{\tau_m} = \overline{\tau_1\tau_1}\cdots\overline{\tau_m\tau_m} = 1$$

Por lo tanto $\sigma^2 \,\varepsilon\, G = \Omega_n$. Así Ω_n contiene los cuadrados de todos los elementos de $O_n(\mathcal{V})$.

Pero Ω_n está generado por lo cuadrados $(\tau_x\tau_y)^2$ por definición de $G = \Omega_n$. Por lo tanto Ω_n está generado por los cuadrados de todos los elementos de $O_n^+(\mathcal{V})$. ■

Proposición 62 *Ω_n es también el subgrupo conmutador de $O_n^+(\mathcal{V})$ cuando $n \geq 3$.*

Demostración. Sea Ω_n^+ el subgrupo conmutador de $O_n^+(\mathcal{V})$, solo bastaría demostrar que es igual a Ω_n.

$\subseteq$) Como $O_n^+(\mathcal{V}) \leq O_n(\mathcal{V})$, entonces $\Omega_n^+ \subseteq \Omega_n$.

$\supseteq$) Como Ω_n está generado por el conmutador $[\tau_x, \tau_y]$, donde τ_x, τ_y son reflexiones de $\mathcal{V}$. Hay que demostrar que $[\tau_x, \tau_y] \; \varepsilon \; \Omega_n^+$.

Sean $x, y \; \varepsilon \; \mathcal{V}$ anisótropo, entonces existe $\mathcal{U}$ subespacio regular de dimensión 3 de $\mathcal{V}$, tal que $< x, y > \; \varepsilon \, \mathcal{U}$, en efecto

a) Si $< x, y >$ es regular, existe $< x, y >^{\perp}$ anisótropo, luego

$$\mathcal{U} = < x, y > \perp < z >$$

b) Si $< x, y >$ no es regular, entonces $rad\,(< x, y >) = < z >$. Así

$$< x, y > = < x, z >$$

De esta manera, $z \; \varepsilon \; < x >^{\perp}$ y $Q(z) = 0$, luego existe $w \; \varepsilon \; < x >^{\perp}$ tal que $< z, w >$ es un plano hiperbólico, así

$$\mathcal{U} = < x, z, w >$$

Por lo tanto

$$\mathcal{V} = \mathcal{U} \perp \mathcal{W}$$

Consideremos $\overline{\tau_x}$ y $\overline{\tau_y}$ reflexiones de $\mathcal{U}$ con respecto a x e y respectivamente y $1_{\mathcal{W}} \; \varepsilon \; O_{n-3}(\mathcal{W})$, entonces

$$\begin{aligned} [\tau_x, \tau_y] &= \tau_x \tau_y \tau_x \tau_y \\ &= (\overline{\tau_x}\,\overline{\tau_y}\,\overline{\tau_x}\,\overline{\tau_y}) \perp 1_{\mathcal{W}} \\ &= (-\overline{\tau_x} \perp 1_{\mathcal{W}})(-\overline{\tau_y} \perp 1_{\mathcal{W}})(-\overline{\tau_x} \perp 1_{\mathcal{W}})(-\overline{\tau_y} \perp 1_{\mathcal{W}}) \end{aligned}$$

así $-\overline{\tau_x}$ es una rotación, ya que τ_x es una reflexión, además

$$(-\overline{\tau_x} \perp 1_{\mathcal{W}})(-\overline{\tau_x} \perp 1_{\mathcal{W}}) = (\overline{\tau_x}^2 \perp 1_{\mathcal{W}}) = (1_{\mathcal{U}} \perp 1_{\mathcal{W}}) = 1_{\mathcal{V}}$$

por lo tanto

$$(-\overline{\tau_x} \perp 1_{\mathcal{W}})^{-1} = (-\overline{\tau_x} \perp 1_{\mathcal{W}})$$

lo mismo ocurre para $(-\overline{\tau_y} \perp 1_{\mathcal{W}})$. Así $[\tau_x, \tau_y]$ es un conmutador de elementos de $O_n^+(\mathcal{V})$.

Por lo tanto $[\tau_x, \tau_y] \; \varepsilon \; \Omega_n^+$.

■

Observación. Cuando $\dim \mathcal{V} = 1$ el grupo O_1 es un grupo de dos elementos, de esta manera su estructura es trivial.

Si $\dim \mathcal{V} = 2$ conocemos que O_2^+ es conmutativo, luego su subgrupo conmutador es $1_{\mathcal{V}}$. Veremos más adelante que $\Omega_2 = 1_v$, si y sólo si $\mathcal{V}$ es un plano hiperbólico sobre un cuerpo de tres elementos; en particular la Proposición anterior es cierta para espacios de dimensión dos.

Conocemos que el subgrupo conmutador Ω_2 de O_2 está generado por el conjunto de cuadrados de todas las rotaciones; pero este conjunto es un grupo donde O_2^+ es conmutativo; por lo tanto Ω_2 es el conjunto de cuadrados de todas las rotaciones.

3.5. El centro de $O_n(\mathcal{V})$

Denotaremos como Z_n al centro de $O_n(\mathcal{V})$.

Proposición 63 *Sea $(\mathcal{V}, Q)$ un espacio cuadrático regular y $\sigma \,\varepsilon\, O_n(\mathcal{V})$, la cual deja todas las rectas fijas. Entonces $\sigma = \pm 1_{\mathcal{V}}$.*

Demostración. Sea $x \,\varepsilon\, \mathcal{V}$ fijo tal que $Q(x) \neq 0$. Sea $\sigma \,\varepsilon\, O_n$ tal que $\sigma(x) = \alpha x$ por hipótesis, entonces

$$\begin{aligned} \alpha^2 Q(x) &= Q(\alpha x) \\ &= Q(\sigma(x)) \\ &= Q(x) \end{aligned}$$

por lo tanto $\alpha = \pm 1$, ya que $\alpha^2 = 1$. Luego para todo $z \,\varepsilon\, < x >$, tenemos que $\sigma(z) = \alpha z$.

Consideremos $\{x, y\}$ linealmente independientes, así tenemos que $\sigma(y) = \beta y$ para algún $\beta \,\varepsilon\, \mathbb{F}$. Queda demostrar que $\alpha = \beta$. Para ello sabemos que, $\sigma(x + y) = \gamma(x + y)$ con $\gamma \,\varepsilon\, \mathbb{F}$, por hipótesis, así

$$\begin{aligned} \alpha x + \beta y &= \sigma(x) + \sigma(y) \\ &= \sigma(x + y) \\ &= \gamma(x + y) \\ &= \gamma x + \gamma y \end{aligned}$$

por lo tanto $\alpha = \gamma = \beta$. ■

Proposición 64 *Sea $(\mathcal{V}, Q)$ un espacio cuadrático regular isótropo, donde* $\dim \mathcal{V} = n$, *con $n \geq 3$ y $\sigma \,\varepsilon\, O_n(\mathcal{V})$, la cual deja toda recta isótropa fija. Entonces $\sigma = \pm 1_{\mathcal{V}}$.*

Demostración. Como $\mathcal{V}$ es isótropo, entonces tiene como sumando ortogonal a un plano hiperbólico $\mathcal{H}$. Así

$$\mathcal{V} = \mathcal{H} \perp \mathcal{H}^{\perp}$$

Notemos que $\sigma(\mathcal{H}) = \mathcal{H}$, ya que es generado por dos rectas isótropas.

Probemos que σ deja toda recta fija de $\mathcal{H}^{\perp}$.

Sea $z \,\varepsilon\, \mathcal{H}^{\perp}$, tal que $Q(z) \neq 0$. Sabemos que $(\mathcal{H}, Q)$ es universal, entonces $-Q(z) \,\varepsilon\, Q(\mathcal{H})$, por Proposición 32, así existe $x \,\varepsilon\, \mathcal{H}$ tal que $Q(x) = -Q(z)$, además $x + z$ es un vector isótropo, ya que

$$\begin{aligned} Q(x + z) &= Q(x) + Q(z) + 2B(x, z) \\ &= -Q(z) + Q(z) + 0 \\ &= 0 \end{aligned}$$

luego tenemos que $\mathcal{H}' =< x+z, z >$ es un plano hiperbólico, entonces existe $y \,\varepsilon\, < z >\perp \mathcal{H}$ tal que $Q(y) = 0$ y

$$\mathcal{H}' =< x+z, y > \leq < z >\perp \mathcal{H}$$

Como $\sigma(\mathcal{H}') = \mathcal{H}'$, entonces

$$\sigma(z) \,\varepsilon\, < z >\perp \mathcal{H}$$

pero $\sigma(\mathcal{H}) = \mathcal{H}$, por lo tanto

$$\sigma(z) \perp \mathcal{H}$$

Con lo cual tenemos que $\sigma(z) \,\varepsilon\, < z >$. Por lo tanto σ deja toda recta de $\mathcal{H}^{\perp}$ fija. Por la Proposición anterior, tenemos que $\sigma = \pm 1_{\mathcal{H}^{\perp}}$. Podemos suponer que $\sigma(z) = z$ para todo $z \,\varepsilon\, \mathcal{H}^{\perp}$, reemplazando σ por $-\sigma$.

Ahora probaremos que $\sigma\mid_{\mathcal{H}} = 1_{\mathcal{H}}$. Como σ fija las rectas isótropas, $\sigma\mid_{\mathcal{H}}$ es una rotación, como probamos en el Ejemplo 10. Una rotación en espacios de dimensión dos, fija al 0 o a todo el espacio.

Como $x+z$ es isótropo, entonces $\sigma(x+z) = \alpha(x+z)$, por hipótesis. De esta manera

$$\alpha x + \alpha z = \sigma(x+z) = \sigma(x) + z$$

entonces

$$\begin{aligned} \alpha x + \alpha z - z &= \sigma(x) \\ \alpha x + (\alpha - 1)z &= \sigma(x) \quad \varepsilon\, \mathcal{H} \end{aligned}$$

De esta manera $\alpha = 1$ y $\sigma(x) = x$. Por lo tanto $\sigma\mid_{\mathcal{H}} = 1_{\mathcal{H}}$. Con esto, hemos demostrado que

$$\sigma\mid_{\mathcal{H}} = 1_{\mathcal{H}} \qquad \text{y} \qquad \sigma\mid_{\mathcal{H}^{\perp}} = 1_{\mathcal{H}^{\perp}}$$

Luego obtenemos $\sigma = \pm 1_{\mathcal{V}}$. ■

Proposición 65 *Sea $(\mathcal{V}, Q)$ un espacio cuadrático regular de dimensión n, distinto de un plano hiperbólico sobre un cuerpo de 3 elementos y sea $\sigma \,\varepsilon\, O_n(\mathcal{V})$, la cual deja toda recta anisótropa fija, entonces $\sigma = \pm 1_{\mathcal{V}}$.*

Demostración.

$n = 1$ Trivial.

$n \geq 2$ a) Si $\mathcal{V}$ es anisótropo, se sigue por la demostración de la Proposición 63.

b) Si $\mathcal{V}$ es isótropo.

$n = 2$ Aquí $\mathcal{V}$ es un plano hiperbólico. Si σ deja las dos rectas isótropas fijas, entonces deja todas las rectas fijas, la demostración sigue de la Proposición 63.

Supongamos que σ intercambia las 2 rectas isótropas. Por Ejemplo 10, σ es una reflexión, con respecto a una recta $< x >$, es decir, $\sigma = \tau_x$. Consideremos

$< y >$ una recta ortogonal a $< x >$ y un vector anisótropo de la forma: $x+\alpha y$ con $\alpha \varepsilon \mathbb{F}$. Entonces

$$\sigma(x) = -x \qquad \sigma(y) = y \qquad \sigma(x+\alpha y) = \gamma(x+\alpha y)$$

para algún $\gamma \varepsilon \mathbb{F}$. De esta manera

$$\gamma x + \gamma\alpha y = \sigma(x+\alpha y) = -x + \alpha y$$

de donde obtenemos que $\alpha = 0$. En otras palabras $< x >$ y $< y >$ son las únicas rectas anisótropas en $\mathcal{V}$. Pero hay al menos cuatro rectas anisótropas en un plano hiperbólicos sobre un cuerpo de cinco o más elementos. Por lo tanto, nuestra suposición de que σ intercambia las rectas isótropas de $\mathcal{V}$ es inaceptable. Así $\sigma = \pm 1_{\mathcal{V}}$.

$n \geq 3$ Todo plano regular en $\mathcal{V}$ es generado por 2 rectas anisótropas, por lo tanto es fijo por σ. Si podemos demostrar que todo vector isótropo x pertenece a dos planos hiperbólicos distintos, entonces $\sigma(x)$ pertenece a cada uno de estos planos y así en $< x >$; esto implicaría que toda recta isótropa, así toda recta, queda fija por σ. Encontremos dos planos hiperbólicos que contengan a x.

Existe al menos un plano hiperbólico $\mathcal{H} =< x, y >$ que contiene a x dado que $\mathcal{V}$ es regular.

Tomando un vector no nulo z ortogonal a $\mathcal{H}$, entonces $\mathcal{H}' =< x, y+z >$ es otro plano hiperbólico que contiene a x y distinto de $\mathcal{H}$. De esta forma $\sigma(x) \varepsilon < x >$ para todo x isótropo.

Por lo tanto, como σ deja toda recta fija, de la Proposición 63, obtenemos que $\sigma = \pm 1_{\mathcal{V}}$.

■

Proposición 66 *Sea $(\mathcal{V}, Q)$ un espacio cuadrático regular. Entonces $\mathrm{Z}_n = \{\pm 1_{\mathcal{V}}\}$ con una única excepción, cuando $\mathcal{V}$ es un plano hiperbólico sobre un cuerpo de tres elementos. En este caso $\mathrm{Z}_2 = O_2(\mathcal{V})$.*

Demostración.

$\supseteq$) Claramente $\pm 1_{\mathcal{V}} \varepsilon \mathrm{Z}_n$.

$\subseteq$) Sean $\sigma \varepsilon \mathrm{Z}_n$ y $< x >$ una recta anisótropa en $\mathcal{V}$, entonces consideremos la reflexión τ_x así

$$\tau_x = \sigma \circ \tau_x \circ \sigma^{-1} = \tau_{\sigma(x)}$$

Por lo tanto $\sigma(x) \varepsilon < x >$. De esta manera σ deja toda recta anisótropa fija, así $\sigma = \pm 1_{\mathcal{V}}$ por Proposición anterior.

Veamos el caso en que $\mathcal{V}$ es un plano hiperbólico sobre un cuerpo de tres elementos.

Aquí $\mathcal{V}$ contiene dos rectas anisótropas distintas, por lo tanto $O_2^-(\mathcal{V})$ contiene dos reflexiones distintas, de esta manera $|O_2(\mathcal{V})| = 4$ y todo grupo de orden cuatro es conmutativo.

■

Corolario 11 *$O_n(\mathcal{V})$ es conmutativo en exactamente dos casos, cuando $n = 1$ y $\mathcal{V}$ es un plano hiperbólico sobre un cuerpo de tres elementos. En otro caso, no es conmutativo.*

Demostración. Miremos el caso de $n > 1$.

Aquí $\mathcal{V}$ tiene 2 o más rectas anisótropas (por ejemplo, las rectas en una base ortogonal) y de esta manera $O_n(\mathcal{V})$ tiene a lo menos orden 4. En particular $O_n(\mathcal{V}) \neq \{\pm 1_{\mathcal{V}}\}$. ■

Corolario 12 *$O_n^+(\mathcal{V})$ es conmutativo cuando $n = 1, 2$, para $n \geq 3$ no es conmutativo.*

Demostración. La conmutatividad de $O_1^+(\mathcal{V})$ es evidente, para $O_2^+(\mathcal{V})$ ya está probado en la Proposición 57.

Para $n \geq 3$, tenemos que $\Omega_n \neq 1_{\mathcal{V}}$, ya que $O_n(\mathcal{V})$ no es conmutativo, pero Ω_n es el subgrupo conmutador de $O_n^+(\mathcal{V})$. Por lo tanto $O_n^+(\mathcal{V})$ no es conmutativo. ■

Proposición 67 *Sea $(\mathcal{V}, Q)$ un espacio cuadrático regular. El centralizador de Ω_n en $O_n(\mathcal{V})$ es Z_n, cuando $n \geq 3$.*

Demostración. Tomaremos $\sigma \,\varepsilon\, O_n(\mathcal{V})$ tal que conmute con todo elemento de Ω_n y probaremos que $\sigma \,\varepsilon\, \mathrm{Z}_n$.

1) Sea $\mathcal{V}$ anisótropo. Probaremos que todo plano queda fijo por σ y así probar que deja toda recta fija y por Proposición 63, $\sigma = \pm 1$.

   Consideremos un plano $\mathcal{P}$ en $\mathcal{V}$ y sea $\mathcal{V} = \mathcal{P} \perp \mathcal{W}$ la correspondiente suma ortogonal de $\mathcal{V}$.

   Como $\mathcal{P}$ es anisótropo, este contiene a lo menos 3 rectas anisótropas, de esta manera $O_2^+(\mathcal{P})$ tiene a lo menos 3 rotaciones; en un espacio de dimensión 2 existen exactamente dos involuciones que son rotaciones, las cuales son $\pm 1_{\mathcal{P}}$; de esta manera existe $\rho \,\varepsilon\, O_2^+(\mathcal{P})$ tal que $\rho^2 \neq 1_{\mathcal{V}}$.

   Considerando $\overline{\rho} = \rho \perp 1_{\mathcal{W}}$, entonces $\mathcal{W}$ es el espacio fijo de $\overline{\rho}^2$, ya que

$$\overline{\rho}^2\,(\mathcal{W}) = \rho^2 \perp 1_{\mathcal{W}}\,(\mathcal{W}) = \mathcal{W}$$

   además $\mathcal{V}_{\rho^2} = \{0\}$ y

$$\begin{aligned} \mathcal{V}_{\sigma\circ\overline{\rho}^2\circ\sigma^{-1}} &= \{x \,\varepsilon\, \mathcal{V} \mid \sigma \circ \overline{\rho}^2 \circ \sigma^{-1}(x) = x\} \\ &= \{x \,\varepsilon\, \mathcal{V} \mid \overline{\rho}^2(\sigma^{-1}(x)) = \sigma^{-1}(x)\} \\ &= \{x \,\varepsilon\, \mathcal{V} \mid \sigma^{-1}(x) \,\varepsilon\, \mathcal{W}\} \\ &= \sigma(\mathcal{W}) \end{aligned}$$

pero $\overline{\rho}^2 \,\varepsilon\, \Omega_n$, entonces $\sigma \circ \overline{\rho}^2 \circ \sigma^{-1} = \overline{\rho}^2$ por hipótesis, de esta manera $\mathcal{V}_{\overline{\rho}^2} = \sigma(\mathcal{W})$.

Por lo tanto $\sigma(\mathcal{W}) = \mathcal{W}$ y así $\sigma(\mathcal{P}) = \mathcal{P}$. El resultado es consecuencia inmediata de lo anterior y la Proposición 63.

2) Sea $\mathcal{V}$ isótropo. Por la Proposición 64 es necesario probar que σ deja toda recta isótropa fija. Para esto consideremos $< x >$ una recta isótropa, entonces existe un plano hiperbólico $\mathcal{H} =< x, z >$ con $Q(z) = 0$ y a su vez un subespacio regular $\mathcal{U}$ de dimensión 3 de $\mathcal{V}$, el cual contiene a $< x >$.

Tomando la suma ortogonal $\mathcal{V} = \mathcal{U} \perp \mathcal{W}$. Por el Corolario 10, existe $\rho \,\varepsilon\, O_3^+(\mathcal{U})$ la cual tiene como eje a $< x >$ y $\rho^2 \neq 1_{\mathcal{V}}$.

Colocando $\overline{\rho} = \rho \perp 1_{\mathcal{W}}$, entonces

$$\mathcal{V}_{\overline{\rho}^2} =< x >\perp \mathcal{W}$$

donde $\mathcal{V}_{\rho^2} =< x >$ y además

$$\begin{aligned}
\mathcal{V}_{\sigma\circ\overline{\rho}^2\circ\sigma^{-1}} &= \{y \,\varepsilon\, \mathcal{V} \mid \sigma \circ \overline{\rho}^2 \circ \sigma^{-1}(y) = y\} \\
&= \{y \,\varepsilon\, \mathcal{V} \mid \overline{\rho}^2(\sigma^{-1}(y)) = \sigma^{-1}(y)\} \\
&= \{y \,\varepsilon\, \mathcal{V} \mid \sigma^{-1}(y) \,\varepsilon\, < x >\perp \mathcal{W}\} \\
&= < \sigma(x) >\perp \sigma(\mathcal{W})
\end{aligned}$$

pero $\overline{\rho}^2 \,\varepsilon\, \Omega_n$, entonces $\sigma \circ \overline{\rho}^2 \circ \sigma^{-1} = \overline{\rho}^2$ por hipótesis, de esta manera $\mathcal{V}_{\overline{\rho}^2} =< \sigma(x) >\perp \sigma(\mathcal{W})$.

Por lo tanto

$$< \sigma(x) >\perp \sigma(\mathcal{W}) =< x >\perp \mathcal{W}$$

por Proposición 38, tenemos que

$$\begin{aligned}
rad(< x >\perp \mathcal{W}) &= rad(< x >) + rad(\mathcal{W}) \\
&= < x >
\end{aligned}$$

así, $< \sigma(x) >=< x >$ y entonces $\sigma(x) = x$, por lo tanto σ deja toda recta isótropa fija.

■

Corolario 13 *Sea $n \geq 3$. Entonces el centro de $O_n^+(\mathcal{V})$ es $O_n^+(\mathcal{V}) \cap \mathrm{Z}_n$ y el centro de Ω_n es $\Omega_n \cap \mathrm{Z}_n$.*

3.6. Representación Irreducible de Ω_n

El siguiente resultado muestra que $\mathcal{V}$, es una representación irreducible de Ω_n.

Proposición 68 *Sea $(\mathcal{V}, Q)$ un espacio cuadrático regular de dimensión n, con $n \geq 3$ y $\mathcal{U}$ un subespacio de $\mathcal{V}$ donde $0 \subset \mathcal{U} \subset \mathcal{V}$, entonces existe $\sigma \; \varepsilon \; \Omega_n$ tal que $\sigma(\mathcal{U}) \neq \mathcal{U}$.*

Demostración.

1) $\mathcal{U}$ es regular.

Consideremos la suma ortogonal $\mathcal{V} = \mathcal{U} \perp \mathcal{W}$ y consideremos la involución $-1_{\mathcal{U}} \perp 1_{\mathcal{W}}$. Entonces, existe $\sigma \; \varepsilon \; \Omega_n$ la cual no conmuta con $-1_{\mathcal{U}} \perp 1_{\mathcal{W}}$ ya que el centralizador de Ω_n en $O_n(\mathcal{V})$ es $\{\pm 1_{\mathcal{V}}\}$.

Supongamos que $\sigma(\mathcal{U}) = \mathcal{U}$, entonces $\sigma = \tau \perp \rho$, con $\tau \; \varepsilon \; O_n(\mathcal{U})$ y $\rho \; \varepsilon \; O_m(\mathcal{W})$, de esta manera

$$(\tau \perp \rho)(-1_{\mathcal{U}} \perp 1_{\mathcal{W}}) = (-1_{\mathcal{U}} \perp 1_{\mathcal{W}})(\tau \perp \rho)$$

lo cual es una contradicción. Por lo tanto $\sigma(\mathcal{U}) \neq \mathcal{U}$

2) $\mathcal{U}$ no es regular.

Reemplazando $\mathcal{U}$ por $rad(\mathcal{U})$, si es necesario, para asumir que $Q(\mathcal{U}) = 0$.

Sea $x \; \varepsilon \; \mathcal{U}$, luego existe $y \; \varepsilon \; \mathcal{V}$, tal que $\mathcal{H} =< x, y >$ es un plano hiperbólico, luego existe $z \; \varepsilon \; \mathcal{H}^{\perp}$ anisótropo, entonces

$$\mathcal{T} =< x, y > \perp < z >$$

es regular, tal que $\mathcal{U} \cap \mathcal{T} =< x >$.

Por Corolario 10, existe $\sigma \; \varepsilon \; O_3^+(\mathcal{T})$ la cual es el cuadrado de una rotación en $\mathcal{T}$ y cuyo espacio fijo es $< y >$. Colocando $\overline{\sigma} = \sigma \perp 1_{\mathcal{W}}$ y como $\sigma = \rho^2$, para algún $\rho \; \varepsilon \; O_3^+(\mathcal{T})$, entonces

$$\overline{\sigma} = (\rho \perp 1_{\mathcal{W}})(\rho \perp 1_{\mathcal{W}})$$

así $\overline{\sigma}$ es el cuadrado de una rotación y por lo tanto pertenece a Ω_n.

Sabemos que $\overline{\sigma}(x) = \sigma(x)$, además

$$\sigma(x) \; \varepsilon \; \mathcal{T} \text{ si } \sigma(x) \; \varepsilon \; \mathcal{U}$$

por lo tanto $\sigma(x) \; \varepsilon \; < x >$, entonces σ deja fijo a $\mathcal{H}$ y al vector y, pero el espacio fijo de σ es $< y >$, luego $\sigma(\mathcal{U}) \neq \mathcal{U}$.

■

Proposición 69 *Sea $(\mathcal{V}, Q)$ un espacio cuadrático regular, el cual no es un plano hiperbólico sobre un cuerpo de 3 elementos y $\alpha \; \varepsilon \; Q(\mathcal{V})$.*

i) Si $\alpha \neq 0$, entonces existe una base $\{x_1, x_2, \ldots, x_n\}$ de $\mathcal{V}$, tal que $Q(x_i) = \alpha$.

ii) Si $\mathcal{V}$ es isótropo, entonces existe una base $\{x_1, x_2, \ldots, x_n\}$ de $\mathcal{V}$, tal que $Q(x_i) = 0$.

Demostración.

$n=1$ Si $\mathcal{V} =< x >$ regular, luego $Q(x) = \alpha \neq 0$.

$n=2$ Si $\mathcal{V}$ es un plano hiperbólico, el resultado es evidente.

Si $\mathcal{V}$ es anisótropo, entonces sea $x \; \varepsilon \; \mathcal{V}$ tal que $Q(x) = \alpha$. Considerando τ la reflexión con respecto a la recta, la cual no es igual a $< x >$ ni tampoco ortogonal a $< x >$, de esta manera $\{x, \tau(x)\}$ es una base con las propiedades deseadas.

$n \geq 3$ Sea $x \; \varepsilon \; \mathcal{V} - \{0\}$, tal que $Q(x) = \alpha$.

Sea $\mathcal{U}$ un subespacio de $\mathcal{V}$, tal que

$$\mathcal{U} =< \{\rho(x) \mid \rho \; \varepsilon \; \Omega_n\} >$$

Entonces $\sigma(\mathcal{U}) = \mathcal{U}$, $\forall \; \sigma \; \varepsilon \; \Omega_n$, así $\mathcal{U} = \mathcal{V}$, por la Proposición anterior. Por lo tanto podemos encontrar $\sigma_1, \sigma_2, \ldots, \sigma_n \; \varepsilon \; \Omega_n$ tal que $\{\sigma_1(x), \sigma_2(x), \ldots, \sigma_n(x)\}$ es una base de $\mathcal{V}$.

$\blacksquare$

Capítulo 4

Representación Natural del Grupo Ortogonal

En este capítulo, realizaremos la representación natural del Grupo ortogonal en espacios cuadráticos $(\mathcal{V}, Q)$, en dimensión 2 y 4, sobre el cuerpo finito $\mathbb{F}_q$.

4.1. Representación Natural de $O_2(\mathcal{V})$

4.1.1. $\mathcal{V}$ un plano isótropo

Por la Proposición 46, consideraremos un plano hiperbólico $\mathcal{H}$ sobre un cuerpo de q elementos, $\mathbb{F}_q$. De esta manera $\mathcal{H} =< e_1, e_2 >$, tal que $Q(e_1) = Q(e_2) = 0$.

Por el Ejemplo 10, tenemos que

$$O_2(\mathcal{H}) = \left\{ \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix}, \begin{pmatrix} 0 & \zeta \\ \zeta^{-1} & 0 \end{pmatrix} \mid \zeta \,\varepsilon\, \mathbb{F}_q^* \right\} = \{\tau_{e_1-\zeta e_2}, \tau_{e_1-e_2} \circ \tau_{e_1-\zeta e_2} \mid \zeta \,\varepsilon\, \mathbb{F}_q^*\}$$

Consideremos una descomposición de $\mathcal{H}$, dada de la siguiente forma:

$$\mathcal{H} = O_{ani} \,\dot{\cup}\, \mathcal{O}_{iso} \,\dot{\cup}\, \{0\}$$

donde

$$O_{ani} = \{z \,\varepsilon\, \mathcal{H} - \{0\} \mid Q(z) \neq 0\} \text{ y } \mathcal{O}_{iso} = \{w \,\varepsilon\, \mathcal{H} - \{0\} \mid Q(w) = 0\}$$

y en nuestro caso:

$$O_{ani} = \{\alpha e_1 + \beta e_2 \mid \alpha, \beta \,\varepsilon\, \mathbb{F}_q^*\}$$

y

$$\mathcal{O}_{iso} = \{\alpha e_j \mid \alpha \,\varepsilon\, \mathbb{F}_q^* \text{ y } j = 1, 2\}$$

Sea la acción por evaluación de $O_2(\mathcal{H})$ en $\mathcal{H}$, dada por:

$$\begin{aligned} \cdot : \quad O_2(\mathcal{H}) \times \mathcal{H} &\to \mathcal{H} \\ (\sigma, x) &\rightsquigarrow \sigma \cdot x = \sigma(x) \end{aligned}$$

Notación. A los elementos de $O_{ani} = \{\alpha e_1 + \beta e_2 \mid \alpha, \beta \,\varepsilon\, \mathbb{F}_q^*\}$, los denotaremos como $(\alpha\ \beta)$.

Lema 4 *O_{ani}, bajo la acción por evaluación de $O_2(\mathcal{H})$, no es transitivo.*

Demostración. Consideremos

$$\mathcal{O}_\lambda = \{(\alpha\ \beta) \,\varepsilon\, \mathcal{O}_{ani} \mid \alpha\beta = \lambda, \text{ con } \lambda \,\varepsilon\, \mathbb{F}_q^*\}$$

1) Sean $z \,\varepsilon\, \mathcal{O}_{\lambda_1}$ e $y \,\varepsilon\, \mathcal{O}_{\lambda_2}$, con $\lambda_1 \neq \lambda_2$.
   Entonces si O_{ani} fuese transitivo, existiría $\sigma \,\varepsilon\, O_2(\mathcal{H})$, tal que $\sigma(z) = y$, entonces

$$\begin{aligned} Q(z) &= Q(\sigma(z)) \\ &= Q(y) \end{aligned}$$

   luego $\lambda_1 = \lambda_2$, lo cual es una contradicción.

2) Ahora probaremos que $\mathcal{O}_\lambda$ es transitivo. Sean $(\alpha\ \beta), (\gamma\ \delta) \,\varepsilon\, \mathcal{O}_\lambda$, luego

$$\alpha\beta = \lambda \wedge \gamma\delta = \lambda \Rightarrow \beta = \alpha^{-1}\lambda \wedge \delta = \gamma^{-1}\lambda$$

   entonces

$$\begin{pmatrix} \gamma\alpha^{-1} & 0 \\ 0 & \alpha\gamma^{-1} \end{pmatrix} \begin{pmatrix} \alpha \\ \alpha^{-1}\lambda \end{pmatrix} = \begin{pmatrix} \gamma \\ \gamma^{-1}\lambda \end{pmatrix}$$

   Además, podemos describir a $\mathcal{O}_\lambda$ de la siguiente forma:

$$\mathcal{O}_\lambda = \{(\alpha\ \lambda\alpha^{-1}) \mid \alpha \,\varepsilon\, \mathbb{F}_q^*\}$$

$\blacksquare$

De esta manera consideraremos $O_{ani} = \dot{\bigcup}_{\lambda \,\varepsilon\, \mathbb{F}_q^*} \mathcal{O}_\lambda$, donde $\mathcal{O}_\lambda$ es transitivo.

Descomposición de $L^2(\mathcal{O}_\lambda)$

Para poder conocer las subrepresentaciones de $L^2(\mathcal{O}_\lambda)$, primero debemos saber cuántas hay. La siguiente proposición nos entrega un resultado de gran utilidad, para conocer este número.

Proposición 70 *Sea $\lambda \,\varepsilon\, \mathbb{F}_q^*$, entonces*

$$\mid \mathcal{O}_\lambda \times \mathcal{O}_\lambda / O_2(\mathcal{H}) \mid = \frac{q+1}{2}$$

Demostración. Sean $(\alpha\ \beta), (\gamma\ \delta) \,\varepsilon\, \mathcal{O}_\lambda$, entonces

$$\mathcal{O}_{((\alpha\ \beta),(\gamma\ \delta))} = \{(\sigma \cdot (\alpha\ \beta), \sigma \cdot (\gamma\ \delta)) \mid \sigma \,\varepsilon\, O_2(\mathcal{H})\}$$

1) Como $\mathcal{O}_\lambda$ es transitivo, existe $\sigma \varepsilon O_2(\mathcal{H})$ tal que, $\sigma \cdot (\alpha\ \beta) = (1\ \lambda)$, en efecto,

$$\begin{pmatrix} 0 & \beta^{-}1 \\ \beta & 0 \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} 1 \\ \lambda \end{pmatrix}$$

además,

$$\begin{pmatrix} 0 & \beta^{-1} \\ \beta & 0 \end{pmatrix}\begin{pmatrix} \gamma \\ \delta \end{pmatrix} = \begin{pmatrix} \beta^{-1}\delta \\ \beta\gamma \end{pmatrix} = \begin{pmatrix} \beta^{-1}\delta \\ \lambda\beta\delta^{-1} \end{pmatrix} = \begin{pmatrix} \beta^{-1}\delta \\ \lambda(\beta^{-1}\delta)^{-1} \end{pmatrix}$$

ya que $\gamma\delta = \lambda$. Sea $\epsilon = \beta^{-1}\delta$, de esta manera

$$\mathcal{O}_{((\alpha\ \beta),(\gamma\ \delta))} = \mathcal{O}_{((1\ \lambda),(\epsilon\ \lambda\epsilon^{-1}))}$$

2) Ahora si miramos el estabilizador de $(1\ \lambda)$, es decir

$$\sigma \cdot (1\ \lambda) = (1\ \lambda)$$

obtenemos que

$$\sigma = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{o} \quad \sigma = \begin{pmatrix} 0 & \lambda^{-1} \\ \lambda & 0 \end{pmatrix}$$

así tenemos que

$$\sigma \cdot (1\ \lambda) = (1\ \lambda) \quad \wedge \quad \sigma \cdot (\alpha\ \lambda\alpha^{-1}) = (\alpha^{-1}\ \lambda\alpha)$$

Por lo tanto

$$\mathcal{O}_{(1\ \lambda)(\alpha\ \lambda\alpha^{-1})} = \mathcal{O}_{(1\ \lambda)(\alpha^{-1}\ \lambda\alpha)}$$

donde $(\alpha\ \lambda\alpha^{-1}) = (\alpha^{-1}\ \lambda\alpha)$ si y sólo si $\alpha^2 = 1$.

De esta manera, un sistema de representantes para esta órbita, esta dado por

$$I = \{\{\alpha, \alpha^{-1}\} \mid \alpha \,\varepsilon\, \mathbb{F}_q^*\}$$

denotaremos por $\overline{\alpha}$ a los elementos de I, es decir

$$I = \{\overline{\alpha} = \{\alpha, \alpha^{-1}\} \mid \alpha \,\varepsilon\, \mathbb{F}_q^*\}$$

Notemos que $\overline{\alpha} = \overline{\alpha^{-1}}$, de esta manera obtenemos que $\#I = \dfrac{q+1}{2}$. Así

$$\mathcal{O}_\lambda \times \mathcal{O}_\lambda / O_2(\mathcal{H}) = \{\mathcal{O}_{((1\ \lambda),(\alpha\ \lambda\alpha^{-1}))} \mid \overline{\alpha} \,\varepsilon\, I\}$$

y por lo tanto

$$\mid \mathcal{O}_\lambda \times \mathcal{O}_\lambda / O_2(\mathcal{H}) \mid = \frac{q+1}{2}$$

■

De esta manera la $\dim(End(L^2(\mathcal{O}_\lambda))) = \dfrac{q+1}{2}$, lo cual nos dice, que si

$$L^2(\mathcal{O}_\lambda) = \bigoplus_{i=1}^{t} m_i \mathcal{V}_i$$

donde $\mathcal{V}_i$ son subrepresentaciones irreducibles de $L^2(\mathcal{O}_\lambda)$ y m_i su multiplicidad respectiva, entonces

$$\sum_{i=1}^{t} m_i^2 = \frac{q+1}{2}$$

Tabla de Caracteres

Sea $(L^2(\mathcal{O}_\lambda), \rho)$ la representación natural de $O_2(\mathcal{H})$, es decir,

$$\begin{array}{rlll} \rho: & O_2(\mathcal{H}) & \to Aut(L^2(\mathcal{O}_\lambda)) & \\ & \sigma & \rightsquigarrow \quad \rho_\sigma : L^2(\mathcal{O}_\lambda) \to L^2(\mathcal{O}_\lambda) & \\ & & \qquad\qquad \delta_{(\alpha\ \lambda\alpha^{-1})} \ \rightsquigarrow \delta_{\sigma(\alpha\ \lambda\alpha^{-1})} & \end{array}$$

entonces el caracter de ρ esta dado por:

$$\begin{array}{rll} \chi_\rho : & O_2(\mathcal{H}) & \to \mathbb{C} \\ & \sigma & \rightsquigarrow Tr([\rho_\sigma]_{\mathcal{B}}) = \#(Fix_\sigma(\mathcal{O}_\lambda)) \end{array}$$

donde $\mathcal{B}$ es una base de $L^2(\mathcal{O}_\lambda)$ y

$$Fix_\sigma(\mathcal{O}_\lambda) = \{(\alpha\ \lambda\alpha^{-1}) \mid \sigma(\alpha\ \lambda\alpha^{-1}) = (\alpha\ \lambda\alpha^{-1})\}$$

De esta forma, calcularemos el caracter en cada elemento del grupo:

a) $\chi_\rho(1_{O_2(\mathcal{H})}) = \dim(L^2(\mathcal{O}_\lambda)) = q - 1$

b) Sea $\beta \,\varepsilon\, \mathbb{F}_q^* - \{1\}$, luego

$$\begin{aligned} \chi_\rho \begin{pmatrix} \beta & 0 \\ 0 & \beta^{-1} \end{pmatrix} &= \#\left\{(x\ y) \,\varepsilon\, \mathcal{O}_\lambda \mid \begin{pmatrix} \beta & 0 \\ 0 & \beta^{-1} \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}\right\} \\ &= \#\left\{(x\ y) \,\varepsilon\, \mathcal{O}_\lambda \mid \begin{pmatrix} \beta x \\ \beta^{-1} y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}\right\} \\ &= \#\{(x\ y) \,\varepsilon\, \mathcal{O}_\lambda \mid \beta x = x\} \\ &= 0 \end{aligned}$$

ya que $\beta x = x$ implica que $\beta = 1$ y esto es una contradicción.

c) Sea $\beta \,\varepsilon\, \mathbb{F}_q^*$, entonces

$$\begin{aligned}
\chi_\rho \begin{pmatrix} 0 & \beta \\ \beta^{-1} & 0 \end{pmatrix} &= \#\left\{(x\ y)\,\varepsilon\,\mathcal{O}_\lambda \mid \begin{pmatrix} 0 & \beta \\ \beta^{-1} & 0 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}\right\} \\
&= \#\left\{(x\ y)\,\varepsilon\,\mathcal{O}_\lambda \mid \begin{pmatrix} \beta y \\ \beta^{-1}x \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}\right\} \\
&= \#\left\{(x\ y)\,\varepsilon\,\mathcal{O}_\lambda \mid \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \beta y \\ y \end{pmatrix}\right\}
\end{aligned}$$

como $(x\ y)\,\varepsilon\,\mathcal{O}_\lambda$, entonces

$$\begin{aligned}
\beta y * y &= \lambda \\
y^2 &= \lambda\beta^{-1}
\end{aligned}$$

lo cual tiene solución si y sólo si $\lambda\beta^{-1}$ es un cuadrado, es decir, que exista $\alpha\,\varepsilon\,\mathbb{F}_q$, tal que $\alpha^2 = \lambda\beta^{-1}$, por lo tanto

$$\chi_\rho \begin{pmatrix} 0 & \beta \\ \beta^{-1} & 0 \end{pmatrix} = \begin{cases} 2 & \lambda\beta^{-1} \text{ es un cuadrado} \\ 0 & \lambda\beta^{-1} \text{ no es un cuadrado} \end{cases}$$

Notación. Definimos el conjunto de los cuadrados como:

$$\square = \{\alpha^2 \mid \alpha\,\varepsilon\,\mathbb{F}_q\}$$

De esta manera, la tabla de caracteres queda como

	$1_{O_2(\mathcal{H})}$	$\begin{pmatrix} \beta & 0 \\ 0 & \beta^{-1} \end{pmatrix}$	$\begin{pmatrix} 0 & \beta \\ \beta^{-1} & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & \beta \\ \beta^{-1} & 0 \end{pmatrix}$
		$\beta\,\varepsilon\,\mathbb{F}_q^* - \{1\}$	$\beta\,\varepsilon\,\mathbb{F}_q^*$ $\lambda\beta^{-1}\,\varepsilon\,\square$	$\beta\,\varepsilon\,\mathbb{F}_q^*$ $\lambda\beta^{-1} \not\varepsilon\ \square$
χ_ρ	$q-1$	0	2	0

Claramente tenemos

$$\begin{aligned}
<\chi_\rho, \chi_\rho> &= \frac{1}{|O_2(\mathcal{H})|}\left((q-1)^2 + 4\left(\frac{q-1}{2}\right)\right) \\
&= \frac{1}{2(q-1)}\left((q-1)(q+1)\right) \\
&= \frac{q+1}{2}
\end{aligned}$$

Observación. Esto muestra que las subrepresentaciones de $L^2(\mathcal{O}_\lambda)$ y $L^2(\mathcal{O}_\mu)$ son isomorfas, si y sólo si $\lambda\mu$ es un cuadrado con $\lambda, \mu\,\varepsilon\,\mathbb{F}_q^*$, ya que tienen la misma tabla de caracteres.

Además si $\lambda\mu$ no es un cuadrado entonces

$$<\chi_{\rho_\lambda}, \chi_{\rho_\mu}> = \frac{q-1}{2}$$

Construcción de los Núcleos

Consideremos $\mathcal{O}_\lambda \times \mathcal{O}_\lambda = \dot{\bigcup}_{\overline{\alpha}\,\varepsilon\, I} \mathcal{U}_\alpha$, donde $\mathcal{U}_\alpha = \mathcal{O}_{(1\ \lambda)(\alpha\ \lambda\alpha^{-1})}$ e $I = \{\overline{\alpha} = \{\alpha, \alpha^{-1}\} \mid \alpha\ \varepsilon\ \mathbb{F}_q^*\}\}$. Definamos la función característica:

$$\begin{array}{rll} K_\alpha : & \mathcal{O}_\lambda \times \mathcal{O}_\lambda & \to \mathbb{C} \\ & (z,w) & \rightsquigarrow \left\{ \begin{array}{ll} 1 & (z,w)\ \varepsilon\ \mathcal{U}_\alpha \\ 0 & (z,w)\ \notin\ \mathcal{U}_\alpha \end{array} \right. \end{array}$$

el hecho que $(z,w) = ((z_1\ z_2),(w_1\ w_2))\ \varepsilon\ \mathcal{U}_\alpha$, implica que existe $\sigma\ \varepsilon\ O_2(\mathcal{H})$ tal que:

$$\begin{array}{r} \sigma\cdot(1\ \lambda) = (z_1\ z_2) \\ \sigma\cdot(\alpha\ \lambda\alpha^{-1}) = (w_1\ w_2) \end{array}$$

si consideramos $\sigma = \begin{pmatrix} 0 & \zeta \\ \zeta^{-1} & 0 \end{pmatrix}$, obtenemos que $w_1 = z_1\alpha$ o $w_1 = z_1\alpha^{-1}$. De esta manera

$$\begin{array}{rll} K_\alpha : & \mathcal{O}_\lambda \times \mathcal{O}_\lambda & \to \mathbb{C} \\ & ((z_1\ z_2),(w_1\ w_2)) & \rightsquigarrow \left\{ \begin{array}{ll} 1 & w_1 = z_1\alpha \text{ o } w_1 = z_1\alpha^{-1} \\ 0 & \textit{en otro caso} \end{array} \right. \end{array}$$

así definimos el siguiente operador de entrelazamiento:

$$\begin{array}{rll} \phi_\alpha : & L^2(\mathcal{O}_\lambda) & \to L^2(\mathcal{O}_\lambda) \\ & \delta_{(z_1\ z_2)} & \rightsquigarrow \phi_\alpha(\delta_{(z_1\ z_2)}) = \displaystyle\sum_{(w_1\ w_2)\ \varepsilon\ \mathcal{O}_\lambda} K_\alpha((w_1\ w_2),(z_1\ z_2))\delta_{(w_1\ w_2)} \\ & & = \delta_{(z_1\alpha\ z_2\alpha^{-1})} + \delta_{(z_1\alpha^{-1}\ z_2\alpha)} \end{array}$$

como $z_1 z_2 = \lambda,$ entonces

$$= \delta_{(z_1\alpha\ \lambda(z_1\alpha)^{-1})} + \delta_{(z_1\alpha^{-1}\ \lambda(z_1\alpha^{-1})^{-1})}$$

Por Proposición 15, tenemos que los espacios propios de ϕ_α, son subrepresentaciones irreducibles de $L^2(O_{ani})$.

Otro resultado importante, es el hecho que $\{K_\alpha \mid \alpha\ \varepsilon\ I\}$ sea conmutativo, lo cual en nuestro caso sucede. Esto sucede ya que las órbitas son simétricas, es decir,

$$K_\alpha(x,y) = K_\alpha(y,x)$$

y de esta forma

$$\begin{array}{rcl} K_\alpha * K_\beta(x,y) & = & \displaystyle\sum_{z\ \varepsilon\ \mathcal{O}_\lambda} K_\alpha(x,z)K_\beta(z,y) \\ & = & K_\alpha(z,x)K_\beta(y,z) \\ & = & K_\beta(y,z)K_\alpha(z,x) \\ & = & K_\beta * K_\alpha(y,x) \\ & = & K_\beta * K_\alpha(x,y) \end{array}$$

Por lo tanto, si

$$L^2(\mathcal{O}_\lambda) = \bigoplus_{i=1}^{t} m_i \mathcal{V}_i$$

entonces

$$m_i = 1 \wedge t = \frac{q+1}{2}$$

De esta manera, podemos enunciar la siguiente proposición:

Proposición 71 *Sea $\chi : \mathbb{F}_q^* \to \mathbb{C}^*$, un homomorfismo. Se define*

$$f_\chi = \sum_{\alpha\,\varepsilon\,\mathbb{F}_q^*} \chi(\alpha)\delta_{(\alpha\ \lambda\alpha^{-1})}$$

entonces

$$\mathcal{U}_\chi =< f_\chi, f_{\overline{\chi}} >$$

es una subrepresentación irreducible de $L^2(\mathcal{O}_\lambda)$

Demostración. Sólo nos queda demostrar que $\mathcal{U}_\chi$ es estable, para todo $\sigma\,\varepsilon\,O_2(\mathcal{H})$.

Sea $f_\chi\,\varepsilon\,\mathcal{U}_\chi$, entonces

$$\begin{aligned} \rho_\sigma(f_\chi) &= \rho_\sigma\left(\sum_{\alpha\,\varepsilon\,\mathbb{F}_q^*} \chi(\alpha)\delta_{(\alpha\ \lambda\alpha^{-1})}\right) \\ &= \sum_{\alpha\,\varepsilon\,\mathbb{F}_q^*} \chi(\alpha)\rho_\sigma\left(\delta_{(\alpha\ \lambda\alpha^{-1})}\right) \\ &= \sum_{\alpha\,\varepsilon\,\mathbb{F}_q^*} \chi(\alpha)\delta_{(\sigma\cdot(\alpha\ \lambda\alpha^{-1}))} \end{aligned}$$

a) Si $\sigma = \begin{pmatrix} \gamma & 0 \\ 0 & \gamma^{-1} \end{pmatrix}$, con $\gamma\,\varepsilon\,\mathbb{F}_q^*$, entonces

$$\begin{pmatrix} \gamma & 0 \\ 0 & \gamma^{-1} \end{pmatrix}\begin{pmatrix} \alpha \\ \lambda\alpha^{-1} \end{pmatrix} = \begin{pmatrix} \alpha\gamma \\ \lambda(\alpha\gamma)^{-1} \end{pmatrix} = \begin{pmatrix} \beta \\ \lambda\beta^{-1} \end{pmatrix} \text{ donde } \beta = \alpha\gamma$$

de esta manera

$$\begin{aligned} \rho_\sigma(f_\chi) &= \sum_{\alpha\,\varepsilon\,\mathbb{F}_q^*} \chi(\alpha)\delta_{(\sigma\cdot(\alpha\ \lambda\alpha^{-1}))} \\ &= \sum_{\beta\,\varepsilon\,\mathbb{F}_q^*} \chi(\beta\gamma^{-1})\delta_{(\beta\ \lambda\beta^{-1}))} \\ &= \chi(\gamma^{-1}) \sum_{\beta\,\varepsilon\,\mathbb{F}_q^*} \chi(\beta)\delta_{(\beta\ \lambda\beta^{-1}))} \\ &= \chi(\gamma^{-1}) f_\chi \end{aligned}$$

b) Si $\sigma = \begin{pmatrix} 0 & \gamma \\ \gamma^{-1} & 0 \end{pmatrix}$, con $\gamma \,\varepsilon\, \mathbb{F}_q^*$, entonces

$$\begin{pmatrix} 0 & \gamma \\ \gamma^{-1} & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \lambda\alpha^{-1} \end{pmatrix} = \begin{pmatrix} \lambda\gamma\alpha^{-1} \\ \alpha\gamma^{-1} \end{pmatrix} = \begin{pmatrix} \beta \\ \lambda\beta^{-1} \end{pmatrix}; \text{ donde } \beta = \lambda\gamma\alpha^{-1}$$

así tenemos que

$$\begin{aligned} \rho_\sigma(f_\chi) &= \sum_{\alpha \,\varepsilon\, \mathbb{F}_q^*} \chi(\alpha)\delta_{(\sigma\cdot(\alpha\ \lambda\alpha^{-1}))} \\ &= \sum_{\beta \,\varepsilon\, \mathbb{F}_q^*} \chi(\lambda\gamma\beta^{-1})\delta_{(\beta\ \lambda\beta^{-1}))} \\ &= \chi(\lambda\gamma) \sum_{\beta \,\varepsilon\, \mathbb{F}_q^*} \chi(\beta^{-1})\delta_{(\beta\ \lambda\beta^{-1}))} \\ &= \chi(\lambda\gamma) f_{\overline{\chi}} \end{aligned}$$

Entonces, para $f = \theta f_\chi + \eta f_{\overline{\chi}}$, tenemos que:

a) Si $\sigma = \begin{pmatrix} \gamma & 0 \\ 0 & \gamma^{-1} \end{pmatrix}$.

$$\begin{aligned} \rho_\sigma(f) &= \theta' f_\chi + \eta' f_{\overline{\chi}} \\ &\varepsilon\ \mathcal{U}_\chi \end{aligned}$$

b) Si $\sigma = \begin{pmatrix} 0 & \gamma \\ \gamma^{-1} & 0 \end{pmatrix}$

$$\begin{aligned} \rho_\sigma(f) &= \theta' f_{\overline{\chi}} + \eta' f_\chi \\ &\varepsilon\ \mathcal{U}_\chi \end{aligned}$$

De esta manera

$$\rho_\sigma(f) \,\varepsilon\, \mathcal{U}_\chi \quad \forall\, \sigma \,\varepsilon\, O_2(\mathcal{H}) \text{ y } \forall\, f \,\varepsilon\, \mathcal{U}_\chi$$

Por lo tanto $\mathcal{U}_\chi$ es una subrepresentación de $L^2(\mathcal{O}_\lambda)$. ■

Observemos que la dimensión de $\mathcal{U}_\chi$, se desglosa de la siguiente forma:

1) Si $\chi = 1$, al cual denotaremos como $\mathbb{1}$, entonces la $\dim(\mathcal{U}_{\mathbb{1}}) = 1$.

2) Definimos

$$\begin{aligned} sgn:\ \mathbb{F}_q^* &\to \mathbb{C}^* \\ \beta &\rightsquigarrow sgn(\beta) = \begin{cases} 1 & \beta \,\varepsilon\, \square \\ -1 & \beta \notin \square \end{cases} \end{aligned}$$

de esta forma, si $\chi = sgn$, entonces la $\dim(\mathcal{U}_{sgn}) = 1$.

3) $\chi^2 \neq 1$, entonces $\dim(\mathcal{U}_\chi) = 2$.

Proposición 72 *Sea* $\lambda \,\varepsilon\, \mathbb{F}_q^*$

i)

$$L^2(O_{ani}) = \bigoplus_{\lambda \,\varepsilon\, \mathbb{F}_q^*} L^2(\mathcal{O}_\lambda)$$

ii)

$$L^2(\mathcal{O}_\lambda) = \mathcal{U}_{\mathbb{1}} \oplus \mathcal{U}_{sgn_\lambda} \oplus \left(\bigoplus_{\substack{\mu \,\varepsilon\, \widehat{\mathbb{F}_q^*} \\ \mu \neq \overline{\mu}}} \mathcal{U}_\mu \right)$$

donde

	$\begin{pmatrix} \beta & 0 \\ 0 & \beta^{-1} \end{pmatrix}$	$\begin{pmatrix} 0 & \beta \\ \beta^{-1} & 0 \end{pmatrix}$
$\mathbb{1}$	1	1
sgn_λ	$sgn(\beta)$	$sgn(\beta\lambda)$
μ	$\mu(\beta) + \mu(\beta^{-1})$	0

Descomposición de $L^2(\mathcal{O}_{iso})$

Para esto, recordemos que

$$\mathcal{O}_{iso} = \{\alpha e_i \mid \alpha \,\varepsilon\, \mathbb{F}_q^* \text{ y } i = 1, 2\}$$

y la acción por evaluación

$$\begin{array}{rll} \cdot : & O_2(\mathcal{H}) \times \mathcal{O}_{iso} & \to \mathcal{O}_{iso} \\ & (\sigma, \alpha e_i) & \rightsquigarrow \sigma(\alpha e_i) \end{array}$$

naturalmente tenemos la acción

$$\begin{array}{rll} * : & O_2(\mathcal{H}) \times (\mathcal{O}_{iso} \times \mathcal{O}_{iso}) & \to (\mathcal{O}_{iso} \times \mathcal{O}_{iso}) \\ & (\sigma, (\alpha e_i, \beta e_j)) & \rightsquigarrow (\sigma(\alpha e_i), \sigma(\beta e_j)) \end{array}$$

La cantidad de órbitas la tenemos en la siguiente proposición.

Proposición 73

$$\mid \mathcal{O}_{iso} \times \mathcal{O}_{iso} / O_2(\mathcal{H}) \mid = 2(q-1)$$

Demostración. Sean $\alpha e_i, \beta e_j \,\varepsilon\, \mathcal{O}_{iso}$, entonces

$$\mathcal{O}_{(\alpha e_i, \beta e_j)} = \{(\sigma(\alpha e_i), \sigma(\beta e_j)) \mid \sigma \,\varepsilon\, O_2(\mathcal{H})\}$$

Como $\mathcal{O}_{iso}$ es transitivo, existe $\sigma \,\varepsilon\, O_2(\mathcal{H})$, tal que $\sigma(\alpha e_i) = e_1$.

a) Si $i=j$, entonces
$$\mathcal{O}_{(\alpha e_i,\beta e_j)} = \mathcal{O}_{(e_1,\lambda e_1)} \qquad \text{para algún } \lambda \ \varepsilon\ \mathbb{F}_q^*$$

b) Si $i\neq j$, entonces
$$\mathcal{O}_{(\alpha e_i,\beta e_j)} = \mathcal{O}_{(e_1,\lambda e_2)} \qquad \text{para algún } \lambda \ \varepsilon\ \mathbb{F}_q^*$$

Por lo tanto

$$\mathcal{O}_{iso}\times\mathcal{O}_{iso}/O_2(\mathcal{H}) \;=\; \{\mathcal{O}_{(e_1,\lambda e_1)},\mathcal{O}_{(e_1,\lambda e_2)} \mid \lambda\ \varepsilon\ \mathbb{F}_q^*\}$$

donde

$$\begin{aligned}
\mathcal{O}_{(e_1,\lambda e_1)} &= \{(\alpha e_j,\lambda\alpha e_j) \mid \alpha\ \varepsilon\ \mathbb{F}_q^*\}\\
\mathcal{O}_{(e_1,\lambda e_2)} &= \{(\alpha e_i,\lambda\alpha^{-1} e_j) \mid \alpha\ \varepsilon\ \mathbb{F}_q^*,\ i\neq j\}
\end{aligned}$$

así
$$\mid \mathcal{O}_{iso}\times\mathcal{O}_{iso}/O_2(\mathcal{H}) \mid = 2(q-1)$$

■

Construcción de los Núcleos

Para $\mathcal{O}_{(e_1,\lambda e_1)}$ definimos el núcleo por:

$$\begin{aligned}
K_{(e_1,\lambda e_1)}: \quad \mathcal{O}_{iso}\times\mathcal{O}_{iso} &\to \mathbb{C}\\
(\alpha e_i,\beta e_j) &\rightsquigarrow K_{(e_1,\lambda e_1)}(\alpha e_i,\beta e_j) = \begin{cases} 1 & (\alpha e_i,\beta e_j)\ \varepsilon\ \mathcal{O}_{(e_1,\lambda e_1)}\\ 0 & (\alpha e_i,\beta e_j)\ \not\varepsilon\ \mathcal{O}_{(e_1,\lambda e_1)}\end{cases}
\end{aligned}$$

es decir,

$$\begin{aligned}
K_{(e_1,\lambda e_1)}: \quad \mathcal{O}_{iso}\times\mathcal{O}_{iso} &\to \mathbb{C}\\
(\alpha e_i,\beta e_j) &\rightsquigarrow K_{(e_1,\lambda e_1)}(\alpha e_i,\beta e_j) = \begin{cases} 1 & \beta=\lambda\alpha \text{ e } i=j\\ 0 & \text{en otro caso}\end{cases}
\end{aligned}$$

Luego

$$\begin{aligned}
\phi_{(e_1,\lambda e_1)}: \quad L^2(\mathcal{O}_{iso}) &\to L^2(\mathcal{O}_{iso})\\
\delta_{\alpha e_i} &\rightsquigarrow \phi_{(e_1,\lambda e_1)}(\delta_{\alpha e_i}) = \sum_{\beta e_j\ \varepsilon\ \mathcal{O}_{iso}} K_{(e_1,\lambda e_1)}(\beta e_j,\alpha e_i)\delta_{\beta e_j}\\
&\qquad = \delta_{\lambda^{-1}\alpha e_i}
\end{aligned}$$

es un operador de entrelazamiento.

Si realizamos un procedimiento parecido para las órbitas $\mathcal{O}_{(e_1,\lambda e_2)}$, obtenemos el siguiente operador de entrelazamiento:

$$\begin{array}{rll} \phi_{(e_1,\lambda e_2)}: & L^2(\mathcal{O}_{iso}) & \rightarrow L^2(\mathcal{O}_{iso}) \\ & \delta_{\alpha e_i} & \rightsquigarrow \phi_{(e_1,\lambda e_2)}(\delta_{\alpha e_i}) = \displaystyle\sum_{\beta e_j \,\varepsilon\, \mathcal{O}_{iso}} K_{(e_1,\lambda e_2)}(\beta e_j, \alpha e_i)\delta_{\beta e_j} \\ & & = \delta_{\lambda\alpha^{-1}e_j} \end{array}$$

Proposición 74 *Sea $\chi : \mathbb{F}_q^* \rightarrow \mathbb{C}^*$, un homomorfismo, entonces*

$$\mathcal{U}_\chi = < f_\chi, g_\chi >$$

es una subrepresentación irreducible de $L^2(\mathcal{O}_{iso})$, donde

$$f_\chi = \sum_{\alpha \,\varepsilon\, \mathbb{F}_q^*} \chi(\alpha)\delta_{\alpha e_1} \qquad g_\chi = \sum_{\alpha \,\varepsilon\, \mathbb{F}_q^*} \chi(\alpha)\delta_{\alpha e_2}$$

Demostración. Nos queda demostrar que $\mathcal{U}_\chi$ es estable. Para esto sea $f = \theta f_\chi + \theta' g_\chi \,\varepsilon\, \mathcal{U}_\chi$, con $\theta, \theta' \,\varepsilon\, \mathbb{C}$. Entonces

$$\begin{aligned} \rho_\sigma(f) &= \rho_\sigma(\theta f_\chi + \theta' g_\chi) \\ &= \theta\left(\sum_{\alpha \,\varepsilon\, \mathbb{F}_q^*} \chi(\alpha)\rho_\sigma\left(\delta_{\alpha e_1}\right)\right) + \theta'\left(\sum_{\alpha \,\varepsilon\, \mathbb{F}_q^*} \chi(\alpha)\rho_\sigma\left(\delta_{\alpha e_2}\right)\right) \\ &= \theta\left(\sum_{\alpha \,\varepsilon\, \mathbb{F}_q^*} \chi(\alpha)\delta_{\sigma(\alpha e_1)}\right) + \theta'\left(\sum_{\alpha \,\varepsilon\, \mathbb{F}_q^*} \chi(\alpha)\delta_{\sigma(\alpha e_2)}\right) \end{aligned}$$

a) Si $\sigma = \begin{pmatrix} 0 & \beta \\ \beta^{-1} & 0 \end{pmatrix}$, entonces

$$\sigma(\alpha e_1) = \alpha\beta e_2 \quad \text{y} \quad \sigma(\alpha e_2) = \alpha\beta^{-1}e_1$$

entonces

$$\begin{aligned} \rho_\sigma(f) &= \theta\left(\sum_{\alpha \,\varepsilon\, \mathbb{F}_q^*} \chi(\alpha)\delta_{(\alpha\beta e_2)}\right) + \theta'\left(\sum_{\alpha \,\varepsilon\, \mathbb{F}_q^*} \chi(\alpha)\delta_{(\alpha\beta^{-1}e_1)}\right) \\ &= \theta\left(\sum_{\gamma \,\varepsilon\, \mathbb{F}_q^*} \chi(\gamma\beta^{-1})\delta_{(\gamma e_2)}\right) + \theta'\left(\sum_{\gamma \,\varepsilon\, \mathbb{F}_q^*} \chi(\gamma\beta)\delta_{(\gamma e_1)}\right) \\ &= (\theta'\chi(\beta))\left(\sum_{\gamma \,\varepsilon\, \mathbb{F}_q^*} \chi(\gamma)\delta_{(\gamma e_1)}\right) + (\theta\chi(\beta^{-1}))\left(\sum_{\gamma \,\varepsilon\, \mathbb{F}_q^*} \chi(\gamma)\delta_{(\gamma e_2)}\right) \\ &\varepsilon \quad \mathcal{U}_\chi \end{aligned}$$

b) Si $\sigma = \begin{pmatrix} \beta & 0 \\ 0 & \beta^{-1} \end{pmatrix}$, entonces

$$\sigma(\alpha e_1) = \alpha\beta e_1 \quad \text{y} \quad \sigma(\alpha e_2) = \alpha\beta^{-1} e_2$$

entonces

$$\begin{aligned} \rho_\sigma(f) &= \theta\left(\sum_{\alpha\,\varepsilon\,\mathbb{F}_q^*} \chi(\alpha)\delta_{(\alpha\beta e_1)}\right) + \theta'\left(\sum_{\alpha\,\varepsilon\,\mathbb{F}_q^*} \chi(\alpha)\delta_{(\alpha\beta^{-1} e_2)}\right) \\ &= \theta\left(\sum_{\gamma\,\varepsilon\,\mathbb{F}_q^*} \chi(\gamma\beta^{-1})\delta_{(\gamma e_1)}\right) + \theta'\left(\sum_{\gamma\,\varepsilon\,\mathbb{F}_q^*} \chi(\gamma\beta)\delta_{(\gamma e_2)}\right) \\ &= (\theta\chi(\beta^{-1}))\left(\sum_{\gamma\,\varepsilon\,\mathbb{F}_q^*} \chi(\gamma)\delta_{(\gamma e_1)}\right) + (\theta'\chi(\beta))\left(\sum_{\gamma\,\varepsilon\,\mathbb{F}_q^*} \chi(\gamma)\delta_{(\gamma e_2)}\right) \\ &\varepsilon\ \ \mathcal{U}_\chi \end{aligned}$$

De esta manera

$$\rho_\sigma(f) \subseteq \mathcal{U}_\chi \qquad \forall\,\sigma\,\varepsilon\,O_2(\mathcal{H}),\ \forall f\,\varepsilon\,\mathcal{U}_\chi$$

Por lo tanto $\mathcal{U}_\chi$ es una subrepresentación de $L^2(\mathcal{O}_{iso})$. El hecho que sea irreducible, sale de lo siguiente:

1) Si consideramos $< f_\chi >$ como posible subrepresentación de $L^2(\mathcal{O}_{iso})$, por a), de la prueba anterior, obtenemos que $< f_\chi > \subseteq < g_\chi >$ y viceversa, por lo tanto $< f_\chi >$ o $< g_\chi >$ no son estables.

2) Sea $f\,\varepsilon\,\mathcal{U}_\chi$, tal que $< f >$ es estable. Por lo tanto

$$f = f_\chi + \theta g_\chi$$

con $\theta\,\varepsilon\,\mathbb{C}$. Aplicando a), de la demostración anterior, obtenemos que

$$\begin{aligned} \sigma(f) &= \sigma(f_\chi) + \theta\sigma(g_\chi) \\ &= \chi(\beta) f_\chi + \theta\chi(\beta^{-1}) g_\chi \end{aligned} \tag{4.1}$$

de esta manera $\sigma(f) \notin < f >$, y por lo tanto $< f >$ no es estable, si $\chi \neq \overline{\chi}$.

Por lo tanto $\mathcal{U}_\chi$, es una subrepresentación irreducible de $L^2(\mathcal{O}_{iso})$, para $\chi \neq \overline{\chi}$. ■

Corolario 14 *Por 4.1, tenemos que*

$$< f_\chi + g_\chi > \qquad y \qquad < f_\chi - g_\chi >$$

son estables si $\chi = \overline{\chi}$.

Proposición 75 *La descomposición de $L^2(\mathcal{O}_{iso})$ es:*

$$L^2(\mathcal{O}_{iso}) =< f_{\mathbb{1}} \pm g_{\mathbb{1}} > \oplus < f_{sgn} \pm g_{sgn} > \oplus \left(\bigoplus_{\substack{\chi \,\varepsilon\, \widehat{\mathbb{F}_q^*} \\ \chi \neq \overline{\chi}}} 2\mathcal{U}_\chi \right)$$

Demostración. Solo nos queda ver la multiplicidad de $\mathcal{U}_\chi$.

Si miramos la tabla de caracteres de $\mathcal{U}_\chi$ obtenemos lo siguiente:

	$\tau_{e_1-\beta e_2}$	$\tau_{e_1-e_2} \circ \tau_{e_1-\beta e_2}$
$\mathcal{U}_\chi$	0	$\chi(\beta) + \chi(\beta^{-1})$

Este resultado aparece en la demostración de la Proposición anterior, de donde obtenemos que,

$$[\rho_{\tau_{e_1-\beta e_2}}]_{\mathcal{B}} = \begin{pmatrix} 0 & \chi(\beta) \\ \chi(\beta^{-1}) & 0 \end{pmatrix} \quad \text{y} \quad [\rho_{\tau_{e_1-e_2} \circ \tau_{e_1-\beta e_2}}]_{\mathcal{B}} = \begin{pmatrix} \chi(\beta) & 0 \\ 0 & \chi(\beta^{-1}) \end{pmatrix}$$

donde $\mathcal{B} = \{f_\chi, g_\chi\}$ es una base de $\mathcal{U}_\chi$. De esta manera la tabla de caracteres de $\mathcal{U}_{\overline{\chi}}$, obtenemos

	$\tau_{e_1-\beta e_2}$	$\tau_{e_1-e_2} \circ \tau_{e_1-\beta e_2}$
$\mathcal{U}_{\overline{\chi}}$	0	$\overline{\chi(\beta)} + \overline{\chi(\beta^{-1})} = \chi(\beta) + \chi(\beta^{-1})$

de esta forma

$$\mathcal{U}_\chi \cong \mathcal{U}_{\overline{\chi}}$$

así

$$| \mathcal{O}_{iso} \times \mathcal{O}_{iso}/O_2(\mathcal{H}) |= 2(q-1) = 1^2 + 1^2 + 1^2 + 1^2 + 2^2 \left(\frac{q-3}{2}\right)$$

■

Resumen

1º Describimos $O_2(\mathcal{H})$, con $\mathcal{H} =< e_1, e_2 >$ y $Q(\alpha e_1 + \beta e_2) = \alpha\beta$.

$$O_2(\mathcal{H}) = \left\{ \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix}, \begin{pmatrix} 0 & \zeta \\ \zeta^{-1} & 0 \end{pmatrix} \mid \zeta \,\varepsilon\, \mathbb{F}_q^* \right\} = \{\tau_{e_1-\zeta e_2}, \tau_{e_1-e_2} \circ \tau_{e_1-\zeta e_2} \mid \zeta \,\varepsilon\, \mathbb{F}_q^*\}$$

2º Descomponemos $\mathcal{H}$ en órbitas.

$$\mathcal{H} = O_{ani} \,\dot{\cup}\, \mathcal{O}_{iso} \,\dot{\cup}\, \{0\}$$

$$\mathcal{H} = \dot{\bigcup_{\lambda \,\varepsilon\, \mathbb{F}_q^*}} \mathcal{O}_\lambda \,\dot{\cup} \mathcal{O}_{iso} \dot{\cup}\, \{0\}$$

3º Representación Natural de $L^2(\mathcal{H})$.

$$L^2(\mathcal{H}) = \bigoplus_{\lambda \,\varepsilon\, \mathbb{F}_q^*} L^2(\mathcal{O}_\lambda) \oplus L^2(\mathcal{O}_{iso}) \oplus L^2(\{0\})$$

4º Descomposición en subrepresentaciones irreducibles.

$$L^2(\mathcal{O}_\lambda) = \mathcal{U}_{\mathbb{1}} \oplus \mathcal{U}_{sgn_\lambda} \oplus \left(\bigoplus_{\substack{\mu\,\varepsilon\,\widehat{\mathbb{F}_q^*}\\ \mu\neq\overline{\mu}}} \mathcal{U}_\mu \right) \; ; \; \lambda\,\varepsilon\,\mathbb{F}_q^*$$

$$L^2(\mathcal{O}_{iso}) = < f_{\mathbb{1}} \pm g_{\mathbb{1}} > \oplus < f_{sgn} \pm g_{sgn} > \oplus \left(\bigoplus_{\substack{\chi\,\varepsilon\,\widehat{\mathbb{F}_q^*}\\ \chi\neq\overline{\chi}}} 2\mathcal{U}_\chi \right)$$

4.1.2. $\mathcal{V}$ un plano anisótropo

Sea $\mathbb{F}_{q^2}$ la extensión cuadrática de $\mathbb{F}_q$ y δ un no cuadrado en $\mathbb{F}_q$. Definimos el espacio cuadrático anisótropo $(\mathbb{F}_{q^2}, N)$, dado por:

$$\begin{array}{rll} N: & \mathbb{F}_{q^2} & \to \mathbb{F}_q \\ & a+\epsilon b & \rightsquigarrow a^2-\delta b^2 \end{array}$$

con $\epsilon^2 = \delta$.

Observación. Sabemos, por teoría de cuerpos finitos, que $\mathbb{F}_{q^2}^*$ es cíclico, de esta forma, existe $a\,\varepsilon\,\mathbb{F}_{q^2}^*$, tal que

$$\begin{array}{rcl} a^{q^2-1} & = & 1 \\ (a^{q-1})^{q+1} & = & 1 \end{array}$$

por lo tanto $a^{t(q-1)}$, con $t = 0, 1, 2, \ldots, q$, son las $q+1$ soluciones de $x^{q+1}-1$ sobre $\mathbb{F}_{q^2}$.

Si consideramos la función conjugado, es decir

$$\begin{array}{rll} -: & \mathbb{F}_{q^2} & \to \mathbb{F}_{q^2} \\ & v & \rightsquigarrow \overline{v} \end{array}$$

la cual es un automorfismos de cuerpos, tal que deja fijo a $\mathbb{F}_q$.

De esta manera, si $v\,\varepsilon\,\mathbb{F}_{q^2}$, es solución del polinomio $\alpha x^2 + \beta x + c$ sobre $\mathbb{F}_q$, entonces

$$\begin{array}{rcl} 0 & = & \overline{\alpha v^2 + \beta v + c} \\ & = & \alpha \overline{v}^2 + \beta\overline{v} + c \end{array}$$

obtenemos que $\overline{v}$ es la otra solución de este polinomio.

Además, tenemos que:

$$(v+u)^q = v^q + u^q$$

de esta forma

$$\begin{array}{c} (\alpha v^2 + \beta v + c)^q = 0^q \\ \alpha (v^q)^2 + \beta v^q + c = 0 \end{array}$$

así, v^q es también solución de $\alpha x^2 + \beta x + c$, por lo tanto

$$v^q = \overline{v}$$

Proposición 76

$$O_2(\mathbb{F}_{q^2}) \cong \{\mu \,\varepsilon\, \mathbb{F}_{q^2} \mid N(\mu) = 1\}$$

Además

$$\mid O_2(\mathbb{F}_{q^2}) \mid = q + 1$$

Demostración. Consideremos $A = \{\mu \,\varepsilon\, \mathbb{F}_{q^2} \mid N(\mu) = 1\}$ y definamos

$$\begin{array}{rll} \phi : & A & \to End(\mathbb{F}_{q^2}) \\ & \mu & \rightsquigarrow h_\mu : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2} \\ & & \qquad\qquad v \rightsquigarrow \mu v \end{array}$$

Es claro que ϕ es función

1) Homomorfismo. Sean $\mu, \nu \,\varepsilon\, A$ y $w \,\varepsilon\, \mathbb{F}_{q^2}$, entonces

$$\begin{aligned} h_{\mu\nu}(w) &= \mu\nu w \\ &= h_\mu(\nu w) \\ &= h_\mu(h_\nu(w)) \\ &= h_\mu \circ h_\nu(w) \end{aligned}$$

así $h_{\mu\nu} = h_\mu \circ h_\nu$. Por lo tanto

$$\phi(\mu\nu) = \phi(\mu) \circ \phi(\nu)$$

2) Inyectividad. Sea

$$\begin{aligned} ker(\phi) &= \{\mu \,\varepsilon\, A \mid h_\mu = 1_{\mathbb{F}_{q^2}}\} \\ &= \{\mu \,\varepsilon\, A \mid h_\mu(v) = 1_{\mathbb{F}_{q^2}}(v) \quad \forall\, v \,\varepsilon\, \mathbb{F}_{q^2}\} \\ &= \{\mu \,\varepsilon\, A \mid \mu v = v \quad \forall\, v \,\varepsilon\, \mathbb{F}_{q^2}\} \\ &= \{\mu \,\varepsilon\, A \mid v(\mu - 1) = 0 \quad \forall\, v \,\varepsilon\, \mathbb{F}_{q^2}\} \\ &= \{1\} \end{aligned}$$

así es inyectiva.

Además, para $v \,\varepsilon\, \mathbb{F}_{q^2}$, tenemos que

$$\begin{aligned} N(h_\mu(v)) &= N(\mu v) \\ &= N(\mu)N(v) \\ &= N(v) \end{aligned}$$

entonces h_μ traslada la forma cuadrática, también tenemos que

$$\begin{array}{rcl} ker(h_\mu) & = & \{v \,\varepsilon\, \mathbb{F}_{q^2} \mid h_\mu(v) = 0\} \\ & = & \{v \,\varepsilon\, \mathbb{F}_{q^2} \mid \mu v = 0\} \\ & = & \{0\} \end{array}$$

de esta manera $h_\mu \,\varepsilon\, O_2(\mathbb{F}_{q^2})$.

3) Epiyectividad. Sea $\sigma \,\varepsilon\, O_2(\mathbb{F}_{q^2})$ y consideremos $\mu = \sigma(1) \,\varepsilon\, \mathbb{F}_{q^2}$, demostraremos que

$$h_\mu = \sigma \qquad \forall v \,\varepsilon\, \mathbb{F}_{q^2}$$

Como $\mathbb{F}_{q^2}$ es un espacio vectorial sobre $\mathbb{F}_q$, con base $\mathcal{B} = \{1, \epsilon\}$, entonces solo bastaría demostrar lo anterior en esta base.

Para todo $\alpha \,\varepsilon\, \mathbb{F}_q$, tenemos que

$$h_\mu(\alpha) = \alpha\mu = \alpha\sigma(1) = \sigma(\alpha)$$

Solo queda ver, que sucede en ϵ. Para esto, sea $v \,\varepsilon\, \mathbb{F}_{q^2}$, entonces

$$\begin{array}{rcl} N(\sigma(v)) & = & N(v) \\ N(\sigma(v))N(v)^{-1} & = & 1 \\ N(\sigma(v)v^{-1}) & = & 1 \end{array}$$

de esta manera, $\sigma(v)v^{-1} = \nu$ o $\sigma(v) = \nu v$, con $\nu \,\varepsilon\, A$. Supongamos que $\sigma(\epsilon) = \nu\epsilon$, para algún $\nu \,\varepsilon\, A$, entonces

$$\begin{array}{rcl} \sigma(1+\epsilon) & = & w(1+\epsilon) \\ \mu + \nu\epsilon & = & w + w\epsilon \end{array}$$

como $\{1, \epsilon\}$ es base de $\mathbb{F}_{q^2}$, entonces $\mu = w = \nu$. Así $\sigma(\epsilon) = \sigma(1)\epsilon$.

De esta manera

$$\begin{array}{rcl} h_{\sigma(1)}(\epsilon) & = & \sigma(1)\epsilon \\ & = & \sigma(\epsilon) \end{array}$$

Por lo tanto

$$h_{\sigma(1)} = \sigma$$

De esta manera ϕ es un isomorfismo de grupos.

Si consideramos a N como:

$$\begin{array}{rll} N: & \mathbb{F}_{q^2}^* & \to \mathbb{F}_q^* \\ & a & \rightsquigarrow a^{q+1} \end{array}$$

por la Observación anterior, obtenemos que $\mid ker(N) \mid = q+1$, como $ker(N) = A$, entonces

$$\mid O_2(\mathbb{F}_{q^2}) \mid = q+1$$

■

Corolario 15

$$O_2(\mathbb{F}_{q^2}) \quad \textit{es conmutativo}$$

Demostración. De la demostración anterior, obtuvimos que $ker(N) = O_2(\mathbb{F}_{q^2})$. Como $ker(N) \leq \mathbb{F}^*_{q^2}$. Entonces $O_2(\mathbb{F}_{q^2})$, es conmutativo. ■

Notación. Para los elementos $h_\mu \, \varepsilon \, O_2(\mathbb{F}_{q^2})$, los denotaremos simplemente como μ, entendiendo que

$$\mu v = h_\mu(v)$$

Sea

$$\begin{array}{rll} \cdot : & O_2(\mathbb{F}_{q^2}) \times \mathbb{F}_{q^2} & \to \mathbb{F}_{q^2} \\ & (\mu, v) & \rightsquigarrow \mu v \end{array}$$

la acción natural de $O_2(\mathbb{F}_{q^2})$ en $\mathbb{F}_{q^2}$.

Proposición 77 *$\mathbb{F}_{q^2}$, con la acción natural, tiene q órbitas.*

$$\mathbb{F}_{q^2} = \dot{\bigcup_{\lambda \, \varepsilon \, \mathbb{F}^*_q}} \mathcal{O}_\lambda \,\dot{\cup}\, \{0\}$$

con $\mathcal{O}_\lambda = \{v \, \varepsilon \, \mathbb{F}_{q^2} \mid N(v) = \lambda\}$, *con* $\lambda \, \varepsilon \, \mathbb{F}^*_q$.

Demostración.

i) Sea $u \, \varepsilon \, \mathcal{O}_\lambda$ y $v \, \varepsilon \, \mathcal{O}_{\lambda'}$, tal que $\lambda \neq \lambda'$, entonces si $\mathbb{F}_{q^2}$ fuese transitivo, existiría $\mu \, \varepsilon \, O_2(\mathbb{F}_{q^2})$, tal que $\mu u = v$, entonces

$$\begin{array}{rcl} \lambda & = & N(u) \\ & = & N(\mu u) \\ & = & N(v) \\ & = & \lambda' \end{array}$$

lo cual es una contradicción.

ii) Sean $w, z \, \varepsilon \, \mathcal{O}_\lambda$, es decir $N(w) = N(z) = \lambda$, como $\lambda \, \varepsilon \, \mathbb{F}^*_q$, entonces

$$\begin{array}{rcl} N(w) & = & N(z) \\ N(wz^{-1}) & = & 1 \end{array}$$

luego $wz^{-1} \varepsilon O_2(\mathbb{F}_{q^2})$ entonces $w = \mu z$, para algún $\mu \varepsilon O_2(\mathbb{F}_{q^2})$. De esta manera, sea $v \varepsilon \mathbb{F}_{q^2}$ tal que $N(v) = \lambda$, entonces

$$\mathcal{O}_\lambda = \{\mu v \mid \mu \varepsilon O_2(\mathbb{F}_{q^2})\}$$

Además

$$\mid \mathcal{O}_\lambda \mid = q + 1$$

Así obtenemos

$$\mathbb{F}_{q^2} = \dot{\bigcup_{\lambda \varepsilon \mathbb{F}_q^*}} \mathcal{O}_\lambda \,\dot{\cup}\, \{0\}$$

■

Descomposición de $L^2(\mathcal{O}_\lambda)$

Para esta sección, consideraremos a $\lambda \varepsilon \mathbb{F}_q^*$.

Proposición 78 *Sea $v \varepsilon \mathcal{O}_\lambda$ fijo, entonces*

$$\mathcal{O}_\lambda \times \mathcal{O}_\lambda / O_2(\mathbb{F}_{q^2}) = \{\mathcal{O}_{(v,\mu v)} \mid \mu \varepsilon O_2(\mathbb{F}_{q^2})\}$$

de esta forma

$$\mid \mathcal{O}_\lambda \times \mathcal{O}_\lambda / O_2(\mathbb{F}_{q^2}) \mid = q + 1$$

Demostración. Sean $u, w \varepsilon \mathcal{O}_\lambda$, entonces

$$\mathcal{O}_{(u,w)} = \{(\mu u, \mu w) \mid \mu \varepsilon O_2(\mathbb{F}_{q^2})\}$$

Como $\mathcal{O}_\lambda$ es transitivo, podemos suponer que $\mu u = v$, con $v \varepsilon \mathcal{O}_\lambda$, entonces

$$\mu = vu^{-1}$$

de esta forma

$$\mu w = vu^{-1}w$$

ahora

$$\begin{aligned} N(u^{-1}w) &= (N(u))^{-1}N(w) \\ &= 1 \end{aligned}$$

entonces $u^{-1}w = \nu$, para algún $\nu \varepsilon O_2(\mathbb{F}_{q^2})$ Por lo tanto

$$\mathcal{O}_{(u,w)} = \mathcal{O}_{(v,\nu v)} \qquad \text{para algún } \nu \varepsilon O_2(\mathbb{F}_{q^2})$$

Así

$$\mathcal{O}_\lambda \times \mathcal{O}_\lambda / O_2(\mathbb{F}_{q^2}) = \{\mathcal{O}_{(v,\mu v)} \mid \mu \varepsilon O_2(\mathbb{F}_{q^2})\}$$

de esta manera

$$\mid \mathcal{O}_\lambda \times \mathcal{O}_\lambda / O_2(\mathbb{F}_{q^2}) \mid = q + 1$$

■

Como $O_2(\mathbb{F}_{q^2})$ es conmutativo, tenemos que la dimensión de las representaciones irreducibles es igual a 1.

Proposición 79 *Sean $\chi : O_2(\mathbb{F}_{q^2}) \to \mathbb{C}^*$, un homomorfismo y $v \,\varepsilon\, \mathcal{O}_\lambda$, entonces*

$$\mathcal{U}_\chi =< \sum_{\mu \,\varepsilon\, O_2(\mathbb{F}_{q^2})} \chi(\mu)\delta_{\mu v} >$$

es una subrepresentación de $L^2(\mathcal{O}_\lambda)$.

Demostración. Sólo queda ver la estabilidad de $\mathcal{U}_\chi$. Para esto, sea $f = \sum_{\mu \,\varepsilon\, O_2(\mathbb{F}_{q^2})} \chi(\mu)\delta_{\mu v}$, entonces

$$\begin{aligned}
\rho_\nu(f) &= \rho_\nu\left(\sum_{\mu \,\varepsilon\, O_2(\mathbb{F}_{q^2})} \chi(\mu)\delta_{\mu v}\right) \\
&= \sum_{\mu \,\varepsilon\, O_2(\mathbb{F}_{q^2})} \chi(\mu)\rho_\nu\left(\delta_{\mu v}\right) \\
&= \sum_{\mu \,\varepsilon\, O_2(\mathbb{F}_{q^2})} \chi(\mu)\delta_{\nu\mu v}
\end{aligned}$$

haciendo $\xi = \nu\mu$, tenemos que

$$\begin{aligned}
\rho_\nu(f) &= \sum_{\xi \,\varepsilon\, O_2(\mathbb{F}_{q^2})} \chi(\nu^{-1}\xi)\delta_{\xi v} \\
&= \chi(\nu^{-1}) \sum_{\xi \,\varepsilon\, O_2(\mathbb{F}_{q^2})} \chi(\xi)\delta_{\xi v} \\
&\varepsilon\ \ \mathcal{U}_\chi
\end{aligned}$$

Por lo tanto $\mathcal{U}_\chi$, es una subrepresentación de $L^2(\mathcal{O}_\lambda)$ ■

Proposición 80

$$L^2(\mathcal{O}_\lambda) = \bigoplus_{\mu \,\varepsilon\, \widehat{O_2(\mathbb{F}_{q^2})}} \mathcal{U}_\mu$$

Demostración. De la Proposición anterior obtenemos que $\mathcal{U}_\mu$, con $\mu \,\varepsilon\, \widehat{O_2(\mathbb{F}_{q^2})}$ son todas las subrepresentaciones irreducibles de $L^2(\mathcal{O}_\lambda)$. ■

4.2. Representación Natural de $O_4(\mathcal{V})$

Nos interesa en esta sección determinar todas las representaciones irreducibles, que aparecen en la descomposición de la representación natural, asociada al conjunto de las rectas isótropas en $\mathcal{V}$, para los casos $\mathcal{V} = \mathcal{H} \perp \mathcal{H}'$ o $\mathcal{V} = \mathcal{H} \perp \mathbb{F}_{q^2}$, donde $\mathcal{H}$, $\mathcal{H}'$ son planos hiperbólico y $\mathbb{F}_{q^2}$ es el plano asociado a la extensión cuadrática de $\mathbb{F}_q$.

Para lo anterior definimos

$$\begin{aligned} \mathcal{L} &= \{l \leq \mathcal{V} \mid l \text{ es una recta isótropa}\} \\ &= \{< x > \mid Q(x) = 0, x \neq 0\} \end{aligned}$$

el conjunto de las rectas isótropas.

4.2.1. $\mathcal{V}$ suma de dos planos hiperbólicos

Consideremos $(\mathcal{H} =< e_1, e_2 >, Q_{\mathcal{H}}), (\mathcal{H}' =< e_3, e_4 >, Q_{\mathcal{H}'})$, los respectivos planos hiperbólicos, donde

$$\begin{aligned} Q_{\mathcal{H}} : \quad \mathcal{H} \quad &\to \mathbb{F}_q \\ (\alpha\ \beta) \quad &\rightsquigarrow \alpha\beta \end{aligned}$$

análogamente para $Q_{\mathcal{H}'}$. De esta manera $(\mathcal{V}, Q_{\mathcal{H}} \perp Q_{\mathcal{H}'})$ es nuestro espacio cuadrático. Además la forma bilineal asociada a Q es:

$$B((x, y, z, w), (a, b, c, d)) = \frac{1}{2}(xb + ya + zd + wc)$$

De la sección anterior obtuvimos que todo vector anisótropo, en un plano hiperbólico, es de la forma $(\alpha\ \lambda\alpha^{-1})$ y para los isótropos tenemos que son $(0\ \alpha)$ o $(\alpha\ 0)$, con $\alpha, \lambda\ \varepsilon\ \mathbb{F}_q^*$.

El conjunto de rectas isótropas está contenido por:

$$\begin{aligned} l_1(\alpha) &= < (1, 0, \alpha, 0) > \\ l_2(\alpha) &= < (1, 0, 0, \alpha) > \\ l_3(\alpha) &= < (0, 1, \alpha, 0) > \\ l_4(\alpha) &= < (0, 1, 0, \alpha) > \\ l_5(\alpha, \beta) &= < (1, \alpha, \beta, -\beta^{-1}\alpha) > \end{aligned}$$

además $< e_1 >, < e_2 >, < e_3 >, < e_4 >$, con $\alpha, \beta\ \varepsilon\ \mathbb{F}_q^*$. Luego tenemos que

$$\#\mathcal{L} = 4 + 4(q-1) + (q-1)^2 = (q+1)^2$$

Proposición 81

$$\mid O_4(\mathcal{V}) \mid = 2q^2(q-1)^2(q+1)^2$$

Demostración. Consideremos la siguiente acción

$$\begin{aligned} \cdot : \quad O_4(\mathcal{V}) \times (\mathcal{L} \times \mathcal{L}) \quad &\to (\mathcal{L} \times \mathcal{L}) \\ (\sigma, (l, l')) \quad &\rightsquigarrow (\sigma(l), \sigma(l')) \end{aligned}$$

de esta manera

$$\mid O_4(\mathcal{V}) \mid = \mid \mathcal{O}_{(l,l')} \mid \cdot \mid Stab_{(l,l')} \mid$$

Aplicaremos este resultado al elemento $(< e_1 >, < e_2 >)$.

1) Calculemos $\mid \mathcal{O}_{(<e_1>,<e_2>)} \mid$. Para ello veremos lo siguiente.

Sea $\mathcal{H} =< e_1, e_2 >$, un plano hiperbólico, luego por Teorema 2 de Witt, tenemos que el conjunto de los planos hiperbólicos es transitivo, ya que,

sean $\mathcal{H}_1, \mathcal{H}_2 \leq \mathcal{V}$, dos planos hiperbólicos, luego

$$\sigma: \ \mathcal{H}_1 \ \rightarrow \mathcal{H}_2$$

es una isometría, luego

$$\overline{\sigma}: \ \mathcal{H}_1 \ \rightarrow \mathcal{V}$$

es una isometría y por Witt, existe $\widehat{\sigma} \ \varepsilon \ O_4(\mathcal{V})$, que cumple con $\widehat{\sigma}(\mathcal{H}_1) = \sigma(\mathcal{H}_1) = \mathcal{H}_2$.

De lo anterior, basta contar los posibles pares de rectas, tal que estas rectas forman planos hiperbólicos, es decir, los pares $(< x >, < y >)$, tal que $B(x, y) \neq 0$.

Observemos que $(< x >, < y >) \neq (< y >, < x >)$. De esta forma contaremos en un sentido y después amplificamos por dos para obtener la cuenta total de estas posibles combinaciones.

a) Caso del tipo (l_1, l_2), tenemos que

$$\begin{aligned} B((1,0,\alpha,0),(1,0,0,\beta)) &\neq 0 \\ \alpha\beta &\neq 0 \end{aligned}$$

por lo tanto, existen $(q-1)^2$ posibles pares, con (l_1, l_2). Considerando (l_2, l_1), obtenemos $2(q-1)^2$ posibilidades.

Esta cantidad se repite en: (l_1, l_3), (l_2, l_4) y (l_3, l_4).

b) Caso del tipo (l_1, l_4). Tenemos que

$$\begin{aligned} B((1,0,\alpha,0),(0,1,0,\beta)) &\neq 0 \\ 1 &\neq -\alpha\beta \end{aligned}$$

así, existen $2(q-1)(q-2)$ posible pares

Lo mismo ocurre, para (l_2, l_3).

c) (l_1, l_5).

$$\begin{aligned} B((1,0,\alpha,0),(1,\beta,\gamma,-\beta\gamma^{-1})) &\neq 0 \\ \beta - \alpha\beta\gamma^{-1} &\neq 0 \\ \beta(1-\alpha\gamma^{-1}) &\neq 0 \qquad \text{como } \beta \neq 0 \\ 1 &\neq \alpha\gamma^{-1} \end{aligned}$$

por lo tanto obtenemos $2(q-1)^2(q-2)$ posibilidad. Esto se repite con (l_2, l_5), (l_3, l_5) y (l_4, l_5).

d) Con $(< e_1 >, l_3)$ obtenemos $2(q-1)$ posibilidades. Esto también ocurre con: $(< e_1 >, l_4)$, $(< e_2 >, l_1)$, $(< e_2 >, l_2)$, $(< e_3 >, l_2)$, $(< e_3 >, l_4)$, $(< e_4 >, l_1)$ y $(< e_4 >, l_3)$

e) $(< e_1 >, l_5)$. Aquí tenemos

$$\begin{aligned} B((1,0,0,0),(1,\beta,\gamma,-\beta\gamma^{-1})) &\neq 0 \\ \beta &\neq 0 \end{aligned}$$

entonces, existen $2(q-1)^2$ posibilidades. Lo mismo ocurre para:

$$(< e_2 >, l_5),\ (< e_3 >, l_5) \text{ y } (< e_4 >, l_5)$$

f) (l_5, l_5).

$$\begin{aligned} B((1,\alpha,\beta,-\alpha\beta^{-1}),(1,\gamma,\delta,-\gamma\delta^{-1})) &\neq 0 \\ \alpha+\gamma-\beta\gamma\delta^{-1}-\alpha\delta\beta^{-1} &\neq 0 \qquad \text{colocando } u=\beta\delta^{-1} \\ \alpha(1-u^{-1})+\gamma(1-u) &\neq 0 \end{aligned}$$

i) $u=0$. Este caso es imposible, ya que $\beta,\delta\ \varepsilon\ \mathbb{F}_q^*$.

ii) $u=1$, implica que $0+0\neq 0$, lo cual es una contradicción.

iii) $u>1$, entonces u, tiene $(q-1)(q-2)$ posibilidades. Así de

$$\alpha(1-u^{-1})+\gamma(1-u)\neq 0$$

obtenemos en total $(q-1)^2(q-2)^2$.

g) Por ultimo, nos que $(< e_1 >, < e_2 >)$, $(< e_2 >, < e_1 >)$, $(< e_3 >, < e_4 >)$ y $(< e_4 >, < e_3 >)$.

Por lo tanto, de la suma de a), b),...,g) obtenemos que

$$\mid \mathcal{O}_{(<e_1>,<e_2>)} \mid = q^2(q+1)$$

2) Ahora, calcularemos el orden de $Stab_{(<e_1>,<e_2>)}$ en $O_4(\mathcal{V})$. Sea

$$H_0 = Stab_{\mathcal{H}} \perp O_2(\mathcal{H}') \leq O_4(\mathcal{V})$$

a) Sea $\sigma\ \varepsilon\ H_0$, entonces

$$\sigma = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} \perp \tau \qquad \text{o} \qquad \sigma = \begin{pmatrix} 0 & \alpha \\ \alpha^{-1} & 0 \end{pmatrix} \perp \tau$$

donde $\tau\ \varepsilon\ O_2(\mathcal{H}')$. Entonces

$$\left(\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} \perp \tau\right)(< e_1 >, < e_2 >) = (< e_1 >, < e_2 >)$$

pero
$$\left(\left(\begin{array}{cc} 0 & \alpha \\ \alpha^{-1} & 0 \end{array}\right) \perp \tau\right)(< e_1 >, < e_2 >) = (< e_2 >, < e_1 >)$$
De esta manera
$$\sigma = \left(\begin{array}{cc} \alpha & 0 \\ 0 & \alpha^{-1} \end{array}\right) \perp \tau$$
fija a $(< e_1 >, < e_2 >)$, para toda $\tau \ \varepsilon \ O_2(\mathcal{H}_2)$

b) Sea $\sigma \ \varepsilon \ Stab_{(<e_1>,<e_2>)}$ y supongamos que $\sigma(e_3) = \alpha e_1 + \beta e_2 + \gamma e_3 + \delta e_4$, entonces
$$\begin{aligned} 0 &= B(e_1, e_3) \\ &= B(\sigma(e_1), \sigma(e_3)) \\ &= B(e_1, \alpha e_1 + \beta e_2 + \gamma e_3 + \delta e_4) \\ &= \beta e_2 \end{aligned}$$
por lo tanto $\beta = 0$. Ahora si lo hacemos para e_2, es decir
$$\begin{aligned} 0 &= B(e_2, e_3) \\ &= B(\sigma(e_2), \sigma(e_3)) \\ &= B(e_2, \alpha e_1 + \beta e_2 + \gamma e_3 + \delta e_4) \\ &= \alpha e_2 \end{aligned}$$
obtenemos que $\alpha = 0$. De esta manera $\sigma(e_3) = \gamma e_3 + \delta e_4$. Ahora si suponemos algo parecido para $\sigma(e_4)$, obtenemos que $\sigma(e_4) = \gamma' e_3 + \delta' e_4$. De esta manera $\sigma(\mathcal{H}') \subseteq \mathcal{H}'$, por lo tanto $\sigma \ \varepsilon \ H_0$.

Por lo tanto
$$| \ Stab_{(<e_1>,<e_2>)} \ | = 2(q-1)^2$$
De esta manera
$$| \ O_4(\mathcal{V}) \ | = 2q^2(q-1)^2(q+1)^2$$
■

Proposición 82
$$| \ \mathcal{L} \times \mathcal{L}/O_4(\mathcal{V}) \ | = 3$$

Demostración. Por lo anterior, tenemos que $\mathcal{O}_{(<e_1>,<e_2>)}$ contiene a todos los pares de rectas que generan planos hiperbólicos, o de otra forma, contiene a $(< x >, < y >)$, tal que $B(x, y) \neq 0$.

Por lo tanto solo nos queda ver que sucede con aquellas rectas, en las cuales $B(x, y) = 0$, es decir, rectas ortogonales.

Para esto consideremos $\mathcal{O}_{(<e_1>,<e_3>)} = \{(\sigma(< e_1 >), \sigma(< e_3 >)) \mid \sigma \ \varepsilon \ O_4(\mathcal{V})\}$.

Supongamos que $(\sigma(< e_1 >), \sigma(< e_3 >)) = (< x >, < y >)$, entonces existe una isometría
$$\tau :< e_1, e_2 > \rightarrow < x, x' >$$

tal que $Q(x')=0$, recíprocamente existe

$$\tau' :< e_3, e_4 > \to < y, y' >$$

De esta forma $\tau \perp \tau' : \mathcal{V} \to < x, x' > \perp < y, y' >$, la cual pertenece a $O_4(\mathcal{V})$. Por lo tanto

$$\mathcal{O}_{(<e_1>,<e_3>)} = \{(< x >, < y >) \mid B(x,y) = 0 \text{ y } x \neq y\}$$

Así

$$\mathcal{O}_{(<e_1>,<e_1>)} = \{(< x >, < x >) \mid Q(x) = 0\}$$

y por lo tanto

$$\mathcal{L} \times \mathcal{L}/O_4(\mathcal{V}) = \{\mathcal{O}_{(<e_1>,<e_1>)}, \mathcal{O}_{(<e_1>,<e_2>)}, \mathcal{O}_{(<e_1>,<e_3>)}\}$$

y así

$$\mid \mathcal{L} \times \mathcal{L}/O_2(\mathcal{V}) \mid = 3$$

■

Notación. Sean $l, l' \,\varepsilon\, \mathcal{L}$.

Si l, l' son ortogonales, lo denotamos por $l \perp l'$, en caso contrario lo denotamos como $l \not\perp l'$.

Construcción de los Núcleos

Consideremos $\mathcal{B} = \{\delta_l \mid l \,\varepsilon\, L^2(\mathcal{L})\}$ una base de $L^2(\mathcal{L})$. Entonces para cada una de las órbitas, construimos la función característica, dada por:

$$\begin{aligned} K_{(l,l')} : \quad & \mathcal{L} \times \mathcal{L} && \to \mathbb{C} \\ & (l_1, l_2) && \rightsquigarrow K_{(l,l')}(l_1, l_2) = \begin{cases} 1 & (l_1, l_2) \,\varepsilon\, \mathcal{O}_{(l,l')} \\ 0 & (l_1, l_2) \notin \mathcal{O}_{(l,l')} \end{cases} \end{aligned}$$

De esta forma construimos los respectivos operadores de entrelazamiento, dados por:

a) Para la órbita $\mathcal{O}_{(<e_1>,<e_1>)}$, tenemos que su operador asociado es simplemente $1_{L^2(\mathcal{L})}$.

b) Para $\mathcal{O}_{(<e_1>,<e_2>)}$, obtenemos

$$\begin{aligned} \phi_{\not\perp} : \quad & L^2(\mathcal{L}) && \to L^2(\mathcal{L}) \\ & \delta_l && \rightsquigarrow \phi_{\not\perp}(\delta_l) = \sum_{l' \,\varepsilon\, \mathcal{L}} K_{(<e_1>,<e_2>)}(l', l)\delta_{l'} \\ & && = \sum_{\substack{l' \not\perp l \\ l' \neq l}} \delta_{l'} \end{aligned}$$

c) Para $\mathcal{O}_{(<e_1>,<e_3>)}$, obtenemos

$$\begin{aligned}\phi_\perp : \quad L^2(\mathcal{L}) &\to L^2(\mathcal{L})\\ \delta_l &\rightsquigarrow \phi_\perp(\delta_l) = \sum_{l' \,\varepsilon\, \mathcal{L}} K_{(<e_1>,<e_3>)}(l',l)\delta_{l'}\\ &= \sum_{\substack{l'\perp l\\ l'\neq l}} \delta_{l'}\end{aligned}$$

Para calcular las subrepresentaciones de $L^2(\mathcal{L})$, utilizaremos la Proposición 15, junto al operador $\phi_\perp$.

Proposición 83 $L^2(\mathcal{L})$ *se descompone como:*

$$L^2(\mathcal{L}) = \oplus V_\alpha$$

donde V_α *son los espacios propios asociados a* $\phi_\perp$*.*

Demostración. Primero realizaremos unos cálculos previos, teniendo en cuenta que $\phi = \alpha 1_{L^2(\mathcal{L})} + \beta\phi_\perp + \gamma\phi_{\not\perp}$, para todo ϕ un operador de entrelazamiento de $L^2(\mathcal{L})$.

a) Calculemos $\alpha, \beta, \gamma \,\varepsilon\, \mathbb{C}$, tal que $\phi_\perp^2 = \alpha 1_{L^2(\mathcal{L})} + \beta\phi_\perp + \gamma\phi_{\not\perp}$.

$$\begin{aligned}\phi_\perp^2(\delta_{<e_1>}) &= \sum_{l\perp <e_1>} \phi_\perp(\delta_l)\\ &= \sum_{l\perp <e_1>} \sum_{l'\perp l} \delta_{l'}\end{aligned}$$

donde el conjunto de rectas ortogonales a $< e_1 >$ son

$$\{< (1,0,\alpha,0) >, < (1,0,0,\alpha) >, < e_3 >, < e_4 > \mid \alpha \,\varepsilon\, \mathbb{F}_q^*\}$$

de esta forma obtenemos que

$$\phi_\perp^2(\delta_{<e_1>}) = (2q 1_{L^2(\mathcal{L})} + (q-1)\phi_\perp + 2\phi_{\not\perp})(\delta_{<e_1>})$$

como $\delta_{<e_1>}$ es base de $L^2(\mathcal{L})$, entonces

$$\phi_\perp^2 = 2q 1_{L^2(\mathcal{L})} + (q-1)\phi_\perp + 2\phi_{\not\perp}$$

Si realizamos un calculo parecido para $\phi_{\not\perp} \circ \phi_\perp$, obtenemos que

$$\phi_{\not\perp}(\phi_\perp) = q\phi_\perp + 2(q-1)\phi_{\not\perp}$$

b)

$$\begin{aligned}
\phi_{\perp}^3 &= \phi_{\perp}^2(\phi_{\perp}) \\
&= 2q\phi_{\perp} + (q-1)\phi_{\perp}^2 + 2\phi_{\not\perp}(\phi_{\perp}) \\
&= 2q(q-1)1_{L^2(\mathcal{L})} + (q+1)^2\phi_{\perp} + 6(q-1)\phi_{\not\perp}
\end{aligned}$$

Resolviendo el sistema

$$\begin{aligned}
\phi_{\perp}^2 &= 2q1_{L^2(\mathcal{L})} + (q-1)\phi_{\perp} + 2\phi_{\not\perp} \\
\phi_{\perp}^3 &= 2q(q-1)1_{L^2(\mathcal{L})} + (q+1)^2\phi_{\perp} + 6(q-1)\phi_{\not\perp}
\end{aligned}$$

obtenemos que

$$\phi_{\perp}^3 - 3(q-1)\phi_{\perp}^2 + 2(q^2-4q+1)\phi_{\perp} + 4q(q-1)1_{L^2(\mathcal{L})} = 0$$

de esta forma el polinomio anulador de $\phi_{\perp}$ es:

$$P_{\phi_{\perp}}(x) = (x-2q)(x+2)(x-(q-1))$$

Ahora

$$tr([\phi_{\perp}]_{\mathcal{B}}) = 0$$

dado que $\phi_{\perp}$, no tienen puntos fijos, así

$$2q \dim V_{2q} - 2\dim V_{-2} + (q-1)\dim V_{(q-1)} = 0$$

además

$$\dim V_{2q} + \dim V_{-2} + \dim V_{(q-1)} = (q+1)^2$$

de esta forma obtenemos que

$$\begin{aligned}
\dim V_{2q} &= 1 \\
\dim V_{-2} &= q^2 \\
\dim V_{(q-1)} &= 2q
\end{aligned}$$

Luego

$$L^2(\mathcal{L}) = V_{2q} \oplus V_{-2} \oplus V_{(q-1)}$$

■

4.2.2. $\mathcal{V}$ suma de un plano hiperbólico y un plano anisótropo

Con las notaciones anteriores, tenemos que $(\mathcal{H} \perp \mathbb{F}_{q^2}, Q_{\mathcal{H}} \perp N)$ es nuestro espacio cuadrático, con

$$B((x,y,z,w),(a,b,c,d)) = \frac{1}{2}(xb+ya) + zc - \delta wd$$

la forma bilineal simétrica asociada a Q.

De esta forma, el conjunto de rectas isótropas es :

$$\mathcal{L} = \{< e_1 >, < e_2 >, < (1, -\alpha^2 + \delta\beta^2, \alpha, \beta) >| \ \alpha, \beta \ \varepsilon \ \mathbb{F}_q; \alpha = 0 \veebar \beta = 0\}$$

Además tenemos

$$\#\mathcal{L} = q^2 + 1$$

Para encontrar la descomposición en subrepresentaciones irreducibles, trabajaremos en forma similar al caso anterior.

Proposición 84

$$| \ \mathcal{L} \times \mathcal{L}/O_4(\mathcal{V}) \ | = 2$$

Demostración. para calcular este número, primero veremos las rectas ortogonales y no ortogonales. Para esto, tenemos que

$$\begin{aligned}
B(e_1, e_2) &\neq 0 \\
B(e_1, (1, -\alpha^2 + \delta\beta^2, \alpha, \beta)) &\neq 0 \\
B(e_2, (1, -\alpha^2 + \delta\beta^2, \alpha, \beta)) &\neq 0 \\
B((1, -\alpha^2 + \delta\beta, \alpha, \beta), (1, -a^2 + \delta b^2, a, b)) &= \begin{cases} 0 & \alpha = a, \beta = b \\ \gamma \ \varepsilon \ \mathbb{F}_q^* & \text{en otro caso} \end{cases}
\end{aligned}$$

por lo tanto, $\mathcal{L}$ es un conjunto con rectas no ortogonales entre ellas.

De esta forma, por Witt, tenemos que $\mathcal{O}_{(<e_1>,<e_2>)}$ contiene a todos los pares de rectas, las cuales son no ortogonales y $\mathcal{O}_{(<e_1>,<e_1>)}$ contiene las rectas ortogonales a si mismas. Así

$$\mathcal{L} \times \mathcal{L}/O_4(\mathcal{V}) = \{O_{(<e_1>,<e_1>)}, \mathcal{O}_{(<e_1>,<e_2>)}\}$$

y por lo tanto

$$| \ \mathcal{L} \times \mathcal{L}/O_4(\mathcal{V}) \ | = 2$$

■

Proposición 85

$$L^2(\mathcal{L}) = \mathcal{U}_{\mathbb{1}} \oplus (\mathcal{U}_{\mathbb{1}})^{\perp}$$

Demostración. Como ya sabemos, $\mathcal{U}_{\mathbb{1}}$ el espacio constante, siempre se encuentra en la descomposición de $L^2(X)$, con X un conjunto finito. De esta manera, por la Proposición 14,

$$L^2(\mathcal{L}) = \mathcal{U}_{\mathbb{1}} \oplus (\mathcal{U}_{\mathbb{1}})^{\perp}$$

es la descomposición en subrepresentaciones irreducibles de $L^2(\mathcal{L})$. ■

Bibliografía

[1] O. T. O'Meara, Introduction to Quadratic Forms, Springe-Verlag, 1963.

[2] Jesus Juyumaya, Apuntes de Algebra Lineal, Universidad de Valparaíso, 2003.

[3] Jean-Pierre Serre, Linear Representations of Finite Groups, Hermann, 1967.