UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS

Matrices de Clifford y Transformaciones de Möbius

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

MATEMÁTICA

P R E S E N T A:

Helena Lizárraga Collí

DIRECTOR DE TESIS:
Dr. Antonio Lascurain Orive

Ciudad Universitaria, Ciudad de México, 2018

Hoja de datos del jurado

1. Datos del alumno

Lizárraga
Collí
Helena
686 115 9954
Universidad Nacional Autónoma de México
Facultad de Ciencias
Matemáticas
414004298

2. Datos del tutor

Dr.
Antonio
Lascurain
Orive

3. Datos del sinodal 1

Dr.
Javier
Bracho
Carpizo

4. Datos del sinodal 2

Dr.
Pierre
Michel
Bayard

5. Datos del sinodal 3

M. en C.
José Antonio
Gómez
Ortega

6. Datos del sinodal 4

Dr.
Alberto
León
Kushner
Schnur

7. Datos del trabajo escrito

Matrices de Clifford y Transformaciones de Möbius
58 p.
2018

Agradecimientos

Le agradezco a mi papá Alfonso, que en paz descanse, por motivarme a siempre aprender más y a luchar por la justicia y por la vida, a mi mamá Rosario, por su cariño y cuidados incondicionales; a ambos por inspirarme a estudiar y por el gran ejemplo de amor que me han demostrado. A mi hermano Joel por acompañarme todos los años de mi vida, por motivarme a ser una mejor persona y estar ahí siempre que lo he necesitado.

Gracias a Pablo, junto con quien he aprendido mucho los últimos años, tanto de matemáticas como de la vida en general, por su agradable compañía, cariño y apoyo tanto en los momentos divertidos como en los difíciles.

Doy gracias a mi tía Chayo, a mis tíos Olga y Franciso y a mi tío José por las reuniones familiares y por permanecer unidos en todo momento. También doy gracias a toda mi familia y amigos por acompañarme en este camino de la vida y en particular en la etapa universitaria.

Agradezco al profesor Antonio Lascurain por su apoyo, paciencia y por todo el tiempo dedicado a mi aprendizaje durante la carrera y por ayudarme en la realización de esta tesis.

También le doy gracias a mis sinodales Javier Bracho, Pierre Bayard, Toño Gómez y León Kushner por el tiempo y la atención dedicada a esta tesis.

Finalmente, gracias a la UNAM y a la Facultad de Ciencias por darme la oportunidad de estudiar la bella carrera de matemáticas y tener un espacio divertido donde puedo aprender y desarrollarme profesionalmente.

Introducción

Los grupos de transformaciones Möbius resultan ser de enorme importancia en la matemática actual. En particular, $PSL(2,\mathbb{Z})$, $PSL(2,\mathbb{R})$ y $PSL(2,\mathbb{C})$ juegan un papel esencial en muchas áreas, como la topología de las variedades de dimensión 3 y la teoría de los números, entre otras. De manera especial, los grupos de Möbius proporcionan un enorme caudal de información a la geometría hiperbólica. Véase, por ejemplo, [4] y ciertamente esta información coadyuva a conocer las 3-variedades hiperbólicas y por ende, las posibles formas del universo [1].

Ahlfors observó, usando trabajos anteriores ([7]) que se podía trabajar con las transformaciones de Möbius en cualquier dimensión, usando matrices de 2x2 (lo cual es un hecho notable). Las entradas de estas matrices son elementos del grupo de Clifford, que cumplen una importante propiedad de conjugación. Wada ([9]) desarrolló esta técnica para presentar una versión unificada de tres modelos del espacio hiperbólico n-dimensional, y probando ciertos teoremas de invariancia bajo conjugación en el álgebra de Clifford, exhibe formas normales (canónicas) de las transformaciones de Möbius en cualquier dimensión.

En esta tesis se desarrollan con detalle y formalidad las técnicas usadas por Wada para el análisis de sus resultados, como el manejo de ciertos invariantes bajo conjugación (Teorema 2.0.3) y las propiedades de las matrices de Clifford (Proposición 3.0.7), en particular, su identificación con el grupo general de Möbius actuando en $\mathbb{R}^n$.

En el primer capítulo se prueban las propiedades básicas del álgebra de Clifford $C^{n,p}$ y del comportamiento de sus automorfismos y antiautomorfismos principales (la involución principal, la reversión y la conjugación). Se define el grupo de Clifford $\Gamma^{n,p}$ y la conjugación que lo caracteriza $\rho_a : v \to av(a')^{-1}$, que resulta ser ortogonal (Proposición 1.0.5). Se prueba que los vectores, es decir, los elementos del espacio euclidiano de dimensión

$n+p$ con la forma cuadrática que define el Álgebra de Clifford (este espacio es denotado por $E^{n,p}$), están en este grupo. Además se prueba que en cualquier espacio ortogonal no degenerado X de dimensión finita, cualquier transformación ortogonal se puede expresar como composición de reflexiones en hiperplanos de codimensión 1(Teorema 1.0.10) y en consecuencia se exhibe un epimorfismo de $\Gamma^{n,p}$ en $O(n,p)$ (este último denota el grupo de transformaciones ortogonales de $E^{n,p}$), dado por $a \to \rho_a$ (Proposición 1.0.12). Como corolario se caracteriza a los elementos en $\Gamma^{n,p}$ como producto de vectores invertibles (Corolario 1.0.13). En el capítulo dos se prueban varios resultados sobre la conjugación en el álgebra de Clifford mediante elementos del grupo de Clifford, que son muy importantes para entender los resultados de Wada, en particular el Teorema 2.0.3.

En el último capítulo se identifica al grupo de matrices de Clifford $\mathscr{C}^n$ con el grupo de transformaciones de Möbius. En primera instancia se prueba un resultado que identifica a los elementos del grupo de Clifford $\overline{\Gamma}^n = \Gamma^n \cup \{0\}$ como suma de elementos de $\overline{\Gamma}^{n-1}$, uno de estos multiplicado por i_n, el elemento n-ésimo de la base (Proposición 3.0.4). Se definen las matrices de Clifford, que son matrices de 2x2 cuyas entradas son elementos de $\overline{\Gamma}^n$ que cumplen ciertas propiedades del determinante y de los productos de sus entradas. Este resultado, simplifica las condiciones que definen a estas matrices (Proposición 3.0.7). Usando esto se prueba que las matrices de Clifford forman un grupo. Los resultados mencionados involucran técnicas sofisticadas que requieren largos cálculos. Para estos propósitos se identifican también los anillos $M(2, End(C^n)$ y $End((C^n)^2)$ (Lema 3.0.5). Finalmente, se prueba que estas matrices actúan en E^n (el espacio euclidiano n-dimensional) de manera continua (Proposiciones 3.0.11 y 3.0.12). La tesis concluye identificando a estas matrices con el grupo general de Möbius actuando en $\mathbb{R}^n$. Se prueba que cualquier transformación definida por alguna matriz de Clifford es producto de matrices de Clifford que representan traslaciones, homotecias, transformaciones ortogonales o la inversión en la esfera unitaria $x \to x^*$ y viceversa, cualquier transformación de Möbius en cualquier dimensión se puede expresar de esta manera.

Contenido

Capítulo 1

El Álgebra de Clifford

Recordamos que un espacio ortogonal es un espacio vectorial con un producto escalar asociado. Sea $E^{n,p}$ el espacio ortogonal real con una forma cuadrática q de tipo (n,p). Fijamos una base $B = \{i_1, \ldots, i_n, i_{n+1}, \ldots, i_{n+p}\}$ de $E^{n,p}$.

La forma cuadrática q es la inducida por el producto escalar

$$\langle , \rangle : E^{n,p} \times E^{n,p} \to \mathbb{R}$$

dado por

$$\langle u, v\rangle = -\sum_{j=1}^{n} u_j v_j + \sum_{j=n+1}^{n+p} u_j v_j \tag{1.1}$$

donde $u = \Sigma_{j=1}^{n+p} u_j i_j, v = \Sigma_{j=1}^{n+p} v_j i_j$, de modo que: si $v \in E^{n,p}$, entonces

$$q(v) = \langle v, v\rangle = -\sum_{j=1}^{n} v_j^2 + \sum_{j=n+1}^{n+p} v_j^2.$$

Sea $C^{n,p}$ el álgebra de Clifford de $E^{n,p}$, esto es, los elementos de B satisfacen:

$$i_j^2 = -1 \qquad \text{si} \quad j \in \{1, \ldots, n\}$$

$$i_j^2 = 1 \qquad \text{si} \quad j \in \{n+1, \ldots, n+p\}$$

$$i_j i_k = -i_k i_j \quad \text{si} \quad j, k \in \{1, \ldots, n+p\},\ j \neq k.$$

$C^{n,p}$ es generado por B como una $\mathbb{R}$-álgebra.

Cualquier elemento $a \in C^{n,p}$ puede ser escrito de manera única como:

$$\sum a_I I, \quad a_I \in \mathbb{R}$$

donde I varía entre los elementos de

$$\mathscr{B} = \{i_{j_1} \cdots i_{j_r} | 0 \leq r \leq n+p,\ j_1 < \cdots < j_r\}.$$

En particular se tiene que, como los elementos de $\mathscr{B}$ varían sobre las combinaciones de los $n+p$ elementos de la base B usando r elementos, con $r \in \{0, \ldots, n+p\}$, entonces se sigue del teorema del binomio que $|\mathscr{B}| = 2^{n+p}$, es decir, $C^{n,p}$ es un espacio vectorial real de dimensión 2^{n+p}.

Para $a = \Sigma a_I I \in C^{n,p}$ se define su norma como: $|a| = \sqrt{\Sigma a_I^2}$. Para $I = i_{j_1} ... i_{j_r} \in \mathscr{B}$, se dice que su longitud es r y se denota por $l(I)$.

Para cualquier $v \in E^{n,p}$ se tiene que

$$v^2 = q(v), \tag{1.2}$$

porque si $v = \sum_{j=1}^{n+p} v_j i_j$, entonces

$$\begin{aligned} v^2 &= \left(\sum_{j=1}^{n+p} v_j i_j\right)^2 = \sum_{j,k=1}^{n+p} v_j v_k i_j i_k \\ &= \sum_{j=1}^{n+p} v_j^2\, i_j^2 + \sum_{j<k}^{n+p} v_j v_k i_j i_k + \sum_{k<j}^{n+p} v_j v_k i_j i_k \\ &= \sum_{j=1}^{n} v_j^2\, i_j^2 + \sum_{j=n+1}^{n+p} v_j^2\, i_j^2 + \sum_{j<k}^{n+p} v_j v_k i_j i_k + \sum_{k<j}^{n+p} v_k v_j (-i_k i_j) \\ &= -\sum_{j=1}^{n} v_j^2 + \sum_{j=n+1}^{n+p} v_j^2 = q(v). \end{aligned}$$

Usamos la siguiente notación:

Para cada entero k:

$$\begin{aligned} C^{n,p\,(k)} &= \{\Sigma a_I I \in C^{n,p} \mid l(I) \neq k \Rightarrow a_I = 0\}, \\ C^{n,p}_{par} &= \bigoplus_{k \in 2\mathbb{N}} C^{n,p\,(k)}, \\ C^{n,p}_{impar} &= \bigoplus_{k \in 2\mathbb{N}-1} C^{n,p\,(k)}, \end{aligned}$$

donde $\bigoplus$ denota la suma directa de espacios vectoriales.

Para cada $A \subseteq C^{n,p}$:

$$\begin{aligned} A^{(k)} &= A \cap C^{n,p\,(k)}, \\ A_{par} &= A \cap C^{n,p}_{par}, \\ A_{impar} &= A \cap C^{n,p}_{impar}. \end{aligned}$$

Para cada elemento $a = \Sigma a_I I \in C^{n,p}$:

$$a^{(k)} = \sum_{l(I)=k} a_I I \in C^{n,p}$$

Notamos que entonces $C^{n,p}$ tiene una descomposición en sumas directas:

$$C^{n,p} = \bigoplus_{k=0}^{n+p} C^{n,p\,(k)},$$

donde $C^{n,p\,(0)} = \mathbb{R}$, y $C^{n,p\,(1)} = E^{n,p}$.

Definición 1 *Para un elemento $a = \Sigma a_I I \in C^{n,p}$, se definen:*

$$\begin{aligned} a' &= \Sigma a_I (-1)^{l(I)} I, \\ a^* &= \Sigma a_I (-1)^{\frac{l(I)(l(I)-1)}{2}} I, \\ a^- &= \Sigma a_I (-1)^{\frac{l(I)(l(I)+1)}{2}} I \end{aligned}$$

Notamos que si $I \in \mathscr{B}$, para la transformación $a \to a'$, los términos que tengan como factor a I cambian de signo si y sólo si $l(I)$ es impar.

Para $a \to a^*$, como

$$\begin{aligned} \frac{l(I)(l(I)-1)}{2} = 2k &\iff l(I)(l(I)-1) = 4k, \quad k \in \mathbb{Z} \\ &\iff l(I) = 4k_1 \quad o \quad l(I) - 1 = 4k_2, \quad k_1, k_2 \in \mathbb{Z} \\ &\iff l(I) \equiv 0 \ \ mod(4) \quad o \quad l(I) \equiv 1 \ \ mod(4), \end{aligned}$$

entonces los términos que tengan como factor a I cambian de signo si y sólo si $l(I) \equiv 2 \ \ mod(4)$ ó $l(I) \equiv 3 \ \ mod(4)$.

Para $a \to a^-$, como

$$\begin{aligned}\frac{l(I)(l(I)+1)}{2} = 2k &\iff l(I)(l(I)+1) = 4k, \quad k \in \mathbb{Z} \\ &\iff l(I) = 4k_1 \quad o \quad l(I)+1 = 4k_2, \quad k_1, k_2 \in \mathbb{Z} \\ &\iff l(I) \equiv 0 \ mod(4) \quad o \quad l(I) \equiv 3 \ mod(4),\end{aligned}$$

entonces los términos que tengan como factor a I cambian de signo si y sólo si $l(I) \equiv 1 \bmod(4)$ ó $l(I) \equiv 2 \bmod(4)$.

Observamos que si $a \in C^{n,p}$, podemos escribirlo como

$$a = a^{(0)} + a^{(1)} + a^{(2)} + a^{(3)} + ... + a^{(n+p)},$$

y entonces,

$$\begin{aligned}a' &= a^{(0)} - a^{(1)} + a^{(2)} - a^{(3)} + ... + (-1)^k a^{(k)} + ... \pm a^{(n+p)}, \\ a^* &= a^{(0)} + a^{(1)} - a^{(2)} - a^{(3)} + ... + (-1)^{\frac{k(k-1)}{2}} a^{(k)} + ... \pm a^{(n+p)}, \\ a^- &= a^{(0)} - a^{(1)} - a^{(2)} + a^{(3)} + ... + (-1)^{\frac{k(k+1)}{2}} a^{(k)} + ... \pm a^{(n+p)}.\end{aligned}$$

Proposición 1.0.1 *Las transformaciones $a \to a'$, $a \to a^*$ y $a \to a^-$ conmutan entre sí y además son biyecciones de $C^{n,p}$. Más aún, se tiene que son involuciones, es decir $(a')' = (a^*)^* = (a^-)^- = a$.*

Demostración. Debido a las observaciones anteriores, vemos que estas transformaciones conmutan entre sí, puesto que no importa el orden en que se cambian los signos en cada término de a al aplicar cada transformación. También tenemos que $(a')' = (a^*)^* = (a^-)^- = a$ ya que al aplicar una vez una de estas transformaciones, cambia el signo de los términos de a de la manera señalada anteriormente, por lo que al aplicarlo una segunda vez, volverá a cambiar el signo del mismo modo, obteniendo a finalmente. □

Proposición 1.0.2 *Se tiene que $a^- = (a^*)' = (a')^*$*

Demostración. Debido a la conmutatividad de las transformaciones, basta ver únicamente la primera igualdad. La transformación $a \to a^-$ cambia los signos de los términos que tengan como factor a I con $l(I) \equiv 1 \ mod(4)$ ó $l(I) \equiv 2 \ mod(4)$. Ahora, si en a tenemos un término que contiene como factor a I, entonces al aplicar $a \to a^*$, este cambiará de signo si y sólo si

$l(I) \equiv 2 \ mod(4)$ ó $l(I) \equiv 3 \ mod(4)$, por lo que si ahora aplicamos $a \to a'$, cambiará el signo si y sólo si $l(I) \equiv 1 \ mod(4)$ ó $l(I) \equiv 3 \ mod(4)$, de modo que al aplicar la transformación $a \to (a^*)'$ cambian los signos si y sólo si $l(I) \equiv 1 \ mod(4)$ ó $l(I) \equiv 2 \ mod(4)$. □

Teorema 1.0.3 *La transformación $a \to a'$ es automorfismo de $C^{n,p}$ y las transformaciones $a \to a^*$ y $a \to a^-$ son antiautomorfismos de $C^{n,p}$.*

Demostración. Es suficiente ver que $a \to a'$ es automorfismo y que $a \to a^*$ es antiautomorfismo, pues como $a^- = (a^*)'$, esto implica que $a \to a^-$ es antiautomorfismo de $C^{n,p}$.

Debido a la linealidad de la suma se tiene que las transformaciones definidas anteriormente son lineales, por lo que basta ver que $(IJ)' = I'J'$ y que $(IJ)^* = J^*I^*$ donde $I, J \in \mathscr{B}$.

Primero veamos que si $I = i_{k_1}...i_{k_r}, J = i_{j_1}...i_{j_s} \in \mathscr{B}$, se tiene que $IJ \in \mathscr{B}$ es de la forma $IJ = (-1)^m i_{l_1}...i_{l_t}$, entonces

$$(IJ)' = ((i_{k_1}...i_{k_r})(i_{j_1}...i_{j_s}))' = ((-1)^m i_{l_1}...i_{l_t})' = (-1)^{t+m} i_{l_1}...i_{l_t}.$$

Por otra parte

$$\begin{aligned} I'J' &= (i_{k_1}...i_{k_r})'(i_{j_1}...i_{j_s})' = (-1)^r (i_{k_1}...i_{k_r})(-1)^s (i_{j_1}...i_{j_s}) \\ &= (-1)^{r+s}(i_{k_1}...i_{k_r})(i_{j_1}...i_{j_s}) = (-1)^{r+s+m} i_{l_1}...i_{l_t}, \end{aligned}$$

de donde se tiene que

$$(IJ)' = I'J' \iff r+s+m \equiv t+m \ \ mod(2) \iff r+s \equiv t \ \ mod(2).$$

Esto último sí sucede ya que al multiplicar dos elementos de B estos conmutan y cambian signo si $i_{j_p} \neq i_{k_q}$ (lo cual no modifica la longitud) o bien, se multiplican consigo mismos si $i_{j_p} = i_{k_q}$ (lo cual disminuye la longitud por 2), de donde se sigue que $r+s$ y t tienen la misma paridad.

Ahora veamos por inducción sobre r que $(i_{j_1}...i_{j_r})^* = i_{j_r}...i_{j_1}$, donde $i_{j_1}...i_{j_r} \in \mathscr{B}$.

Para $r = 1$, $(i_{j_1})^* = (-1)^{\frac{(1)(0)}{2}} i_{j_1} = i_{j_1}$.

Supongamos que para $i_{j_1}...i_{j_r} \in \mathscr{B}$, se tiene que $(i_{j_1}...i_{j_r})^* = i_{j_r}...i_{j_1}$.

Sea $i_{j_1}...i_{j_r}i_{j_{r+1}} \in \mathscr{B}$, entonces:

$$\begin{aligned}(i_{j_1}...i_{j_r}i_{j_{r+1}})^* &= (-1)^{\frac{(r+1)(r)}{2}} i_{j_1}...i_{j_r}i_{j_{r+1}} = (-1)^{\frac{r(r-1+2)}{2}} i_{j_1}...i_{j_r}i_{j_{r+1}} \\ &= ((-1)^{\frac{r(r-1)}{2}} i_{j_1}...i_{j_r})((-1)^r i_{j_{r+1}}) = (i_{j_1}...i_{j_r})^*((-1)^r i_{j_{r+1}}) \\ &= i_{j_r}...i_{j_1}((-1)^r i_{j_{r+1}}) = (-1)^r(i_{j_r}...i_{j_1})(i_{j_{r+1}}) \\ &= (-1)^{2r} i_{j_{r+1}} i_{j_r}...i_{j_1} = i_{j_{r+1}} i_{j_r}...i_{j_1},\end{aligned}$$

donde la penúltima igualdad se tiene debido a que $\forall k \in \{1, ..., r\}, j_{r+1} \neq j_k$, ya que $i_{j_1}...i_{j_r}i_{j_{r+1}} \in \mathscr{B}$. □

A la transformación $a \to a'$ se le llama la **involución principal**, mientras que $a \to a^*$ es la **reversión** y $a \to a^-$ es la **conjugación**.

A los elementos de $E^{n,p}$ se les llamará vectores.

Definición 2 *Se define*

$$\Gamma^{n,p} := \{a \in C^{n,p} \,|\, a \text{ es invertible y } \forall v \in E^{n,p}\, av(a')^{-1} \in E^{n,p}\}$$

Notamos que el conjunto anterior está bien definido, es decir que si a es invertible, entonces también a' lo es. Esto se tiene ya que $a \to a'$ es automorfismo de $C^{n,p}$ y por tanto $a'(a^{-1})' = (aa^{-1})' = 1 = (a^{-1}a)' = (a^{-1})'a'$, lo que implica que a' es invertible y además $(a')^{-1} = (a^{-1})'$.

Definición 3 *Dado $a \in \Gamma^{n,p}$, definimos la transformación $\rho_a : E^{n,p} \to E^{n,p}$ tal que $\rho_a(v) = av(a')^{-1}$.*

Proposición 1.0.4 *El conjunto $\Gamma^{n,p}$ es un grupo bajo la multiplicación. A $\Gamma^{n,p}$ se le llama el grupo de Clifford de $E^{n,p}$.*

Demostración. Sean $a, b \in \Gamma^{n,p}$. Se tiene que $(ab)^{-1} = b^{-1}a^{-1}$, ya que $(ab)(b^{-1}a^{-1}) = 1$. Ahora, dado $v \in E^{n,p}$ tenemos que

$$(ab)v((ab)')^{-1} = (ab)v(a'b')^{-1} = (ab)v((b')^{-1}(a')^{-1}) = a(bv(b')^{-1})(a')^{-1}$$

y como $b \in \Gamma^{n,p}$, entonces $bv(b')^{-1} \in E^{n,p}$, por lo que $a(bv(b')^{-1})(a')^{-1} \in E^{n,p}$, ya que $a \in \Gamma^{n,p}$. Esto implica que $ab \in \Gamma^{n,p}$, es decir, $\Gamma^{n,p}$ es cerrado bajo la multiplicación.

También tenemos que $1 \in \Gamma^{n,p}$ ya que $1^{-1} = 1$ y $1' = 1$, por lo que dado $v \in E^{n,p}$, $1v(1')^{-1} = v \in E^{n,p}$.

Notamos que ρ_a es una transformación lineal en el espacio de dimensión finita $E^{n,p}$. Ahora, como $\rho_a(v) = 0$ si y sólo si $v = 0$, entonces ρ_a es inyectiva, lo que equivale a que ρ_a sea suprayectiva. Así, dado $v \in E^{n,p}$, existe $u \in E^{n,p}$ tal que $\rho_a(u) = v$, es decir, $au(a')^{-1} = v$ de modo que

$$(a^{-1})v((a^{-1})')^{-1} = (a^{-1})(au(a')^{-1})((a^{-1})^{-1})' = (a^{-1}a)u((a')^{-1})a' = u \in E^{n,p},$$

lo que implica que $a^{-1} \in \Gamma^{n,p}$, por lo que $\Gamma^{n,p}$ contiene a los inversos multiplicativos de cada uno de sus elementos. □

Proposición 1.0.5 *Para $a \in \Gamma^{n,p}$, ρ_a es una transformación ortogonal de $E^{n,p}$, en el sentido definido por el producto interior dado en* (1.1).

Demostración. Basta ver que ρ_a preserva la forma cuadrática q ya que si $x, y \in E^{n,p}$, entonces por la bilinealidad del producto interior tenemos que $q(x+y) = \langle x+y, x+y\rangle = \langle x, x\rangle + 2\langle x, y\rangle + \langle y, y\rangle = q(x) + 2\langle x, y\rangle + q(y)$, lo que implica que

$$\langle x, y\rangle = \frac{q(x+y) - q(x) - q(y)}{2},$$

de donde se tendría que si ρ_a preserva la forma cuadrática q, entonces

$$\begin{aligned}\langle x, y\rangle &= \frac{q(x+y) - q(x) - q(y)}{2} \\ &= \frac{q(\rho_a(x+y)) - q(\rho_a(x)) - q(\rho_a(y))}{2} \\ &= \frac{q(\rho_a(x) + \rho_a(y)) - q(\rho_a(x)) - q(\rho_a(y))}{2} \\ &= \langle \rho_a(x), \rho_a(y)\rangle .\end{aligned}$$

Ahora notemos que si $v \in E^{n,p}$, entonces $v = -v'$ y por (1.2) se sigue que

$$\begin{aligned} q(\rho_a(v)) &= q(av(a')^{-1}) = (av(a')^{-1})^2 \\ &= (av(a')^{-1})(av(a')^{-1}) = -(av(a')^{-1})'(av(a')^{-1}) \\ &= -(a'v'((a')^{-1})')(av(a')^{-1}) = (a'(-v')a^{-1})(av(a')^{-1}) \\ &= (a'va^{-1})(av(a')^{-1}) = a'v^2(a')^{-1} = v^2a'(a')^{-1} \\ &= v^2 = q(v). \end{aligned}$$

Por lo que en efecto $\forall v \in E^{n,p}$, $q(\rho_a(v)) = q(v)$, es decir, ρ_a preserva la forma cuadrática q. □

Proposición 1.0.6 *Si $v \in E^{n,p}$ y $q(v) \neq 0$, entonces $v \in \Gamma^{n,p}$*

Demostración. Sea $v \in E^{n,p}$ tal que $q(v) \neq 0$. Notamos que v es invertible con inverso

$$v^{-1} = \frac{v}{q(v)}$$

ya que debido a (1.2) tenemos que

$$\frac{vv}{q(v)} = \frac{v^2}{q(v)} = 1.$$

Se afirma que $E^{n,p} = \langle v \rangle \oplus \langle v \rangle^{\perp}$, donde el complemento ortogonal es respecto al producto interior (1.1). Para probar esto, tomamos $\{v, u_1, ..., u_{n+p-1}\}$ una base para $E^{n,p}$ que contiene a v. Para $i \in \{1, ..., n+p-1\}$, consideramos $c_i = \dfrac{\langle u_i, v \rangle}{\langle v, v \rangle}$ y $w_i = u_i - c_i v$, de manera que

$$\langle w_i, v \rangle = \langle u_i - c_i v, v \rangle = \langle u_i, v \rangle - c_i \langle v, v \rangle = \langle u_i, v \rangle - \frac{\langle u_i, v \rangle}{\langle v, v \rangle} \langle v, v \rangle = 0,$$

es decir, $\forall i \in \{1, ..., n+p-1\}$ se tiene que $w_i \perp v$.

Tenemos que el conjunto $\{v, w_1, ..., w_{n+p-1}\}$ es una base de $E^{n,p}$. Para notar esto, como dicho conjunto es de cardinalidad $n+p$, basta ver que es un conjunto linealmente independiente.

Si para algunas $\lambda_0, \lambda_1, ..., \lambda_{n+p-1} \in \mathbb{R}$ sucede que

$$\lambda_0 v + \lambda_1 w_1 + ... + \lambda_{n+p-1} w_{n+p-1} = 0,$$

entonces se sigue que

$$\begin{aligned} 0 &= \lambda_0 v + \lambda_1 (u_1 - c_1 v) + ... + \lambda_{n+p-1}(u_{n+p-1} - c_{n+p-1} v) \\ &= \left(\lambda_0 - \sum_{i=1}^{n+p-1} \lambda_i c_i \right) v + \lambda_1 u_1 + ... + \lambda_{n+p-1} u_{n+p-1} \end{aligned}$$

de donde, por ser $\{v, u_1, ..., u_{n+p-1}\}$ un conjunto linealmente independiente, se tiene que $\forall i \in \{1, ..., n+p-1\}$ $\lambda_i = 0$ y $\lambda_0 - \sum_{i=1}^{n+p-1} \lambda_i c_i = 0$, lo que implica que también $\lambda_0 = 0$. Por lo anterior, $\{v, w_1, ..., w_{n+p-1}\}$ es un conjunto linealmente independiente y por tanto una base de $E^{n,p}$.

Sea $u = \lambda_0 v + \lambda_1 w_1 + ... + \lambda_{n+p-1} w_{n+p-1} \in \langle v \rangle^{\perp}$. Como $\langle u, v \rangle = 0$, entonces

$$0 = \langle u, v \rangle = \lambda_0 \langle v, v \rangle + \lambda_1 \langle w_1, v \rangle + ... + \lambda_{n+p-1} \langle w_{n+p-1}, v \rangle = \lambda_0 \langle v, v \rangle ,$$

por lo que $\lambda_0 = 0$ y con esto se tiene que $\langle v \rangle^{\perp} \subset \langle \{w_1, ..., w_{n+p-1}\} \rangle$.

Ahora, como $\{w_1, ..., w_{n+p-1}\} \subset \langle v \rangle^{\perp}$, entonces $\langle \{w_1, ..., w_{n+p-1}\} \rangle \subset \langle v \rangle^{\perp}$. Podemos concluir que $\langle \{w_1, ..., w_{n+p-1}\} \rangle = \langle v \rangle^{\perp}$.

Notamos ahora que si $u \in \langle v \rangle \cap \langle v \rangle^{\perp}$, entonces $\langle u, u \rangle = 0$ lo que implica que $u = 0$, esto es, $\langle v \rangle \cap \langle v \rangle^{\perp} = \{0\}$. De esto y de lo anterior, observamos que en efecto $E^{n,p} = \langle v \rangle \oplus \langle v \rangle^{\perp}$.

Sea $u \in E^{n,p}$. Por lo visto anteriormente, podemos escribir a u de la forma $u = tv + w$, con $t \in \mathbb{R}$ y $w \perp v$. Notamos que

$$\begin{aligned} v^2 + w^2 &= \langle v, v \rangle + 2\langle v, w \rangle + \langle w, w \rangle = \langle v + w, v + w \rangle \\ &= q(v + w) = (v + w)^2 = v^2 + vw + wv + w^2, \end{aligned}$$

de donde obtenemos que $vw = -wv$. Usando esto y el hecho de que $v = -v'$, tenemos que

$$\begin{aligned} vu(v')^{-1} &= v(tv + w)(v')^{-1} \\ &= (tv^2 + vw)(v')^{-1} \\ &= (tv^2 - wv)(v')^{-1} \\ &= (tv - w)v(v')^{-1} \\ &= (tv - w)(-v')(v')^{-1} \\ &= (tv - w)(-1) \\ &= -tv + w \in E^{n,p} \end{aligned}$$

Esto implica que $\forall u \in E^{n,p}\ vu(v')^{-1} \in E^{n,p}$ y como v es invertible, concluimos que $v \in \Gamma^{n,p}$. □

En la demostración del teorema anterior se probó que $E^{n,p} = \langle v \rangle \oplus \langle v \rangle^{\perp}$. Esto se puede generalizar por medio de la siguiente proposición.

Proposición 1.0.7 *Sea V un espacio ortogonal de dimensión finita. Si W es un subespacio vectorial de V tal que es no degenerado, entonces $V = W \oplus W^{\perp}$.*

Demostración. Primero notamos que si W es no degenerado, necesariamente $W \cap W^{\perp} = \{0\}$, pues si $x \in W \cap W^{\perp}$, entonces $x \in W$ es tal que para todo elemento $w \in W$ sucede que $\langle x, w \rangle = 0$, pero como W es no degenerado, el único elemento que puede cumplir con esto es el 0. Debido a lo anterior, es posible definir la suma directa $W \oplus W^{\perp}$.

Sean $\beta = \{w_1, ..., w_n\}$ y $\beta' = \{w'_1, ..., w'_n\}$ bases de W y de $W^{\perp}$, respectivamente. Ahora observemos que $\beta \cup \beta'$ es una base para $W \oplus W^{\perp}$. Esto se sigue ya que si

$$\alpha_1 w_1 + ... + \alpha_n w_n + \alpha'_1 w'_1 + ... + \alpha'_m w'_m = 0$$

entonces

$$\alpha_1 w_1 + ... + \alpha_n w_n = -(\alpha'_1 w'_1 + ... + \alpha'_m w'_m),$$

sin embargo, esto quiere decir que

$$\alpha_1 w_1 + ... + \alpha_n w_n\ ,\ -(\alpha'_1 w'_1 + ... + \alpha'_m w'_m) \in W \cap W^{\perp} = \{0\},$$

de manera que $\alpha_1 w_1 + ... + \alpha_n w_n = 0$ y $\alpha'_1 w'_1 + ... + \alpha'_m w'_m = 0$ y como cada uno de los conjuntos β y β' son linealmente independientes, debe suceder que todos los coeficientes son 0, es decir, $\forall i \in \{1, ..., n\}\ \alpha_i = 0$ y también $\forall j \in \{1, ..., m\}\ \alpha'_j = 0$. Esto implica que $\beta \cup \beta'$ es linealmente independiente.

Consideramos $\phi : V \to W \oplus W^{\perp}$ dada por

$$\phi(x) = \sum_{i=1}^{n} \langle x, w_i \rangle w_i\ +\ \sum_{i=1}^{m} \langle x, w'_i \rangle w'_i.$$

Como el producto interior es una forma bilineal, es fácil notar que ϕ es lineal. Ahora, si $x \in Ker(\phi)$ entonces

$$\sum_{i=1}^{n} \langle x, w_i \rangle w_i\ +\ \sum_{i=1}^{m} \langle x, w'_i \rangle w'_i = 0$$

y como $\beta \cup \beta'$ es base se tiene que $\forall i \in \{1, ..., n\}$ $\langle x, w_i \rangle = 0$ y también $\forall j \in \{1, ..., m\}$ $\langle x, w'_j \rangle = 0$, pero esto implica que $x \in W \cap W^{\perp}$, es decir $x = 0$ y podemos concluir que ϕ es inyectiva.

Como ϕ es una transformación lineal inyectiva de V en uno de sus subespacios, necesariamente ϕ es también suprayectiva y por tanto, es un isomorfismo. Se sigue del teorema de la dimensión, que

$$dim(V) = dim(Ker(\phi)) + dim(Im(\phi)) = dim(W \oplus W^{\perp})$$

y por lo tanto $V = W \oplus W^{\perp}$. □

Usando la proposición anterior, demostramos el siguiente teorema, que nos será útil más adelante.

Teorema 1.0.8 *Sea V un espacio ortogonal no degenerado de dimensión finita. Entonces V tiene una base ortonormal.*

Demostración. Procederemos por inducción sobre la dimensión de V.

Si $dim(V) = 1$ entonces $V = \langle v \rangle$. Como V es no degenerado, necesariamente $\langle v, v \rangle \neq 0$, por lo que

$$V = \langle \frac{v}{\|v\|} \rangle,$$

donde $\|v\| = \sqrt{|\langle v, v \rangle|}$.

Supongamos que todo espacio ortogonal no degenerado de dimensión $n-1$ tiene una base ortonormal.

Sea V un espacio ortogonal no degenerado de dimensión n. Podemos encontrar $v_1 \in V$ tal que $\langle v_1, v_1 \rangle \neq 0$. La afirmación anterior se tiene ya que como V es no degenerado, entonces existen $v, w \in V$ tales que $\langle v, w \rangle \neq 0$ y tomando en cuenta que $\langle v + w, v + w \rangle = \langle v, v \rangle + 2\langle v, w \rangle + \langle w, w \rangle$ como $2\langle v, w \rangle \neq 0$ entonces alguno de los otros sumandos debe ser distinto de 0. Dividiendo entre la norma de v_1, podemos suponer que v_1 es de norma 1.

Sea $W = \langle v_1 \rangle$. Como W es no degenerado, entonces por la proposición anterior se tiene que $V = W \oplus W^{\perp}$. Sin embargo, como $dim(W) = 1$ entonces $dim(W^{\perp}) = n - 1$ y por la hipótesis de inducción, $W^{\perp}$ tiene una base ortonormal, digamos $\{v_2, ..., v_n\}$. Así, al considerar $\{v_1, v_2, ..., v_n\}$ se tiene que $\forall i, j \in \{1, ..., n\}$ $v_i \perp v_j$ y el conjunto es linealmente independiente, pues si

$$\alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_n v_n = 0$$

entonces para todo $i \in \{1, ..., n\}$, como $\langle v_i, v_i \rangle = \pm 1$, tenemos

$$\pm\alpha_i = \alpha_i \langle v_i, v_i \rangle = \langle v_i, \alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_n v_n \rangle = \langle v_i, 0 \rangle = 0.$$

De manera que el conjunto $\{v_1, v_2, ..., v_n\}$ es una base ortonormal para V, lo que concluye la inducción. □

Definición 4 *Sea X un espacio ortogonal con descomposición en suma directa $X = W \oplus Y$, donde Y es subespacio vectorial de $W^\perp$. Decimos que la transformación*

$$X \to X \text{ dada por } w + y \to w - y, \text{ donde } w \in W,\ y \in Y$$

es una reflexión de X en W. Cuando $Y = W^\perp$ decimos que la transformación anterior es la reflexión de X en W.

Notamos que las reflexiones son transformaciones ortogonales ya que si $w_1, w_2 \in W$, $y_1, y_2 \in Y$, como Y es subespacio de $W^\perp$ se tiene que

$$\begin{aligned} \langle w_1 - y_1, w_2 - y_2 \rangle &= \langle w_1, w_2 \rangle + \langle w_1, -y_2 \rangle + \langle -y_1, w_2 \rangle + \langle -y_1, -y_2 \rangle \\ &= \langle w_1, w_2 \rangle + \langle y_1, y_2 \rangle = \langle w_1 + y_1, w_2 + y_2 \rangle. \end{aligned}$$

Si $x \in X$ es tal que $\langle x, x \rangle \neq 0$, entonces la reflexión de X en el hiperplano $\langle x \rangle^\perp$ será denotada por ρ_x. Si $\langle x, x \rangle = 0$, entonces $x \in \langle x \rangle \cap \langle x \rangle^\perp$ por lo que debería suceder que $x = 0$ o bien, $\langle x \rangle \cap (\langle x \rangle)^\perp \neq \{0\}$ y entonces no sería posible descomponer a X como la suma directa de ambos subespacios.

Observamos que en la prueba de la proposición 1.0.6, se demostró que **si $\mathbf{v} \in \mathbf{E^{n,p}}$ es tal que $\mathbf{q(v) \neq 0}$, entonces $\rho_{\mathbf{v}}$ es la reflexión en el hiperplano $\langle \mathbf{v} \rangle^\perp$**, es decir, la notación anterior se corresponde con la dada en la definición 3.

Denotamos por $O(n, p)$ al grupo de transformaciones ortogonales de $E^{n,p}$ y por $SO(n, p)$ al subgrupo de $O(n, p)$ que consiste en las transformaciones que preservan la orientación. Se tiene que $O(n, p)$ está generado por reflexiones en hiperplanos. Para probar esta última afirmación usamos los siguientes resultados.

Proposición 1.0.9 *Si a, b son elementos de un espacio ortogonal X de dimensión finita, tales que $\langle a, a \rangle = \langle b, b \rangle \neq 0$, entonces existe una transformación $u : X \to X$ reflexión en un hiperplano de X o composición de dos reflexiones en hiperplanos de X tal que $u(a) = b$.*

Demostración. Tenemos que $\langle a+b, a+b\rangle \neq 0$ ó $\langle a-b, a-b\rangle \neq 0$, pues de lo contrario, tendríamos que

$$\begin{aligned} 0 &= \langle a+b, a+b\rangle + \langle a-b, a-b\rangle \\ &= (\langle a,a\rangle + 2\langle a,b\rangle + \langle b,b\rangle) + (\langle a,a\rangle - 2\langle a,b\rangle + \langle b,b\rangle) \\ &= 2(\langle a,a\rangle + \langle b,b\rangle) = 4\langle a,a\rangle \end{aligned}$$

lo que contradice el hecho de que $\langle a,a\rangle \neq 0$.

Notamos que $(a-b) \perp (a+b)$, pues $\langle a+b, a-b\rangle = \langle a,a\rangle - \langle b,b\rangle = 0$. En el caso de que $\langle a-b, a-b\rangle \neq 0$, entonces es posible definir la reflexión en el hiperplano $\langle a-b\rangle^{\perp}$ dada por $\rho_{a-b}(t(a-b)+c) = -t(a-b)+c$ donde $c \perp (a-b)$. Así, como $a = \frac{1}{2}(a-b) + \frac{1}{2}(a+b)$

$$\rho_{a-b}(a) = -\frac{1}{2}(a-b) + \frac{1}{2}(a+b) = b.$$

En el otro caso, $\langle a+b, a+b\rangle \neq 0$ y entonces la reflexión en el hiperplano $\langle a+b\rangle^{\perp}$ dada por $\rho_{a+b}(t(a+b)+c) = -t(a+b)+c$ donde $c \perp (a+b)$ está bien definida y también lo está la reflexión en el hiperplano $\langle b\rangle^{\perp}$ dada por $\rho_b(tb+d) = -tb+d$ donde $d \perp b$. De este modo

$$\begin{aligned} \rho_b\rho_{a+b}(a) &= \rho_b\rho_{a+b}\left(\frac{1}{2}(a-b) + \frac{1}{2}(a+b)\right) \\ &= \rho_b\left(\frac{1}{2}(a-b) - \frac{1}{2}(a+b)\right) = \rho_b(-b) = b. \end{aligned}$$

□

Teorema 1.0.10 *Si X es un espacio ortogonal no degenerado de dimensión finita n, entonces cualquier transformación ortogonal puede expresarse como composición de a lo más $2n$ reflexiones en hiperplanos de X.*

Demostración. Sea $t : X \to X$ una transformación ortogonal. Para la demostración de este teorema procederemos por inducción sobre la dimensión de X.

Si $dim(X) = 1$, entonces $X = \langle x\rangle$. Como t es ortogonal y X es no degenerado, entonces $\langle t(x), t(x)\rangle = \langle x,x\rangle \neq 0$. Así, por la proposición anterior, existe $u : X \to X$ composición de a lo más 2 reflexiones en hiperplanos, tal que $u(x) = t(x)$. Esto implica que $t = u$ y por tanto se sigue la base de inducción.

Supongamos que el teorema es cierto para espacios ortogonales no degenerados de dimensión n.

Sea X un espacio ortogonal no degenerado de dimensión $n+1$. Podemos encontrar una base ortonormal de X, digamos $\beta = \{e_0, e_1, ..., e_n\}$.

Como $\langle t(e_n), t(e_n)\rangle = \langle e_n, e_n\rangle \neq 0$, por la proposición anterior, existe $u : X \to X$ composición de a lo más 2 reflexiones en hiperplanos, tal que $u(t(e_n)) = e_n$.

Consideramos $\beta' = \beta - \{e_n\}$ y la transformación ortogonal $ut : X \to X$ restringida a $X' = \langle \beta' \rangle$. Por hipótesis de inducción, tenemos que

$$ut|_{X'} = \rho_{a_1}\rho_{a_2}...\rho_{a_m}$$

donde $\forall i \in \{1, ..., m\}$ ρ_{a_i} es la reflexión en el hiperplano $\langle a_i \rangle^{\perp}$ y $m \leq 2n$.

Notamos que para cada $i \in \{1, ..., m\}$ existe W_i subespacio vectorial de X' tal que $X' = \langle a_i \rangle \oplus W_i$. Así, $\rho_{a_i}(ta_i + w_i) = -ta_i + w_i$ con $w_i \in W_i$.

Entonces tenemos que $X = X' \oplus \langle e_n \rangle = \langle a_i \rangle \oplus W_i \oplus \langle e_n \rangle$, por lo que podemos extender ρ_{a_i} a ρ'_{a_i} de la siguiente forma

$$\rho'_{a_i}(ta_i + w_i + se_n) = -ta_i + w_i + se_n.$$

De este modo $\rho'_{a_i}|_{X'} = \rho_{a_i}$ y $\rho'_{a_i}(e_n) = e_n$ y así

$$ut|_{X'} = \rho_{a_1}...\rho_{a_m} = \rho'_{a_1}|_{X'}...\rho'_{a_m}|_{X'} \text{ y } ut(e_n) = e_n = \rho'_{a_i}(e_n).$$

Por lo tanto

$$ut = \rho'_{a_1}...\rho'_{a_m}.$$

Como las reflexiones en hiperplanos son involuciones y como u es composición de a lo más dos de ellas, entonces se sigue que t es composición de a lo más $m+2$ reflexiones en hiperplanos con $m + 2 \leq 2n + 2 = 2dim(X)$ y con esto concluimos la inducción. □

Observamos que el espacio ortogonal $E^{n,p}$ es no degenerado. Esto sucede ya que si $x \in E^{n,p}$ es tal que $\forall v \in E^{n,p}$ $\langle x, v\rangle = 0$ entonces, en particular, se tiene que $\forall j \in \{1, ..., n, n+1, ..., n+p\}$

$$x_j = \langle x, i_j \rangle = 0,$$

donde $x = \Sigma_{j=1}^{n+p} x_j i_j$, es decir, $x = 0$ y en efecto $E^{n,p}$ es no degenerado.

En virtud del teorema anterior, podemos concluir que $O(n, p)$ está generado por reflexiones en hiperplanos.

Proposición 1.0.11 *Sea $a \in C^{n,p}$. Si $av = va'$ para todo $v \in E^{n,p}$, entonces $a \in \mathbb{R}$.*

Demostración. Sea $a \in C^{n,p}$ tal que $\forall v \in E^{n,p}$ $av = va'$. Primero notamos que para todo $i \in B$ y para cualquier $I = i_{j_1}...i_{j_r} \in \mathscr{B}$, tal que $i \notin \{i_{j_1}, ..., i_{j_r}\}$ se tiene que

$$iI = i(i_{j_1}...i_{j_r}) = (-1)^r(i_{j_1}...i_{j_r})i = I'i. \tag{1.3}$$

También notamos que a puede escribirse de manera única como

$$a = \sum_{j=1}^{s} a_j I_j + \sum_{j=s+1}^{2^{n+p}} a_j I_j,$$

donde $\forall j \in \{1, ..., s\}$ I_j contiene a i como factor y $\forall j \in \{s+1, ..., 2^{n+p}\}$ I_j no contiene a i como factor. Usando (1.3), se tiene que para $j \in \{1, ..., s\}$,

$$I_j = (i_{j_1}...i_{j_{k-1}})i(i_{j_{k+1}}...i_{j_r}) = (i_{j_1}...i_{j_{k-1}})(i_{j_{k+1}}...i_{j_r})'i.$$

Entonces factorizando i en cada término $a_j I_j$ con $j \in \{1, ..., s\}$, podemos escribir a a de manera única como $a = b + ci$, donde ningún término de b y c contiene a i como factor. Dado que

$$ai = (b + ci)i = bi + ci^2 = bi + i^2 c,$$

y por otra parte, usando (1.3) se sigue

$$ia' = i(b + ci)' = i(b' + c'i') = ib' + ic'(-i) = ib' - ic'i = bi - i(ic) = bi - i^2 c,$$

como $ai = ia'$, necesariamente $c = 0$, por tanto, $a = b$ y así, ningún término de a contiene a i como factor.

Aplicando el argumento anterior para cada $i \in B$, tenemos que ningún término de a contiene a un elemento de B como factor, es decir, $a \in \mathbb{R}$. □

Proposición 1.0.12 *La transformación $\rho : \Gamma^{n,p} \to O(n,p)$ tal que para $a \in \Gamma^{n,p}$ $\rho(a) = \rho_a$ es un epimorfismo de grupos. Además, $ker(\rho) = \mathbb{R} - \{0\}$.*

Demostración. Sean $a, b \in \Gamma^{n,p}$. La transformación $\rho_{ab} : E^{n,p} \to E^{n,p}$ es tal que para $v \in E^{n,p}$

$$\rho_{ab}(v) = (ab)v(ab)'^{-1} = (ab)v(a'b')^{-1}$$
$$= (ab)v(b'^{-1}a'^{-1}) = a(bvb'^{-1})a'^{-1} = \rho_a\rho_b(v).$$

De modo que $\rho(ab) = \rho_{ab} = \rho_a\rho_b = \rho(a)\rho(b)$, es decir, ρ es homomorfismo de grupos.

Sea $t \in O(n,p)$. Por la demostración del Teorema 1.0.10 se tiene que para algunas $v_1, ..., v_m \in E^{n,p}$ tales que $\forall j \in \{1, ..., m\}$ $q(v_j) \neq 0$ sucede que

$$t = \rho_{v_1}...\rho_{v_m}.$$

Inductivamente puede verse que $\rho_{v_1}...\rho_{v_m} = \rho_{v_1...v_m}$ y así, $t = \rho_{v_1...v_m}$. Por la Proposición 1.0.6 se tiene entonces que $\forall j \in \{1, ..., m\}$ $v_j \in \Gamma^{n,p}$ y como $\Gamma^{n,p}$ es un grupo se sigue que $v_1...v_m \in \Gamma^{n,p}$. Así, $\rho(v_1...v_m) = t$ y ρ es suprayectiva.

Además, por la Proposición 1.0.11 tenemos que

$$\begin{aligned} a \in ker(\rho) &\Leftrightarrow \rho(a) = \rho_a = Id_{E^{n,p}} \\ &\Leftrightarrow \forall v \in E^{n,p}\ \rho_a(v) = ava'^{-1} = v \\ &\Leftrightarrow \forall v \in E^{n,p}\ av = va' \\ &\Leftrightarrow a \in \mathbb{R} - \{0\}. \end{aligned}$$

□

Tenemos la sucesión exacta corta de grupos:

$$1 \hookrightarrow \mathbb{R} - \{0\} \hookrightarrow \Gamma^{n,p} \overset{\rho}{\twoheadrightarrow} O(n,p) \twoheadrightarrow 1.$$

Teorema 1.0.13 *Todo elemento de $\Gamma^{n,p}$ es producto de vectores invertibles en $E^{n,p}$.*

Demostración. Sea $a \in \Gamma^{n,p}$. Por la Proposición 1.0.5, sabemos que ρ_a es una transformación ortogonal de $E^{n,p}$, así, por el Teorema 1.0.10, es composición de reflexiones en hiperplanos de $E^{n,p}$ y podemos encontrar elementos invertibles $v_1, ..., v_r \in E^{n,p}$ tales que

$$\rho(a) = \rho_a = \rho_{v_1}...\rho_{v_r} = \rho_{v_1...v_m} = \rho(v_1...v_m),$$

de manera que

$$\rho(a(v_1...v_m)^{-1}) = \rho(a)\rho((v_1...v_m)^{-1}) = \rho(a)(\rho(v_1...v_m))^{-1} = Id_{E^{n,p}}.$$

Así, $a(v_1...v_m)^{-1} \in ker(\rho) = \mathbb{R} - \{0\}$ y por tanto existe $t \in \mathbb{R} - \{0\}$ tal que $a(v_1...v_m)^{-1} = t$, es decir, $a = tv_1...v_m$. □

Corolario 1.0.14 $\Gamma^{n,p} = \Gamma^{n,p}_{par} \cup \Gamma^{n,p}_{impar}$ *(unión disjunta).*

Demostración. Sea $a \in \Gamma^{n,p}$ y sea $a = v_1...v_r$ su descomposición como producto de vectores invertibles en $E^{n,p}$. Como cada vector v_j se descompone como suma de términos con palabras de longitud 1, entonces todos los términos del producto $v_1...v_r$ contienen palabras de longitud r, o si hay cancelaciones, la paridad sigue siendo la misma que r, es decir, $a \in \Gamma^{n,p}_{par}$ si r es par y $a \in \Gamma^{n,p}_{impar}$ si r es impar. □

Proposición 1.0.15 *Toda reflexión en un hiperplano de un espacio ortogonal de dimensión finita X invierte la orientación.*

Demostración. Sea $x \in X$ tal que $\langle x, x\rangle \neq 0$ y ρ_x la reflexión de X en el hiperplano $\langle x\rangle^{\perp}$. Sea $B_1 = \{e_1, ..., e_n\}$ una base de X. Como $\langle x\rangle$ es no degenerado, por la Proposición 1.0.7, se tiene que $X = \langle x\rangle \oplus \langle x\rangle^{\perp}$ y si $\{x_1, ..., x_{n-1}\}$ es base de $\langle x\rangle^{\perp}$ entonces $B_2 = \{x_1, ...x_{n-1}, x\}$ es base de X.

La matriz asociada a ρ_x con respecto a la base $B_2 = \{x_1, ..., x_{n-1}, x\}$ es la matriz cuadrada dada por

$$A = \begin{pmatrix} 1 & & & 0 \\ & \cdot & & \\ & & 1 & \\ 0 & & & -1 \end{pmatrix},$$

por lo que $det(A) = -1$.

Ahora, si M es la matriz de cambio de base de B_1 en B_2, es decir, cuyas columnas son las coordenadas de los elementos de la base B_1 con respecto de la base B_2, entonces se tiene que la matriz asociada a ρ_x con respecto a la base $B_1 = \{e_1, ..., e_n\}$ es

$$M^{-1}AM,$$

y además $det(M^{-1}AM) = det(M^{-1})det(A)det(M) = det(A) = -1$, por lo que ρ_x invierte la orientación. □

Como las reflexiones en hiperplanos invierten la orientación, entonces cualquier transformación ortogonal $u \in O(n, p)$ preserva la orientación si y sólo si u es composición par de reflexiones en hiperplanos y, como se vio en la demostración del Teorema 1.0.13, esto ocurre si y sólo si u es la imagen

bajo ρ de un elemento $a \in \Gamma^{n,p}$ tal que a es producto de una cantidad par de vectores invertibles. Ahora, por la demostración del Corolario 1.0.14, esto último ocurre si y sólo si $a \in \Gamma^{n,p}_{par}$.

De las observaciones anteriores podemos concluir que

$$\rho^{-1}(SO(n,p)) = \Gamma^{n,p}_{par}$$

y tenemos la sucesión exacta corta de grupos:

$$1 \hookrightarrow \mathbb{R} - \{0\} \hookrightarrow \Gamma^{n,p}_{par} \overset{\rho}{\twoheadrightarrow} SO(n,p) \twoheadrightarrow 1.$$

Corolario 1.0.16 *$\Gamma^{n,p}$ es cerrado con respecto a la involución principal, la reversión y la conjugación.*

Demostración. Sea $a = v_1...v_r \in \Gamma^{n,p}$ con $v_1, ..., v_r$ elementos invertibles de $E^{n,p}$. Entonces debido a las propiedades de las tres transformaciones y recordando la Proposición 1.0.6 se tiene que

$$\begin{aligned} a' = (v_1...v_r)' = v_1'...v_r' = (-1)^r v_1...v_r = (-1)^r a \in \Gamma^{n,p}, \\ a^* = (v_1...v_r)^* = v_r^*...v_1^* = v_r...v_1 \in \Gamma^{n,p}, \\ a^- = (v_1...v_r)^- = v_r^-...v_1^- = (-1)^r v_r...v_1 \in \Gamma^{n,p}. \end{aligned}$$

□

Definición 5 *Definimos la transformación $N : C^{n,p} \to C^{n,p}$ tal que para $a \in C^{n,p}$ se tiene que $N(a) = a^- a$.*

Proposición 1.0.17 *Si $a \in \Gamma^{n,p}$, entonces $N(a) \in \mathbb{R} - \{0\}$. Más aún, N es un homomorfismo de $\Gamma^{n,p}$ al grupo multiplicativo $\mathbb{R} - \{0\}$.*

Demostración. Sea $a = v_1...v_r \in \Gamma^{n,p}$ con $v_1, ..., v_r \in E^{n,p}$ invertibles. Primero notamos que si $v \in E^{n,p}$ es invertible, como todas las palabras que conforman sus términos son de longitud 1, se tiene que $v^- = -v$, por lo que $N(v) = v^- v = -v^2 = -q(v) \neq 0$. Así, recordando que la transformación $a \to a^-$ es antiautomorfismo, se tiene que

$$\begin{aligned} N(a) &= a^- a = (v_1...v_r)^-(v_1...v_r) \\ &= v_r^-...v_1^- v_1...v_r = N(v_1)...N(v_r) \\ &= (-1)^r q(v_1)...q(v_r) \in \mathbb{R} - \{0\}. \end{aligned}$$

Ahora, si $a, b \in \Gamma^{n,p}$, entonces $N(ab) = (ab)^- ab = b^- a^- ab = N(a)N(b)$ y la transformación N es homomorfismo de grupos. □

Proposición 1.0.18 *Para $a \in \Gamma^{n,p}$, se tiene que $|N(a)| \leq |a|^2$. La igualdad se alcanza si $p = 0$.*

Demostración. Sea $a \in \Gamma^{n,p}$. Recordamos que a puede expresarse de la forma $a = \Sigma a_I I$ y entonces tenemos que

$$|N(a)| = |a^- a| = |(\Sigma a_I I^-)(\Sigma a_I I)| = |\Sigma a_I^2 I^- I| = |\Sigma \pm a_I^2| \leq \Sigma a_I^2 = |a|^2.$$

La tercera igualdad se tiene recordando que $N(a) \in \mathbb{R}$ para $a \in \Gamma^{n,p}$, pues al hacer la multiplicación, si $I_j^- I_k \notin \mathbb{R}$, necesariamente el término $(a_j I_j^-)(a_k I_k)$ es 0 o se cancela con otro término. En caso de que $I_j^- I_k \in \mathbb{R}$, entonces $I_j = \pm I_k$, pero debido a que la expresión de a como combinación lineal de elementos en $\mathscr{B}$ es única, necesariamente $I_j = I_k$.

La cuarta igualdad se tiene ya que

$$I^- I = (i_{j_1}...i_{j_r})^-(i_{j_1}...i_{j_r}) = (-1)^r(i_{j_r}...i_{j_1})(i_{j_1}...i_{j_r}) = (-1)^r i_{j_1}^2...i_{j_r}^2 = \pm 1.$$

Si $a \in \Gamma^{n,0}$, la igualdad se da ya que $\forall I = i_{j_1}...i_{j_r} \in \mathscr{B}$, se tiene que

$$\begin{aligned} I^- I = (i_{j_1}...i_{j_r})^-(i_{j_1}...i_{j_r}) &= (-1)^r(i_{j_r}...i_{j_1})(i_{j_1}...i_{j_r}) \\ &= (-1)^r i_{j_1}^2...i_{j_r}^2 = (-1)^{2r} = 1. \end{aligned}$$

□

Definición 6 *Definimos*

$$\begin{aligned} Pin(n,p) &= \{a \in \Gamma^{n,p} | N(a) = \pm 1\}, \\ Spin(n,p) &= \{a \in \Gamma_{par}^{n,p} | N(a) = \pm 1\}. \end{aligned}$$

Para $a \in \Gamma^{n,p}$, tenemos que $b = |N(a)|^{-\frac{1}{2}} a \in Pin(n,p)$ ya que

$$N(b) = N(|N(a)|^{-\frac{1}{2}} a) = (|N(a)|^{-\frac{1}{2}} a)^-(|N(a)|^{-\frac{1}{2}} a) = |N(a)|^{-1} N(a) = \pm 1.$$

Además, para $v \in E^{n,p}$ se tiene que

$$\rho_b(v) = (|N(a)|^{-\frac{1}{2}} a) v ((|N(a)|^{-\frac{1}{2}} a)')^{-1} = a v (a')^{-1} = \rho_a(v),$$

por lo que $\rho|_{Pin(n,p)}$ sigue siendo suprayectiva. Recordando la Proposición 1.0.12, tenemos que $ker(\rho) = \mathbb{R} - \{0\}$, por lo que $ker(\rho|_{Pin(n,p)}) = \{\pm 1\}$ y entonces se tienen las siguientes sucesiones exactas cortas de grupos:

$$1 \hookrightarrow \{\pm 1\} \hookrightarrow Pin(n,p) \overset{\rho}{\twoheadrightarrow} O(n,p) \twoheadrightarrow 1,$$
$$1 \hookrightarrow \{\pm 1\} \hookrightarrow Spin(n,p) \overset{\rho}{\twoheadrightarrow} SO(n,p) \twoheadrightarrow 1.$$

De la manera natural, consideramos a $E^{n,p-1}$ y $E^{n-1,p}$ como subespacios de $E^{n,p}$. Así, consideramos también a $C^{n,p-1}$ y $C^{n-1,p}$ como subespacios de $C^{n,p}$ (generados por las palabras que no contienen al vector correspondiente).

Proposición 1.0.19

$$i)\ \ \Gamma^{n,p} \cap C^{n,p-1} = \Gamma^{n,p-1},$$
$$ii)\ \Gamma^{n,p} \cap C^{n-1,p} = \Gamma^{n-1,p}.$$

Demostración. i) Sea $a \in \Gamma^{n,p} \cap C^{n,p-1}$. Como $(N(a))^{-1}a^{-}a = 1$, entonces $a^{-1} = (N(a))^{-1}a^{-} \in C^{n,p-1}$, es decir a es invertible en $C^{n,p-1}$.

Además, dada $v \in E^{n,p-1} \subseteq E^{n,p}$, como $a \in \Gamma^{n,p}$, entonces sucede que

$$av(a')^{-1} \in E^{n,p} \cap C^{n,p-1} = E^{n,p-1}.$$

Por tanto, $a \in \Gamma^{n,p-1}$.

Ahora, sea $a \in \Gamma^{n,p-1}$. Dada $v = u + ti_{n+p} \in E^{n,p}$ con $u \in E^{n,p-1}$, $t \in \mathbb{R}$, tenemos que

$$\begin{aligned} av(a')^{-1} &= a(u + ti_{n+p})(a')^{-1} = au(a')^{-1} + a(ti_{n+p})(a')^{-1} \\ &= au(a')^{-1} + ti_{n+p}a'(a')^{-1} = au(a')^{-1} + ti_{n+p} \in E^{n,p}, \end{aligned}$$

donde la penúltima igualdad se sigue ya que si $I \in \mathscr{B}$ es tal que no contiene como factor a i_{n+p}, entonces

$$Ii_{n+p} = i_{j_1}...i_{j_r}i_{n+p} = (-1)^r i_{n+p}i_{j_1}...i_{j_r} = i_{n+p}I'$$

y por tanto, si $a = \Sigma a_I I$ tenemos que

$$ai_{n+p} = \Sigma a_I I i_{n+p} = \Sigma a_I i_{n+p} I' = i_{n+p}a'.$$

Por tanto $a \in \Gamma^{n,p}$ y esto prueba la parte i).

ii) Sea $a \in \Gamma^{n,p} \cap C^{n-1,p}$. Entonces $a^{-1} = (N(a))^{-1}a^- \in C^{n-1,p}$ y por tanto a es invertible en $C^{n-1,p}$. Además, para $v \in E^{n-1,p} \subset E^{n,p}$, sucede que

$$av(a')^{-1} \in E^{n,p} \cap C^{n-1,p} = E^{n-1,p}.$$

Por lo tanto $a \in \Gamma^{n-1,p}$.

Ahora, sea $a \in \Gamma^{n-1,p}$. Dada $v = u + ti_n \in E^{n,p}$ con $u \in E^{n-1,p}$, $t \in \mathbb{R}$, por el mismo argumento que en i), tenemos que

$$\begin{aligned} av(a')^{-1} &= a(u + ti_n)(a')^{-1} = au(a')^{-1} + a(ti_n)(a')^{-1} \\ &= au(a')^{-1} + ti_n a'(a')^{-1} = au(a')^{-1} + ti_n \in E^{n,p}. \end{aligned}$$

Por tanto $a \in \Gamma^{n,p}$ y esto prueba la parte ii). □

Proposición 1.0.20 *Supongamos que $a \in \Gamma^{n,p}$. Entonces*

$$\begin{aligned} &i)\ \ aa^* = a^*a \in \mathbb{R} - \{0\},\ \ y \\ &ii)\ \forall v \in E^{n,p},\ ava^* \in E^{n,p}. \end{aligned}$$

Demostración. i) Recordamos que la transformación $a \to a^*$ es antiautomorfismo de $C^{n,p}$ y que al aplicar esta transformación, $I \in \mathscr{B}$ cambia de signo si y sólo si $l(I) \equiv 2 \ mod(4)$ ó $l(I) \equiv 3 \ mod(4)$. Sea $a = v_1...v_r \in \Gamma^{n,p}$, con $v_1, ..., v_r \in E^{n,p}$ elementos invertibles. Entonces

$$aa^* = (v_1...v_r)(v_r^*...v_1^*) = (v_1...v_r)(v_r...v_1) = v_1^2...v_r^2 = q(v_1)...q(v_r) \in \mathbb{R} - \{0\}.$$

También, $a^*a = (v_r^*...v_1^*)(v_1...v_r) = (v_r...v_1)(v_1...v_r) = q(v_1)...q(v_r)$ y por tanto $aa^* = a^*a \in \mathbb{R} - \{0\}$, lo que demuestra la parte i).

ii) Sea $v \in E^{n,p}$. Sea $a = v_1...v_r \in \Gamma^{n,p}$, con $v_1, ..., v_r \in E^{n,p}$ elementos invertibles. Tenemos que $ava^* = (v_1...v_r)v(v_r...v_1)$, sin embargo, notamos que por la Proposición 1.0.6, se tiene que $\forall j \in \{1, ..., r\}$, $v_j \in \Gamma^{n,p}$ y entonces para cualquier $u \in E^{n,p}$, se tiene que

$$\left(\frac{-1}{q(v_j)}\right) v_j u v_j = v_j u \left(\frac{-v_j}{q(v_j)}\right) = v_j u(-v_j)^{-1} = v_j u(v_j')^{-1} \in E^{n,p},$$

por lo que $v_j u v_j \in E^{n,p}$. De este modo, como $u \in E^{n,p}$ era arbitraria, iterando este proceso podemos concluir que $ava^* = v_1...(v_r v v_r)...v_1 \in E^{n,p}$. □

Proposición 1.0.21 *Supongamos que $a \in \Gamma^{n,p}$. Entonces para $v \in E^{n,p}$ se tiene que $ava^{-1} \in E^{n,p}$.*

Demostración. Sea $v \in E^{n,p}$. Sea $a = v_1...v_r \in \Gamma^{n,p}$, con $v_1, ..., v_r \in E^{n,p}$ elementos invertibles. Por la Proposición 1.0.6 $\forall j \in \{1, ..., r\}$, $v_j \in \Gamma^{n,p}$ entonces para cualquier $u \in E^{n,p}$, se tiene que

$$v_j u v_j^{-1} = -v_j u(-v_j)^{-1} = -v_j u(v_j')^{-1} \in E^{n,p}.$$

Por tanto, como $a^{-1} = v_r^{-1}...v_1^{-1}$ y como $u \in E^{n,p}$ era arbitraria, iterando este proceso concluimos que

$$ava^{-1} = (v_1...v_r)v(v_r^{-1}...v_1^{-1}) = v_1...(v_r v v_r^{-1})...v_1^{-1} \in E^{n,p}.$$

□

Capítulo 2

Invariantes por Conjugación

Lema 2.0.1 *Si $a \in C^{n,p}$, entonces para cualesquiera $\alpha \in \Gamma^{n,p}$, $k \in \mathbb{N} \cup \{0\}$, se tiene que*

$$(\alpha a \alpha^{-1})^{(k)} = \alpha a^{(k)} \alpha^{-1}.$$

Demostración. Sea $v \in E^{n,p}$ tal que $N(v) \neq 0$, probaremos primero que

$$v a^{(k)} v^{-1} \in C^{n,p\,(k)}.$$

Sea $b = v a^{(k)} v^{-1}$. Como los términos de $a^{(k)}$ y v contienen palabras de longitud k y 1, respectivamente, entonces tenemos que

$$b \in C^{n,p\,(k-2)} \oplus C^{n,p\,(k-1)} \oplus C^{n,p\,(k)} \oplus C^{n,p\,(k+1)} \oplus C^{n,p\,(k+2)}.$$

Esto implica que $b = b^{(k-2)} + b^{(k-1)} + b^{(k)} + b^{(k+1)} + b^{(k+2)}$ y por tanto,

$$b' = (-1)^k (b^{(k-2)} - b^{(k-1)} + b^{(k)} - b^{(k+1)} + b^{(k+2)}). \tag{2.1}$$

Por otra parte,

$$\begin{aligned} b' &= (v a^{(k)} v^{-1})' = v'(a^{(k)})'(v^{-1})' \\ &= (-v)(-1)^k a^{(k)}(-v^{-1}) \\ &= (-1)^k v a^{(k)} v^{-1} = (-1)^k b \\ &= (-1)^k (b^{(k-2)} + b^{(k-1)} + b^{(k)} + b^{(k+1)} + b^{(k+2)}). \end{aligned}$$

Por esto y por (2.1) tenemos que $b^{(k-1)} = b^{(k+1)} = 0$, de manera que

$$b^- = (-1)^{\frac{(k-2)(k-1)}{2}} b^{(k-2)} + (-1)^{\frac{k(k+1)}{2}} b^{(k)} + (-1)^{\frac{(k+2)(k+3)}{2}} b^{(k+2)}.$$

Notamos que

$$\frac{(k-2)(k-1)}{2} = \frac{k^2 - 3k + 2}{2} = \frac{k(k+1) - 4k + 2}{2}$$

y que

$$\frac{(k+2)(k+3)}{2} = \frac{k^2 + 5k + 6}{2} = \frac{k(k+1) + 4(k+1) + 2}{2}$$

y así,

$$(-1)^{\frac{(k-2)(k-1)}{2}} = -(-1)^{\frac{k(k+1)}{2}} = (-1)^{\frac{(k+2)(k+3)}{2}},$$

de donde obtenemos que

$$b^- = (-1)^{\frac{k(k+1)}{2}}(-b^{(k-2)} + b^{(k)} - b^{(k+2)}). \tag{2.2}$$

Sin embargo, también tenemos que

$$\begin{aligned} b^- &= (va^{(k)}v^{-1})^- = (v^{-1})^-(a^{(k)})^- v^- = ((N(v))^{-1}v^-)^-((-1)^{\frac{k(k+1)}{2}} a^{(k)})v^- \\ &= (-1)^{\frac{k(k+1)}{2}} va^k((N(v))^{-1}v^-) = (-1)^{\frac{k(k+1)}{2}} va^k v^{-1} = (-1)^{\frac{k(k+1)}{2}} b \\ &= (-1)^{\frac{k(k+1)}{2}}(b^{(k-2)} + b^{(k)} + b^{(k+2)}), \end{aligned}$$

de donde, por (2.2), tenemos que $b^{(k-2)} = b^{(k+2)} = 0$ y esto implica que $b = b^{(k)} \in C^{n,p}$.

De lo anterior, podemos concluir que para toda $k \in \mathbb{N} \cup \{0\}$, se tiene que $va^{(k)}v^{-1} \in C^{n,p\,(k)}$.

Ahora tenemos que

$$vav^{-1} = v\left(\sum_{k=0}^{n+p} a^{(k)}\right) v^{-1} = \sum_{k=0}^{n+p} va^{(k)}v^{-1},$$

donde $va^{(k)}v^{-1} \in C^{n,p\,(k)}$ y por lo tanto $(vav^{-1})^{(k)} = va^{(k)}v^{-1}$.

Finalmente, aplicando varias veces el argumento anterior, se tiene que para $\alpha = v_1...v_r \in \Gamma^{n,p}$ con $v_1, ..., v_r \in E^{n,p}$ vectores invertibles, obtenemos

$$\begin{aligned}(\alpha a \alpha^{-1})^{(k)} &= (v_1...v_r a v_r^{-1}...v_1^{-1})^{(k)} = v_1(v_2...v_r a v_r^{-1}...v_2^{-1})^{(k)} v_1^{-1} \\ &= v_1...(v_r a v_r^{-1})^{(k)}...v_1^{-1} = v_1...(v_r a^{(k)} v_r^{-1})...v_1^{-1} \\ &= \alpha a^{(k)} \alpha^{-1}.\end{aligned}$$

□

Corolario 2.0.2 *Para cualesquiera $a \in C^{n,p}$ y $\alpha \in \Gamma^{n,p}$, se tiene que*

$$(\alpha a \alpha^{-1})^{(0)} = a^{(0)}.$$

Si $n+p$ es impar, entonces

$$(\alpha a \alpha^{-1})^{(n+p)} = a^{(n+p)}.$$

Demostración. Por el lema anterior, para $a \in C^{n,p}$ y $\alpha \in \Gamma^{n,p}$, como $a^{(0)} \in \mathbb{R}$, tenemos que

$$(\alpha a \alpha^{-1})^{(0)} = \alpha a^{(0)} \alpha^{-1} = a^{(0)} \alpha \alpha^{-1} = a^{(0)}.$$

Ahora, supongamos que $n+p$ es impar, entonces por el lema anterior

$$(\alpha a \alpha^{-1})^{(n+p)} = \alpha a^{(n+p)} \alpha^{-1}.$$

Como la única palabra de longitud $n+p$ es $i_1...i_{n+p}$, tenemos que para algún $t \in \mathbb{R}$, $a^{(n+p)}$ es de la forma

$$a^{(n+p)} = t(i_1...i_{n+p}). \tag{2.3}$$

Notemos que para $j \in \{1, ..., n+p\}$, se tiene que

$$i_j(i_1...i_{n+p}) = (-1)^{j-1} i_1...i_{j-1} i_j^2 i_{j+1}...i_{n+p}.$$

Por otra parte, tomando en cuenta que $(n+p)$ es impar, tenemos que

$$(i_1...i_{n+p})i_j = (-1)^{(n+p)-j} i_1...i_{j-1} i_j^2 i_{j+1}...i_{n+p} = (-1)^{1-j} i_1...i_{j-1} i_j^2 i_{j+1}...i_{n+p}.$$

Como $(-1)^{j-1} = (-1)^{1-j}$, podemos concluir que

$$i_j(i_1...i_{n+p}) = (i_1...i_{n+p})i_j.$$

Repitiendo varias veces lo anterior, para $I = i_{j_1}...i_{j_r} \in \mathscr{B}$ obtenemos que

$$\begin{aligned} I(i_1...i_{n+p}) &= (i_{j_1}...i_{j_r})(i_1...i_{n+p}) = (i_{j_1}...i_{j_r-1})i_{j_r}(i_1...i_{n+p}) \\ &= (i_{j_1}...i_{j_{r-1}})(i_1...i_{n+p})i_{j_r} = ... = (i_1...i_{n+p})(i_{j_1}...i_{j_r}) \\ &= (i_1...i_{n+p})I. \end{aligned}$$

De manera que si $\alpha = \sum \alpha_I I$, usando 2.3 tenemos que

$$\begin{aligned} \alpha a^{(n+p)} = \left(\sum \alpha_I I\right) a^{(n+p)} = \sum t\alpha_I I(i_1...i_{n+p}) \\ = \sum t\alpha_I (i_1...i_{n+p})I = a^{(n+p)} \left(\sum \alpha_I I\right) = a^{(n+p)}\alpha. \end{aligned}$$

Finalmente, por lo anterior se tiene que

$$(\alpha a \alpha^{-1})^{(n+p)} = \alpha a^{(n+p)} \alpha^{-1} = a^{(n+p)} \alpha\alpha^{-1} = a^{(n+p)}.$$

□

Definición 7 *Para cualquier entero k y cualquier $a \in C^{n,p}$, definimos*

$$T_k(a) = ((a^{(k)})^- a^{(k)})^{(0)}.$$

Aunque definimos $T_k(a)$ para cualquier entero k, notamos que si $k < 0$ ó $k > n + p$, entonces $T_k(a) = 0$ para toda $a \in C^{n,p}$ ya que $a^{(k)} = 0$.

Teorema 2.0.3 *Dados un entero k, $a \in C^{n,p}$ y $\alpha \in \Gamma^{n,p}$, se tiene que*

$$T_k(\alpha a \alpha^{-1}) = T_k(a).$$

Demostración. Usando el Lema 2.0.1 y recordando que para $\alpha \in \Gamma^{n,p}$, $N(\alpha) = \alpha^{-}\alpha \in \mathbb{R} - \{0\}$ y $\alpha^{-1} = (N(\alpha))^{-1}\alpha^{-}$, tenemos que

$$\begin{aligned}
T_k(\alpha a \alpha^{-1}) &= (((\alpha a \alpha^{-1})^{(k)})^{-}(\alpha a \alpha^{-1})^{(k)})^{(0)} \\
&= ((\alpha a^{(k)} \alpha^{-1})^{-}(\alpha a^{(k)} \alpha^{-1}))^{(0)} \\
&= (N(\alpha))^{-1}((\alpha a^{(k)} \alpha^{-}))^{-}(\alpha a^{(k)} \alpha^{-1}))^{(0)} \\
&= (N(\alpha))^{-1}(\alpha (a^{(k)})^{-}(\alpha^{-}\alpha) a^{(k)} \alpha^{-1})^{(0)} \\
&= (\alpha (a^{(k)})^{-} a^{(k)} \alpha^{-1})^{(0)} \\
&= \alpha ((a^{(k)})^{-} a^{(k)})^{(0)} \alpha^{-1} \\
&= ((a^{(k)})^{-} a^{(k)})^{(0)} \\
&= T_k(a).
\end{aligned}$$

□

Recordamos que $\rho|_{Pin(n,p)}$ es epimorfismo, es decir, para $\xi \in O(n,p)$, existe $a \in Pin(n,p)$ tal que $\rho(a) = \rho_a = \xi$. Además, si $b \in Pin(n,p)$, tenemos que

$$\rho(a) = \rho(b) \Longleftrightarrow ab^{-1} \in ker(\rho|_{Pin(n,p)}) = \{\pm 1\} \Longleftrightarrow b = \pm a,$$

por lo que los únicos elementos en $Pin(n,p)$ tales que bajo ρ van a dar a ξ son $\pm a$.

También notamos que para cualquier $a \in Pin(n,p)$ y $k \in \mathbb{Z}$, tenemos que

$$\begin{aligned}
T_k(-a) &= (((-a)^{(k)})^{-}(-a)^{(k)})^{(0)} \\
&= ((-a^{(k)})^{-}(-a^{(k)}))^{(0)} \\
&= ((a^{(k)})^{-}(a^{(k)}))^{(0)} = T_k(a).
\end{aligned}$$

Debido a estas observaciones, es posible dar la siguiente definición.

Definición 8 *Para $\xi \in O(n,p)$ definimos*

$$T_k(\xi) = T_k(a),$$

donde $a \in Pin(n,p)$ es tal que $\rho_a = \xi$.

Proposición 2.0.4 *Para cualesquiera $\xi, \eta \in O(n,p)$ y $k \in \mathbb{Z}$ se tiene que*

$$T_k(\eta\xi\eta^{-1}) = T_k(\xi).$$

Demostración. Sean $\xi, \eta \in O(n,p)$. Tomamos $a, b \in Pin(n,p)$ tales que

$$\rho_a = \xi,\ \rho_b = \eta.$$

Entonces

$$\eta\xi\eta^{-1} = \rho_b\rho_a(\rho_b)^{-1} = \rho(b)\rho(a)(\rho(b))^{-1} = \rho(bab^{-1}) = \rho_{bab^{-1}}.$$

Así, por el Teorema 2.0.3 se tiene que

$$T_k(\eta\xi\eta^{-1}) = T_k(bab^{-1}) = T_k(a) = T_k(\xi).$$

□

Proposición 2.0.5 *Si $a \in \Gamma^{n,p}$, entonces*

$$\sum_{k=0}^{n+p} T_k(a) = N(a).$$

Demostración. Sea $a = \sum_{k=0}^{n+p} a^{(k)} \in \Gamma^{n,p}$. Recordamos que $N(a) \in \mathbb{R}-\{0\}$, es decir, $N(a) = (N(a))^{(0)}$ y entonces

$$N(a) = a^- a = \left(\left(\sum_{k=0}^{n+p}(a^{(k)})^-\right)\left(\sum_{j=0}^{n+p} a^{(j)}\right)\right)^{(0)}$$
$$= \sum_{k,j=0}^{n+p}((a^{(k)})^- a^{(j)})^{(0)} = \sum_{k=0}^{n+p}((a^{(k)})^- a^{(k)})^{(0)} = \sum_{k=0}^{n+p} T_k(a),$$

donde la penúltima igualdad se tiene ya que si $j, k \in \{0, 1, ..., n+p\}$ y si $I_j, I_k \in \mathscr{B}$ son tales que $l(I_j) = j$ y $l(I_k) = k$, entonces

$$I_j I_k \in \mathbb{R} \iff I_j = \pm I_k \text{ ó } j = k = 0 \implies j = k.$$

Equivalentemente, si $j \neq k$ necesariamente $I_j I_k \notin \mathbb{R}$, lo que prueba que $((a^{(k)})^- a^{(j)})^{(0)} = 0$. □

Capítulo 3

Matrices de Clifford y Transformaciones de Möbius

Denotaremos a $E^{n,0}$, $C^{n,0}$ y $\Gamma^{n,0}$, como E^n, C^n y Γ^n, respectivamente. También escribiremos

$$\overline{\Gamma}^n = \Gamma^n \cup \{0\}.$$

Lema 3.0.1 *Dado $v \in E^n$ se tiene que $v \neq 0$ si y sólo si v es invertible.*

Demostración. Si expresamos a v de la forma

$$v = \sum_{j=1}^{n} \alpha_j i_j, \text{ donde } \forall j \in \{1, ..., n\},\ \alpha_j \in \mathbb{R},$$

entonces

$$q(v) = -\sum_{j=1}^{n} \alpha_j^2 = 0 \Longleftrightarrow \forall j \in \{1, ..., n\},\ \alpha_j = 0 \Longleftrightarrow v = 0,$$

por lo que $v \neq 0 \Longleftrightarrow v^2 = q(v) \neq 0 \Longleftrightarrow v^{-1} = \dfrac{v}{q(v)}$. □

Lema 3.0.2 *Sea $a \in C^{n,p}$ tal que $a \neq 0$. Si a es invertible entonces a no es divisor de cero.*

Demostración. Sea $a \in C^{n,p}$ tal que $a \neq 0$. Supongamos que a es invertible y que es divisor de cero, entonces existe $b \in C^{n,p}$ con $b \neq 0$ tal que $ab = 0$.

Por otra parte, tenemos que $b = (a^{-1}a)b = a^{-1}(ab) = 0$ en contradicción con que $b \neq 0$. De manera que si a es invertible entonces no es divisor de cero. □

Lema 3.0.3 *Supongamos que $a, b \in \overline{\Gamma}^n$. Entonces $ab^* \in E^n$ si y sólo si $b^*a \in E^n$.*

Demostración. Sean $a, b \in \overline{\Gamma}^n$. Si $b = 0$, entonces el resultado es claro pues $ab^* = b^*a = 0 \in E^n$, por lo que podemos asumir que $b \neq 0$. Es útil recordar el Corolario 1.0.16 pues esto implica que $a^*, b^* \in \overline{\Gamma}^n$.

Supongamos que $ab^* \in E^n$. Por la Proposición 1.0.21, se tiene que

$$b^*a = b^*a(b^*(b^*)^{-1}) = b^*(ab^*)(b^*)^{-1} \in E^n.$$

Recíprocamente, si $b^*a \in E^n$, notamos que $b^*a = b^*(a^*)^*$ y aplicando lo anterior tenemos que $(a^*)^*b^* \in E^n$ y por tanto $ab^* = (a^*)^*b^* \in E^n$. □

Proposición 3.0.4 *Supongamos que $b, c \in C^{n-1}$ (es decir, las palabras que conforman los términos de b y c no contienen al vector i_n) . Entonces*

$$a = b + ci_n \in \overline{\Gamma}^n \quad \textit{si y sólo si} \quad b, c \in \overline{\Gamma}^{n-1} \textit{ y } bc^* \in E^{n-1}.$$

Demostración. Sean $b, c \in C^{n-1}$. Probamos primero la necesidad. Supongamos que $a = b + ci_n \in \overline{\Gamma}^n$. Si $b = 0$ ó $c = 0$ entonces $bc^* = 0 \in E^{n-1}$. También, si $b = c = 0$, $a = b + ci_n = 0 \in \overline{\Gamma}^{n-1}$.

Supongamos $b = 0$. Por hipótesis $ci_n = a \in \overline{\Gamma}^n$, pero si $c \neq 0$ entonces recordando que Γ^n es grupo y que $i_n \in \Gamma^n$, tenemos que $c = (ci_n)(i_n^{-1}) \in \Gamma^n$, por lo que $c \in \Gamma^n \cap C^{n-1}$. Por la Proposición 1.0.19, $\Gamma^n \cap C^{n-1} = \Gamma^{n-1}$ y entonces $b, c \in \overline{\Gamma}^{n-1}$.

Supongamos $c = 0$. Por hipótesis $b = a \in \overline{\Gamma}^n$, pero si $b \neq 0$ entonces $b \in \Gamma^n \cap C^{n-1} = \Gamma^{n-1}$, por lo que $b, c \in \overline{\Gamma}^{n-1}$.

Ahora suponemos que $b, c \neq 0$, entonces $a \neq 0$, por lo que $a \in \Gamma^n$ y es útil recordar que por la Proposición 1.0.17 tenemos que $N(a) = aa^- \in \mathbb{R} - \{0\}$.

Notamos que si I es una palabra que no tiene a i_n como factor, entonces $i_nI = (-1)^{l(I)}Ii_n = I'i_n$. De manera que por la linealidad de la involución principal, tenemos que

$$\forall d \in C^{n-1}, \;\; i_nd = d'i_n. \tag{3.1}$$

Usando la observación anterior tenemos que

$$\begin{aligned} aa^- &= (b + ci_n)(b + ci_n)^- = (b + ci_n)(b^- - i_nc^-) \\ &= bb^- - bi_nc^- + ci_nb^- - ci_n^2c^- = bb^- + cc^- - b(c^-)'i_n + c(b^-)'i_n \\ &= bb^- + cc^- - bc^*i_n + cb^*i_n = bb^- + cc^- + (cb^* - bc^*)i_n \in \mathbb{R} - \{0\}. \end{aligned}$$

Esto implica que $cb^* - bc^* = 0$ o equivalentemente,

$$cb^* = bc^* \tag{3.2}$$

pues de otra forma, como $bb^- + cc^- \in C^{n-1}$, entonces $aa^- \in \mathbb{R} - \{0\}$ tendría términos con palabras que contienen a i_n como factor. Observamos que esto implica que $bb^- + cc^- \in \mathbb{R} - \{0\}$.

Por la Proposición 1.0.20 *ii*), se tiene que $ai_na^* \in E^n$ y usando (3.1)

$$\begin{aligned} ai_na^* &= (b + ci_n)i_n(b + ci_n)^* = (b + ci_n)i_n(b^* + i_n^*c^*) \\ &= bi_nb^* + bi_ni_n^*c^* + ci_n^2b^* + ci_n^2i_n^*c^* \\ &= b(b^*)'i_n + bi_n^2c^* - cb^* - ci_nc^* \\ &= bb^-i_n - bc^* - cb^* - c(c^*)'i_n \\ &= -bc^* - cb^* + (bb^- - cc^-)i_n \in E^n. \end{aligned}$$

Esto implica que $bb^- - cc^- \in \mathbb{R}$, pues de otra forma, $ai_na^* \in E^n$ tendría términos con palabras de longitud al menos 2 y que contienen a i_n como factor. Entonces $(bb^- - cc^-)i_n \in E^n$ y por tanto

$$bc^* + cb^* \in E^n. \tag{3.3}$$

De (3.2) y (3.3) tenemos que $bc^*, cb^* \in E^n$ y por lo tanto hemos probado la primera parte, esto es

$$bc^*, cb^* \in E^n \cap C^{n-1} = E^{n-1}. \tag{3.4}$$

Veamos ahora que b y c son invertibles. Como $bb^- + cc^-, bb^- - cc^- \in \mathbb{R}$, entonces la suma y resta de estas expresiones también será un número real, por lo que deducimos que $bb^-, cc^- \in \mathbb{R}$. Ahora, como $bc^* \in E^n$, usando el Lema 3.0.3, tenemos que $c^*b \in E^n$ y por lo tanto $b^*c = (c^*b)^* = c^*b \in E^n$.

Además, como $bb^- + cc^- \neq 0$, entonces $bb^- \neq 0$ ó $cc^- \neq 0$, y así b es invertible con inverso $b^{-1} = (bb^-)^{-1}b^-$ o bien, c es invertible con inverso $c^{-1} = (cc^-)^{-1}c^-$. Como $b \neq 0 \neq c$, entonces $b^*c = c^*b \neq 0$, pues de otra forma, b y c serían divisores de cero, en contradicción con el Lema 3.0.2.

Por el Lema 3.0.1, $b^*c = c^*b$ es invertible, por lo que si $bb^- = 0$, entonces $(c^*b)b^- = c^*(bb^-) = 0$ y c^*b sería divisor de cero, en contradicción con el Lema 3.0.2. Análogamente, si $cc^- = 0$, entonces $(b^*c)c^- = b^*(cc^-) = 0$, por lo que b^*c sería un divisor de cero y nuevamente esto es una contradicción. De manera que $bb^-, cc^- \in \mathbb{R} - \{0\}$, por lo que b y c son invertibles con inversos

$$b^{-1} = \frac{b^-}{bb^-} = \frac{b^-}{N(b)} \quad \text{y} \quad c^{-1} = \frac{c^-}{cc^-} = \frac{c^-}{N(c)}. \tag{3.5}$$

Sea $v \in E^{n-1}$. Como $a \in \Gamma^n$, entonces $av(a')^{-1} \in E^n$, por lo que podemos escribir $av(a')^{-1} = u + ti_n$, con $u \in E^{n-1}$, $t \in \mathbb{R}$.

Entonces

$$av = (u + ti_n)a', \tag{3.6}$$

Ahora, usando (3.1), por una parte tenemos que

$$av = (b + ci_n)v = bv + ci_nv = bv + cv'i_n = bv - cvi_n$$

y por otra parte,

$$\begin{aligned}(u + ti_n)a' &= (u + ti_n)(b + ci_n)' \\ &= (u + ti_n)(b' - c'i_n) \\ &= ub' - uc'i_n + ti_nb' - ti_nc'i_n \\ &= ub' - uc'i_n + t(b')'i_n - ti_n^2(c')' \\ &= ub' - uc'i_n + tbi_n + tc \\ &= ub' + tc + (tb - uc')i_n,\end{aligned}$$

por lo que usando (3.6) se tiene que $bv - cvi_n = ub' + tc + (tb - uc')i_n$ y por tanto, igualando los términos que contienen a i_n como factor, llegamos a que

$$bv = ub' + tc \ \text{ y } \ cv = uc' - tb.$$

De esto último, utilizando (3.5), (3.4), se tiene que

$$\begin{aligned}bv(b')^{-1} &= (ub' + tc)(b')^{-1} = u + tc(b')^{-1} \\ &= u + tc(b^{-1})' = u + tc((N(b))^{-1}b^-)' \\ &= u + t(N(b))^{-1}c(b^-)' \\ &= u + t(N(b))^{-1}cb^* \in E^{n-1},\end{aligned}$$

por lo que $b \in \Gamma^{n-1}$. Análogamente, tenemos que

$$\begin{aligned}cv(c')^{-1} &= (uc' - tb)(c')^{-1} = u - tb(c')^{-1} \\ &= u - tb(c^{-1})' = u - tb((N(c))^{-1}c^-)' \\ &= u - t(N(c))^{-1}b(c^-)' \\ &= u - t(N(c))^{-1}bc^* \in E^{n-1},\end{aligned}$$

por lo que $c \in \Gamma^{n-1}$. Esto prueba la necesidad en la proposición.

Ahora probamos la suficiencia, por lo que suponemos que $b, c \in \overline{\Gamma}^{n-1}$ y que $bc^* \in E^{n-1}$.

Si $b = c = 0$, entonces $a = 0 \in \overline{\Gamma}^n$.

Si $c = 0$ y $b \neq 0$, entonces por hipótesis y por la Proposición 1.0.19 tenemos que $a = b \in \Gamma^{n-1} = \Gamma^n \cap C^{n-1}$, por lo que en particular $a \in \Gamma^n$.

Supongamos que $c \neq 0$, entonces por hipótesis $c \in \Gamma^{n-1}$ y observamos que esto implica que $N(c) \in \mathbb{R} - \{0\}$.

Tenemos que

$$a = b + ci_n = c(c^{-1}b + i_n) \tag{3.7}$$

y usando que $bc^* \in E^{n-1}$ obtenemos

$$c(c^{-1}b)(c')^{-1} = b(c^{-1})' = b((N(c))^{-1}c^-)' = N(c)^{-1}bc^* \in E^{n-1}.$$

Multiplicando esta expresión por la izquierda por c^{-1} y por la derecha por c' y recordando que $c^{-1} \in \Gamma^{n-1}$, obtenemos que

$$c^{-1}b = c^{-1}(N(c)^{-1}bc^*)c' = (c^{-1})(N(c)^{-1}bc^*)((c^{-1})')^{-1} \in E^{n-1},$$

lo que implica que $(c^{-1}b + i_n) \in E^n$ y con esto, usando (3.7) llegamos a que $a \in \Gamma^{n-1}E^n$, donde $\Gamma^{n-1}E^n = \{dv \in C^n \mid d \in \Gamma^{n-1}, v \in E^n\}$.

Veamos que $\Gamma^{n-1}E^n \subseteq \overline{\Gamma}^n$. Sean $d \in \Gamma^{n-1}$ y $v \in E^n$. Claramente $dv \in C^n$.

Si $v = 0$, entonces $dv = 0 \in \overline{\Gamma}^n$, pero si $v \neq 0$, por el Lema 3.0.1 tenemos que $q(v) \neq 0$ y por la Proposición 1.0.6 se tiene que $v \in \Gamma^n$, por lo que en particular, v es invertible y entonces dv también lo es.

Ahora, si $w \in E^n$, como $v \in \Gamma^n$, entonces $vw(v')^{-1} \in E^n$, por lo que $vw(v')^{-1} = u + ti_n$, con $u \in E^{n-1}$ y $t \in \mathbb{R}$. Usando esto y recordando que $d \in \Gamma^{n-1} \subseteq C^{n-1}$ y que por tanto $di_n = i_n d'$, obtenemos

$$\begin{aligned}(dv)w((dv)')^{-1} &= d(vw(v')^{-1})(d')^{-1} = d(u + ti_n)(d')^{-1} \\ &= du(d')^{-1} + d(ti_n)(d')^{-1} = du(d')^{-1} + ti_n d'(d')^{-1} \\ &= du(d')^{-1} + ti_n \in E^n.\end{aligned}$$

Por lo tanto, $dv \in \Gamma^n$ y concluimos que $\Gamma^{n-1}E^n \subseteq \overline{\Gamma}^n$.

Otra forma de probar esto último es usar la Proposición 1.0.19, pues así $\Gamma^{n-1} = \Gamma^n \cap C^{n-1}$ por lo que en particular, $\Gamma^{n-1}E^n \subseteq \Gamma^n E^n \subseteq \overline{\Gamma}^n$ donde la última contención se sigue nuevamente debido al Lema 3.0.1 y a la Proposición 1.0.6. □

Definición 9 *Una matriz de Clifford de dimensión n es una matriz*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M(2, C^n)$$

que satisface las siguientes condiciones

$$(C1) \quad a, b, c, d \in \overline{\Gamma}^n,$$

$$(C2) \quad ab^*, cd^*, a^*c, b^*d \in E^n,$$

$$(C3) \quad ad^* - bc^* = d^*a - b^*c = 1.$$

El conjunto de matrices de Clifford se denota por $\mathscr{C}^n$.

Lema 3.0.5 *Los anillos $M(2, End(C^n))$ y $End((C^n)^2)$ son isomorfos.*

Demostración. Sea $\Phi : M(2, End(C^n)) \to End((C^n)^2)$ dada por

$$\Phi\left(\begin{pmatrix} \varphi_1 & \varphi_2 \\ \varphi_3 & \varphi_4 \end{pmatrix}\right) = \phi, \text{ donde } \phi((x,y)) = (\varphi_1(x) + \varphi_2(y), \varphi_3(x) + \varphi_4(y)).$$

Notamos que $\phi \in End((C^n)^2)$ ya que para $j \in \{1,2,3,4\}$ $\varphi_j \in End(C^n)$.

Afirmamos que Φ es isomorfismo de anillos. Veamos primero que Φ es homomorfismo. Supongamos que para $j \in \{1,2,3,4\}$, $\varphi_j, \varphi'_j \in End(C^n)$. Tenemos que

$$\Phi\left(\begin{pmatrix} \varphi_1 & \varphi_2 \\ \varphi_3 & \varphi_4 \end{pmatrix}\right) = \phi, \text{ donde } \phi((x,y)) = (\varphi_1(x) + \varphi_2(y), \varphi_3(x) + \varphi_4(y))$$

y también

$$\Phi\left(\begin{pmatrix} \varphi'_1 & \varphi'_2 \\ \varphi'_3 & \varphi'_4 \end{pmatrix}\right) = \phi', \text{ donde } \phi'((x,y)) = (\varphi'_1(x) + \varphi'_2(y), \varphi'_3(x) + \varphi'_4(y)).$$

Entonces

$$\Phi\left(\begin{pmatrix} \varphi_1 & \varphi_2 \\ \varphi_3 & \varphi_4 \end{pmatrix} + \begin{pmatrix} \varphi'_1 & \varphi'_2 \\ \varphi'_3 & \varphi'_4 \end{pmatrix}\right) = \Phi\left(\begin{pmatrix} \varphi_1 + \varphi'_1 & \varphi_2 + \varphi'_2 \\ \varphi_3 + \varphi'_3 & \varphi_4 + \varphi'_4 \end{pmatrix}\right) = f,$$

donde $f \in End((C^n)^2)$ es tal que

$$\begin{aligned} f((x,y)) &= ((\varphi_1+\varphi_1')(x)+(\varphi_2+\varphi_2')(y),(\varphi_3+\varphi_3')(x)+(\varphi_4+\varphi_4')(y)) \\ &= (\varphi_1(x)+\varphi_2(y),\varphi_3(x)+\varphi_4(y))+(\varphi_1'(x)+\varphi_2'(y),\varphi_3'(x)+\varphi_4'(y)) \\ &= \phi((x,y))+\phi'((x,y)), \end{aligned}$$

por lo que $f = \phi + \phi'$, es decir,

$$\Phi\left(\begin{pmatrix} \varphi_1 & \varphi_2 \\ \varphi_3 & \varphi_4 \end{pmatrix}+\begin{pmatrix} \varphi_1' & \varphi_2' \\ \varphi_3' & \varphi_4' \end{pmatrix}\right) = \Phi\left(\begin{pmatrix} \varphi_1 & \varphi_2 \\ \varphi_3 & \varphi_4 \end{pmatrix}\right)+\Phi\left(\begin{pmatrix} \varphi_1' & \varphi_2' \\ \varphi_3' & \varphi_4' \end{pmatrix}\right).$$

Además,

$$\Phi\left(\begin{pmatrix} \varphi_1 & \varphi_2 \\ \varphi_3 & \varphi_4 \end{pmatrix}\begin{pmatrix} \varphi_1' & \varphi_2' \\ \varphi_3' & \varphi_4' \end{pmatrix}\right) = \Phi\left(\begin{pmatrix} \varphi_1\varphi_1'+\varphi_2\varphi_3' & \varphi_1\varphi_2'+\varphi_2\varphi_4' \\ \varphi_3\varphi_1'+\varphi_4\varphi_3' & \varphi_3\varphi_2'+\varphi_4\varphi_4' \end{pmatrix}\right) = g,$$

donde $g \in End((C^n)^2)$ es tal que

$$\begin{aligned} &g((x,y)) \\ &= ((\varphi_1\varphi_1'+\varphi_2\varphi_3')(x)+(\varphi_1\varphi_2'+\varphi_2\varphi_4')(y),(\varphi_3\varphi_1'+\varphi_4\varphi_3')(x)+(\varphi_3\varphi_2'+\varphi_4\varphi_4')(y)). \end{aligned}$$

Por otra parte,

$$\begin{aligned} \phi\circ\phi'((x,y)) &= \phi((\varphi_1'(x)+\varphi_2'(y),\varphi_3'(x)+\varphi_4'(y))) \\ &= (\varphi_1(\varphi_1'(x)+\varphi_2'(y))+\varphi_2(\varphi_3'(x)+\varphi_4'(y)),\varphi_3(\varphi_1'(x)+\varphi_2'(y))+\varphi_4(\varphi_3'(x)+\varphi_4'(y))) \\ &= g((x,y)), \end{aligned}$$

por lo que $g = \phi \circ \phi'$, es decir,

$$\Phi\left(\begin{pmatrix} \varphi_1 & \varphi_2 \\ \varphi_3 & \varphi_4 \end{pmatrix}\begin{pmatrix} \varphi_1' & \varphi_2' \\ \varphi_3' & \varphi_4' \end{pmatrix}\right) = \Phi\left(\begin{pmatrix} \varphi_1 & \varphi_2 \\ \varphi_3 & \varphi_4 \end{pmatrix}\right)\circ\Phi\left(\begin{pmatrix} \varphi_1' & \varphi_2' \\ \varphi_3' & \varphi_4' \end{pmatrix}\right).$$

Por lo anterior, podemos concluir que Φ es homomorfismo de anillos.

Ahora veamos que Φ es biyectiva.

$$\begin{aligned} &\begin{pmatrix} \varphi_1 & \varphi_2 \\ \varphi_3 & \varphi_4 \end{pmatrix} \in Ker(\Phi) \Longrightarrow \Phi\left(\begin{pmatrix} \varphi_1 & \varphi_2 \\ \varphi_3 & \varphi_4 \end{pmatrix}\right) \equiv 0 \\ &\Longrightarrow \forall x,y \in C^n\ (\varphi_1(x)+\varphi_2(y),\varphi_3(x)+\varphi_4(y)) = (0,0). \end{aligned}$$

Como $\forall j \in \{1,2,3,4\},\ \varphi_j \in End(C^n)$, entonces $\varphi_j(0) = 0$, por lo que en particular, tomando $y = 0$ tenemos que

$$\forall x \in C^n\ (\varphi_1(x), \varphi_3(x)) = (0,0),\ \text{es decir, } \varphi_1, \varphi_3 \equiv 0.$$

Análogamente, tomando $x = 0$ tenemos que

$$\forall y \in C^n\ (\varphi_2(y), \varphi_4(y)) = (0,0),\ \text{es decir, } \varphi_2, \varphi_4 \equiv 0.$$

De manera que

$$Ker(\Phi) = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\},\ \text{y por lo tanto } \Phi \text{ es inyectiva.}$$

Ahora consideramos a las proyecciones canónicas $\pi_1, \pi_2 : (C^n)^2 \to C^n$ y a las inclusiones canónicas $\iota_1, \iota_2 : C^n \to (C^n)^2$, tales que para $x, y \in C^n$

$$\pi_1((x,y)) = x,\ \ \pi_2((x,y)) = y.$$
$$\iota_1(x) = (x,0),\ \ \iota_2(y) = (0,y).$$

Recordamos que las proyecciones canónicas son epimorfismos, mientras que las inclusiones canónicas son monomorfismos.

Finalmente, dado $\phi \in End((C^n)^2)$ se tiene que para $x, y \in C^n$

$$\begin{aligned}
\phi((x,y)) &= \phi((x,0) + (0,y)) \\
&= \phi((x,0)) + \phi((0,y)) \\
&= \phi\iota_1(x) + \phi\iota_2(y) \\
&= (\pi_1\phi\iota_1(x), \pi_2\phi\iota_1(x)) + (\pi_1\phi\iota_2(y), \pi_2\phi\iota_2(y)) \\
&= (\pi_1\phi\iota_1(x) + \pi_1\phi\iota_2(y), \pi_2\phi\iota_1(x) + \pi_2\phi\iota_2(y)),
\end{aligned}$$

de donde es natural considerar

$$\varphi_1 = \pi_1\phi\iota_1,\ \ \varphi_2 = \pi_1\phi\iota_2,\ \ \varphi_3 = \pi_2\phi\iota_1,\ \ \varphi_4 = \pi_2\phi\iota_2 \in End(C^n)$$

ya que entonces

$$\Phi\left(\begin{pmatrix} \varphi_1 & \varphi_2 \\ \varphi_3 & \varphi_4 \end{pmatrix} \right) = \phi \text{ y por lo tanto } \Phi \text{ es suprayectiva}$$

Con esto concluimos que Φ es isomorfismo de anillos. □

Corolario 3.0.6 *Sea $a \in M(2, End(C^n))$. Si $b \in M(2, End(C^n))$ es inverso izquierdo (derecho) de a, entonces b es inverso derecho (izquierdo) de a.*

Demostración. Primero observamos que como $(C^n)^2$ es espacio vectorial, entonces $End((C^n)^2)$ es el anillo consistente de las transformaciones lineales de $(C^n)^2$ en sí mismo, por lo que debido al teorema de la dimensión, tenemos que una transformación en $End((C^n)^2)$ es inyectiva si y sólo si es suprayectiva.

Sea $\Phi : M(2, End(C^n)) \to End((C^n)^2)$ el isomorfismo dado en el lema anterior. Sea $a \in M(2, End(C^n))$ y supongamos que $b \in M(2, End(C^n))$ es inverso izquierdo de a. De manera que $\Phi(b)$ es inverso izquierdo de $\Phi(a)$ (ya que $\Phi(Id_{M(2,End(C^n))}) = Id_{(C^n)^2}$), lo que implica que $\Phi(a)$ es inyectiva y por lo tanto es también suprayectiva, por lo que es invertible y sabemos que en este caso el inverso es único y podemos concluir que $\Phi(b)$ es también inverso derecho de $\Phi(a)$. Esto implica que b es también inverso derecho de a.

Si suponemos que b es inverso derecho de a, con un argumento análogo al anterior también podemos concluir que b es inverso izquierdo de a. □

Proposición 3.0.7 *Las condiciones para las matrices de Clifford dadas en la Definición 9 pueden ser reducidas a las siguientes:*

$$(C1) \quad a, b, c, d \in \overline{\Gamma}^n,$$

$$(C2) \quad ab^*, cd^* \in E^n,$$

$$(C3) \quad ad^* - bc^* = 1.$$

Demostración. Sea

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathscr{C}^n$$

y tomamos

$$h = \begin{pmatrix} d^* & -b^* \\ -c^* & a^* \end{pmatrix}.$$

Primero notamos que como $ab^*, cd^* \in E^n$ entonces $ab^* = (ab^*)^* = ba^*$ y $cd^* = (cd^*)^* = dc^*$. También tenemos que $ad^* - bc^* = 1$ y por tanto $da^* - cb^* = (ad^* - bc^*)^* = 1$. De manera que

$$gh = \begin{pmatrix} ad^* - bc^* & -ab^* + ba^* \\ cd^* - dc^* & da^* - cb^* \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Consideramos la acción de multiplicación izquierda de C^n en sí mismo:

$$L : C^n \to End(C^n), \text{ tal que para } a \in C^n$$
$$L(a) = L_a : x \to ax, \text{ donde } x \in C^n.$$

L es inyectiva ya que si $a, b \in C^n$ son tales que $L(a) = L(b)$, entonces $L_a = L_b$, es decir, $\forall x \in C^n\ L_a(x) = L_b(x)$, de manera que $\forall x \in C^n\ ax = bx$, por lo que en particular para $x = 1$, tenemos que $a = b$.

La transformación L induce naturalmente un homomorfismo de anillos

$$L^{\#} : M(2, C^n) \to M(2, End(C^n)) \text{ dado por}$$
$$L^{\#}\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = \begin{pmatrix} L_a & L_b \\ L_c & L_d \end{pmatrix}.$$

En efecto $L^{\#}$ es homomorfismo, ya que si $a, b, x \in C^n$ entonces

$$L_{a+b}(x) = (a+b)x = ax + bx = L_a(x) + L_b(x) \text{ y también}$$
$$L_{ab}(x) = (ab)x = a(bx) = L_a L_b(x),$$

es decir,

$$L_{a+b} = L_a + L_b \text{ y } L_{ab} = L_a L_b.$$

Usando esto tenemos que

$$L^{\#}\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\right) = L^{\#}\left(\begin{pmatrix} a+a' & b+b' \\ c+c' & d+d' \end{pmatrix}\right)$$
$$= \begin{pmatrix} L_{a+a'} & L_{b+b'} \\ L_{c+c'} & L_{d+d'} \end{pmatrix} = \begin{pmatrix} L_a + L_{a'} & L_b + L_{b'} \\ L_c + L_{c'} & L_d + L_{d'} \end{pmatrix}$$
$$= \begin{pmatrix} L_a & L_b \\ L_c & L_d \end{pmatrix} + \begin{pmatrix} L_{a'} & L_{b'} \\ L_{c'} & L_{d'} \end{pmatrix} = L^{\#}\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) + L^{\#}\left(\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\right)$$

y también

$$L^{\#}\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\right) = L^{\#}\left(\begin{pmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{pmatrix}\right)$$
$$= \begin{pmatrix} L_{aa'+bc'} & L_{ab'+bd'} \\ L_{ca'+dc'} & L_{cb'+dd'} \end{pmatrix} = \begin{pmatrix} L_a L_{a'} + L_b L_{c'} & L_a L_{b'} + L_b L_{d'} \\ L_c L_{a'} + L_d L_{c'} & L_c L_{b'} + L_d L_{d'} \end{pmatrix}$$
$$= \begin{pmatrix} L_a & L_b \\ L_c & L_d \end{pmatrix}\begin{pmatrix} L_{a'} & L_{b'} \\ L_{c'} & L_{d'} \end{pmatrix} = L^{\#}\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) L^{\#}\left(\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\right).$$

Notamos que como L es inyectiva, entonces también $L^{\#}$ lo es ya que

$$\begin{pmatrix} L_a & L_b \\ L_c & L_d \end{pmatrix} = \begin{pmatrix} L_{a'} & L_{b'} \\ L_{c'} & L_{d'} \end{pmatrix} \Rightarrow L_a = L_{a'},\ L_b = L_{b'},\ L_c = L_{c'},\ L_d = L_{d'}$$
$$\Rightarrow a = a',\ b = b',\ c = c',\ d = d' \Rightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}.$$

Por lo anterior, podemos concluir que $L^{\#}$ es un monomorfismo de anillos. Tenemos que

$$L^{\#}(g)L^{\#}(h) = L^{\#}(gh) = L^{\#}(1) = 1.$$

Y por tanto, por el Corolario 3.0.6, también sucede que

$$L^{\#}(hg) = L^{\#}(h)L^{\#}(g) = 1 = L^{\#}(1).$$

Como $L^{\#}$ es inyectiva, entonces $hg = 1$. Por tanto, tenemos que

$$hg = \begin{pmatrix} d^*a - b^*c & d^*b - b^*d \\ -c^*a + a^*c & a^*d - c^*b \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

De manera que

$$d^*a - b^*c = 1.$$

Además, como $ab^*, cd^* \in E^n$, entonces por el Lema 3.0.3, se tiene que $b^*a, d^*c \in E^n$ y por tanto

$$a^*b = (b^*a)^* = b^*a \in E^n$$

y también

$$c^*d = (d^*c)^* = d^*c \in E^n.$$

Por la Proposición 1.0.20 inciso i), tenemos que $a^*a, b^*b, c^*c, d^*d \in \mathbb{R} - \{0\}$ y así, las observaciones anteriores implican que

$$a^*c = a^*(ad^* - bc^*)c = (a^*a)d^*c - a^*b(c^*c) \in E^n,$$

y también que

$$b^*d = b^*(ad^* - bc^*)d = b^*a(d^*d) - (b^*b)c^*d \in E^n.$$

Es decir, las condiciones de esta proposición implican las condiciones de la Definición 9. Evidentemente, el recíproco también es cierto, lo que concluye la demostración. □

Proposición 3.0.8 *Las matrices de Clifford $\mathscr{C}^n$ forman un grupo bajo la multiplicación.*

Demostración. Es claro que la matriz identidad es un elemento de $\mathscr{C}^n$. Supongamos que

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix},\ h = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathscr{C}^n.$$

Por la demostración de la proposición anterior, sabemos que

$$g^{-1} = \begin{pmatrix} d^* & -b^* \\ -c^* & a^* \end{pmatrix}.$$

Como $a, b, c, d \in \overline{\Gamma}^n$, por el Corolario 1.0.16, $\overline{\Gamma}^n$ es cerrado bajo la reversión, por lo que $d^*, -b^*, -c^*, a^* \in \overline{\Gamma}^n$, es decir, g^{-1} cumple la condición $(C1)$.

Ahora, como $b^*d \in E^n$, entonces $b^*d = (b^*d)^* = d^*b$ y así

$$d^*(-b^*)^* = -d^*b \in E^n.$$

Análogamente, como $a^*c \in E^n$, entonces $a^*c = (a^*c)^* = c^*a$ y así

$$(-c^*)(a^*)^* = -c^*a \in E^n,$$

por lo que g^{-1} cumple la condición $(C2)$ de la proposición anterior.

La condición $(C3)$ es clara ya que $d^*(a^*)^* - (-b^*)(-c^*)^* = d^*a - b^*c = 1$. y entonces se sigue de la Proposición 3.0.7, que $g^{-1} \in \mathscr{C}^n$.

Sólo falta ver que se cumplen las condiciones de la Proposición 3.0.7 para la matriz gh. Tenemos que

$$gh = \begin{pmatrix} a\alpha + b\gamma & a\beta + b\delta \\ c\alpha + d\gamma & c\beta + d\delta \end{pmatrix}.$$

$(C1)$: Para mostrar que $a\alpha + b\gamma \in \overline{\Gamma}^n$, podemos asumir que $a, \gamma \neq 0$, pues $a\alpha, b\gamma \in \overline{\Gamma}^n$. Por la Proposición 1.0.20 i), tenemos que $aa^*, \gamma\gamma^* \in \mathbb{R} - \{0\}$ y así, $a^{-1} = (aa^*)^{-1}a^*$ y $\gamma^{-1} = (\gamma\gamma^*)^{-1}\gamma^*$. Notamos también que como g, h cumplen la condición $(C2)$, en particular $\alpha\gamma^*, a^*b \in E^n$. Teniendo en mente estas observaciones llegamos a que

$$\begin{aligned} a\alpha + b\gamma &= a\alpha\gamma^{-1}\gamma + aa^{-1}b\gamma \\ &= a(\alpha\gamma^{-1} + a^{-1}b)\gamma \\ &= a((\gamma\gamma^*)^{-1}\alpha\gamma^* + (aa^*)^{-1}a^*b)\gamma, \end{aligned}$$

sin embargo $((\gamma\gamma^*)^{-1}\alpha\gamma^* + (aa^*)^{-1}a^*b) \in E^n$ es 0 o es invertible, por lo que en cualquier caso $((\gamma\gamma^*)^{-1}\alpha\gamma^* + (aa^*)^{-1}a^*b) \in \overline{\Gamma}^n$ y esto implica que $a\alpha + b\gamma \in \overline{\Gamma}^n$.

Usando argumentos similares al dado anteriormente, podemos demostrar que las demás entradas de la matriz gh son elementos de $\overline{\Gamma}^n$.

$(C2)$: Por el Lema 3.0.3 basta demostrar que $(a\beta + b\delta)^*(a\alpha + b\gamma) \in E^n$. Escribimos

$$\begin{aligned}(a\beta + b\delta)^*(a\alpha + b\gamma) &= (\beta^*a^* + \delta^*b^*)(a\alpha + b\gamma)\\ &= \beta^*a^*a\alpha + \beta^*a^*b\gamma + \delta^*b^*a\alpha + \delta^*b^*b\gamma,\end{aligned}$$

donde, debido a la Proposición 1.0.20 $i)$ y al hecho de que h cumple la condición $(C2)$, se tiene que

$$\begin{aligned}\beta^*a^*a\alpha &= (a^*a)\beta^*\alpha \in E^n,\\ \delta^*b^*b\gamma &= (b^*b)\delta^*\gamma \in E^n.\end{aligned}$$

Si $\beta = 0$, como h cumple la condición $(C3)$, es decir, $\alpha\delta^* = 1$, entonces debido a la Proposición 1.0.20 $i)$, $\delta^* = \alpha^{-1} = (\alpha\alpha^*)^{-1}\alpha^*$ y también por la parte $ii)$ de esta proposición tenemos que

$$\delta^*b^*a\alpha = (\alpha\alpha^*)^{-1}\alpha^*(b^*a)\alpha \in E^n,$$

por lo que habríamos terminado.

Supongamos que $\beta \neq 0$. Nuevamente por la Proposición 1.0.20 $i)$, en este caso tenemos que

$$\begin{aligned}&(\beta^*\beta)^2(\beta^*a^*b\gamma + \delta^*b^*a\alpha)\\ &= (\beta^*\beta)(\beta^*a^*b\gamma + \delta^*b^*a\alpha)(\beta^*\beta)\\ &= \beta^*(\beta\beta^*a^*b\gamma\beta^* + \beta\delta^*b^*a\alpha\beta^*)\beta\\ &= \beta^*((\beta\beta^*)a^*b(-1 + \delta\alpha^*) + \beta\delta^*b^*a\beta\alpha^*)\beta\\ &= -(\beta\beta^*)\beta^*(a^*b)\beta + \beta^*((a^*b)\delta(\beta^*\beta)\alpha^* + \beta\delta^*b^*a\beta\alpha^*)\beta\\ &= -(\beta\beta^*)\beta^*(a^*b)\beta + \beta^*((a^*b)(\delta\beta^*) + (\beta\delta^*)(b^*a))\beta\alpha^*\beta.\end{aligned} \tag{3.8}$$

Notamos que por el Lema 3.0.3 y por la condición $(C2)$ para g y h, se tiene que $a^*b = (a^*b)^* = b^*a$, $\delta\beta^* = (\delta\beta^*)^* = \beta\delta^* \in E^n = C^{n\,(1)}$ y entonces

$$\zeta = (a^*b)(\delta\beta^*) + (\beta\delta^*)(b^*a) \in C^{n\,(0)} + C^{n\,(2)},$$

pues al multiplicar 2 palabras de longitud 1 podrían formar un real si son iguales o formar una palabra de longitud 2 si son distintas. Por otra parte, es fácil mostrar que $\zeta^* = \zeta$, y entonces ζ no contiene términos con palabras de longitud 2 y por lo tanto, $\zeta \in C^{n\,(0)} = \mathbb{R}$.

De manera que por la Proposición 1.0.20 y por (3.8),

$$(\beta^*\beta)^2(\beta^* a^* b\gamma + \delta^* b^* a\alpha) = -(\beta\beta^*)\beta^*(a^*b)\beta + \zeta\beta^*(\beta\alpha^*)\beta \in E^n,$$

lo que implica que $\beta^* a^* b\gamma + \delta^* b^* a\alpha \in E^n$ y así, $(a\beta + b\delta)^*(a\alpha + b\gamma) \in E^n$.

De manera similar se puede demostrar que $(c\alpha + d\gamma)(c\beta + d\delta)^* \in E^n$.

$(C3)$: Como $\alpha\beta^*$, $\gamma\delta^* \in E^n$, entonces se tiene que $\alpha\beta^* = (\alpha\beta^*)^* = \beta\alpha^*$ y $\gamma\delta^* = (\gamma\delta^*)^* = \delta\gamma^*$, por lo que

$$\begin{aligned}
&(a\alpha + b\gamma)(c\beta + d\delta)^* - (a\beta + b\delta)(c\alpha + d\gamma)^* \\
&= (a\alpha + b\gamma)(\beta^* c^* + \delta^* d^*) - (a\beta + b\delta)(\alpha^* c^* + \gamma^* d^*) \\
&= (a\alpha\beta^* c^* + a\alpha\delta^* d^* + b\gamma\beta^* c^* + b\gamma\delta^* d^*) \\
&\quad - (a\beta\alpha^* c^* + a\beta\gamma^* d^* + b\delta\alpha^* c^* + b\delta\gamma^* d^*) \\
&= (a\alpha\delta^* d^* + b\gamma\beta^* c^*) - (a\beta\gamma^* d^* + b\delta\alpha^* c^*) \\
&= a(\alpha\delta^* - \beta\gamma)d^* - b(\delta\alpha^* - \gamma\beta^*)c^* \\
&= ad^* - bc^* = 1.
\end{aligned}$$

Finalmente, $gh \in \mathscr{C}^n$ y podemos concluir que $\mathscr{C}^n$ es un grupo. □

Proposición 3.0.9 *Sea $g \in \mathscr{C}^n$. Usando la misma notación que en la proposición anterior, se tiene que g cumple exactamente una de las siguientes condiciones*

$$(C1_{par})\ \ a, d \in \overline{\Gamma}^n_{par}\ y\ b, c \in \overline{\Gamma}^n_{impar},$$
$$(C1_{impar})\ \ a, d \in \overline{\Gamma}^n_{impar}\ y\ b, c \in \overline{\Gamma}^n_{par}.$$

Demostración. Sea

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathscr{C}^n.$$

Recordamos que la condición $(C1)$ y la Proposición 1.0.14 implican que cada una de las longitudes de las palabras en a tienen la misma paridad. Esto mismo se tiene también para b, c, d.

La condición $(C2)$ nos dice que $ab^*, cd^* \in E^n = \overline{\Gamma}^{n\,(1)} \subseteq \overline{\Gamma}^n_{impar}$, por lo que cada una de las palabras que conforman los términos de a tiene longitud de paridad distinta a las palabras que conforman los términos de b, pues de otra manera, como al multiplicar dos palabras la longitud disminuye en múltiplos de 2, tendríamos que ab^* contiene palabras de longitud par, lo que es una contradicción. Del mismo modo también notamos que las longitudes de las palabras que conforman los términos de c tienen distinta paridad que las longitudes de las palabras que conforman los términos de d.

Ahora, si las longitudes de las palabras en a y en d tuvieran distintas paridades, por lo explicado anteriormente, tendríamos que las longitudes de las palabras en b y en c también tendrían distintas paridades, de manera que la condición $(C3)$ sería imposible ya que en este caso $ad^* - bc^* \in \overline{\Gamma}^n_{impar}$, lo que contradice el hecho de que $ad^* - bc^* = 1$. Por lo tanto, a y d contienen palabras cuyas longitudes tienen la misma paridad, al igual que b y c.

En consideración de las observaciones anteriores, tenemos que

$$(C1_{par}) \;\; a, d \in \overline{\Gamma}^n_{par} \text{ y } b, c \in \overline{\Gamma}^n_{impar},$$

o bien,

$$(C1_{impar}) \;\; a, d \in \overline{\Gamma}^n_{impar} \text{ y } b, c \in \overline{\Gamma}^n_{par}.$$

□

El conjunto de matrices de Clifford que satisfacen la condición $(C1_{par})$ será denotado por $\mathscr{C}^n_{par}$, mientras que el conjunto de matrices que satisfacen $(C1_{impar})$ será denotado por $\mathscr{C}^n_{impar}$.

Las siguientes observaciones nos serán útiles más adelante, pues probaremos que las matrices en $\mathscr{C}^n_{par}$ son precisamente las que se corresponden con transformaciones de Möbius que preservan la orientación.

Sean

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, h = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathscr{C}^n.$$

Recordamos que

$$gh = \begin{pmatrix} a\alpha + b\gamma & a\beta + b\delta \\ c\alpha + d\gamma & c\beta + d\delta \end{pmatrix}.$$

Entonces, usando la proposición anterior tenemos lo siguiente:

Si $g \in \mathscr{C}^n_{par}$ y $h \in \mathscr{C}^n_{par}$, entonces $a, \alpha \in \overline{\Gamma}^n_{par}$ y $b, \gamma \in \overline{\Gamma}^n_{impar}$, por lo que $a\alpha, b\gamma \in \overline{\Gamma}^n_{par}$ y así $a\alpha + b\gamma \in \overline{\Gamma}^n_{par}$, de manera que $gh \in \mathscr{C}^n_{par}$.

Si $g \in \mathscr{C}^n_{par}$ y $h \in \mathscr{C}^n_{impar}$, entonces $a, \gamma \in \overline{\Gamma}^n_{par}$ y $b, \alpha \in \overline{\Gamma}^n_{impar}$, por lo que $a\alpha, b\gamma \in \overline{\Gamma}^n_{impar}$ y así $a\alpha + b\gamma \in \overline{\Gamma}^n_{impar}$, de manera que $gh \in \mathscr{C}^n_{impar}$. Análogamente vemos que si $g \in \mathscr{C}^n_{impar}$ y $h \in \mathscr{C}^n_{par}$, entonces $gh \in \mathscr{C}^n_{impar}$.

Si $g \in \mathscr{C}^n_{impar}$ y $h \in \mathscr{C}^n_{impar}$, entonces $a, \alpha \in \overline{\Gamma}^n_{impar}$ y $b, \gamma \in \overline{\Gamma}^n_{par}$, por lo que $a\alpha, b\gamma \in \overline{\Gamma}^n_{par}$ y así $a\alpha + b\gamma \in \overline{\Gamma}^n_{par}$, de manera que $gh \in \mathscr{C}^n_{par}$.

En particular notamos que $\mathscr{C}^n_{par}$ es un subgrupo de $\mathscr{C}^n$.

Sea $\hat{E}^n = E^n \cup \{\infty\}$ la compactación por un punto de E^n definida usando la proyección estereográfica (véase [4], cap. 3, pág. 20).

Definición 10 *Definimos la acción del grupo $\mathscr{C}^n$ en $\hat{E}^n$, $G : \mathscr{C}^n \times \hat{E}^n \to \hat{E}^n$ tal que para $z \in \hat{E}^n$ y*

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathscr{C}^n,$$

se tiene que $G(g, z) = gz$, donde

$$gz = (az + b)(cz + d)^{-1} \text{ si } z \in E^n - \{-c^{-1}d\},$$
$$g(-c^{-1}d) = \infty,\ g(\infty) = ac^{-1} \text{ si } c \neq 0 \text{ y}$$
$$g(\infty) = \infty \text{ si } c = 0.$$

Probaremos que esta acción está bien definida y que $\mathscr{C}^n$ actúa por transformaciones continuas en $\hat{E}^n$. Para demostrar la continuidad haremos uso del siguiente lema.

Lema 3.0.10 *Para $v \in E^n$ y $a \in \overline{\Gamma}^n$, se tiene que $|ava^*| = |a|^2|v|$.*

Demostración. Sean $v \in E^n$ y $a \in \overline{\Gamma}^n$. Si $v = 0$ ó $a = 0$, entonces el resultado es evidente, por lo que podemos suponer que v y a son distintos de cero.

Notamos que para $u \in E^n$ se tiene que $|u|^2 = -q(u) = |q(u)| = |u^2|$. De manera que recordando la Proposición 1.0.20, tenemos que

$$|ava^*|^2 = |(ava^*)^2| = |av(a^*a)va^*| = |(a^*a)av^2a^*| = |(a^*a)^2||v^2| = |a^*a|^2|v|^2.$$

Por otra parte, como $a \in \Gamma^n$, puede expresarse como $a = v_1...v_r$, donde $v_1, ..., v_r$ son vectores invertibles. Usando esto y la Proposición 1.0.18, se tiene que

$$\begin{aligned} |a|^2 = |N(a)| = |a^-a| &= |(v_1...v_r)^-(v_1...v_r)| = |(v_r^-...v_1^-)(v_1...v_r)| \\ &= |q(v_1)...q(v_r)| = |(v_r...v_1)(v_1...v_r)| = |(v_1...v_r)^*(v_1...v_r)| = |a^*a|, \end{aligned}$$

lo que concluye la prueba. □

Proposición 3.0.11 *Sean $g \in \mathscr{C}^n$ y $z \in \hat{E}^n$. Se tiene que $gz \in \hat{E}^n$, donde gz es como en la Definición 10. Además, la transformación $z \to gz$ es continua.*

Demostración. Sea $g \in \mathscr{C}^n$. Usaremos la misma notación que la que se usó en la Definición 10.

Supongamos que $c = 0$. Sea $z \in E^n$. Por la condición $(C3)$ de la Definición 9, $ad^* = 1$, lo que implica que $d^{-1} = a^*$. También, por $(C2)$ tenemos que $ab^* \in E^n$ y así $ba^* = (ab^*)^* = ab^* \in E^n$. Usando esto y la Proposición 1.0.20 $ii)$ se tiene que

$$gz = (az + b)d^{-1} = (az + b)a^* = aza^* + ba^* \in E^n.$$

La transformación $z \to gz$ es continua en E^n ya que para $z_1, z_2 \in E^n$, usando el Lema 3.0.10, se tiene que

$$|gz_1 - gz_2| = |(az_1a^* + ba^*) - (az_2a^* + ba^*)| = |a(z_1 - z_2)a^*| = |a|^2|z_1 - z_2|.$$

Además, como

$$|gz| = |aza^* + ba^*| \geq |aza^*| - |ba^*| = |a|^2|z| - |ba^*|,$$

se tiene que $|gz| \to \infty$ conforme $|z| \to \infty$, por lo que g es continua en $z = \infty$.

Supongamos ahora que $c \neq 0$. Por la condición $(C2)$ de la Definición 9, se tiene que $dc^* = (cd^*)^* = cd^*, c^*a = (a^*c)^* = a^*c \in E^n$, de manera que por el Lema 3.0.3, $c^*d, ac^* \in E^n$. Recordamos de la Proposición 1.0.20 $i)$, que $c^{-1} = (cc^*)^{-1}c^*$ y entonces $c^{-1}d = (cc^*)^{-1}c^*d$, $ac^{-1} = (cc^*)^{-1}ac^*$, por lo que de lo anterior tenemos que

$$c^{-1}d, ac^{-1} \in E^n.$$

Notamos que como $c^{-1}d \in E^n$ entonces para $z \in E^n - \{-c^-d\}$, se tiene que $(z+c^{-1}d) \in \Gamma^n$ debido al Lema 3.0.1, de manera que $(cz+d)$ es invertible ya que $cz + d = c(z + c^{-1}d) \in \Gamma^n$.

Además, como $ad^* - bc^* = 1$ debido a $(C3)$, tenemos que

$$\begin{aligned} b &= (ad^* - 1)(c^*)^{-1} = ad^*(c^{-1})^* - (c^*)^{-1} \\ &= a(c^{-1}d)^* - (c^*)^{-1} = ac^{-1}d - (c^*)^{-1}, \end{aligned} \tag{3.9}$$

donde la última igualdad se da ya que $c^{-1}d \in E^n$ y por tanto $(c^{-1}d)^* = c^{-1}d$.

Usando esto último, el hecho de que $ac^{-1}, c^{-1}d \in E^n$ y la Proposición 1.0.20 *ii*), tenemos que para $z \in E^n - \{-c^{-1}d\}$,

$$\begin{aligned} gz &= (az+b)(cz+d)^{-1} \\ &= (az + ac^{-1}d - (c^*)^{-1})(c(z+c^{-1}d))^{-1} \\ &= (a(z+c^{-1}d) - (c^*)^{-1})(z+c^{-1}d)^{-1}c^{-1} \\ &= ac^{-1} - (c^{-1})^*(z+c^{-1}d)^{-1}c^{-1} \in E^n. \end{aligned}$$

Análogamente al caso $c = 0$, puede verse que g es continua en E^n. Nuevamente, usando el Lema 3.0.10 y el hecho de que para $v \in E^n$ sucede que

$$|v^{-1}| = \left|\frac{v}{q(v)}\right| = \frac{|v|}{|q(v)|} = \frac{|v|}{|v|^2} = |v|^{-1},$$

se tiene que

$$\begin{aligned} |gz| &= |ac^{-1} - (c^{-1})^*(z+c^{-1}d)^{-1}c^{-1}| \\ &\geq |(c^{-1})^*(z+c^{-1}d)^{-1}c^{-1}| - |ac^{-1}| \\ &= |c^{-1}|^2|z+c^{-1}d|^{-1} - |ac^{-1}|. \end{aligned}$$

Observamos que $|gz| \to \infty$ conforme $z \to -c^{-1}d$. También, como

$$|gz - ac^{-1}| = |(c^{-1})^*(z+c^{-1}d)^{-1}c^{-1}| = |c^{-1}|^2|z+c^{-1}d|^{-1},$$

observamos que $gz \to ac^{-1}$ conforme $|z| \to \infty$. Debido a estas observaciones podemos concluir que g es continua en $\hat{E}^n$. □

Proposición 3.0.12 *La función $G : \mathscr{C}^n \times \hat{E}^n \to \hat{E}^n$ dada en la Definición 10 es una acción del grupo $\mathscr{C}^n$ en $\hat{E}^n$.*

Demostración. Para $z \in \hat{E}^n$ se tiene que $G(1_{\mathscr{C}^n}, z) = 1_{\mathscr{C}^n} z = z$, donde $1_{\mathscr{C}^n}$ denota la matriz identidad de $\mathscr{C}^n$. Ahora supongamos que

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix},\ h = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathscr{C}^n.$$

Resta demostrar que para $z \in \hat{E}^n$, se tiene que $G(gh, z) = G(g, hz)$, es decir, que $(gh)z = g(hz)$.

Sea $z \in E^n - \{h^{-1}(\infty), (gh)^{-1}(\infty)\}$. Tenemos que

$$\begin{aligned}
&g(hz) = g((\alpha z+\beta)(\gamma z+\delta)^{-1})\\
&= (a(\alpha z+\beta)(\gamma z+\delta)^{-1}+b)(c(\alpha z+\beta)(\gamma z+\delta)^{-1}+d)^{-1}\\
&= (a(\alpha z+\beta)+b(\gamma z+\delta))(\gamma z+\delta)^{-1}((c(\alpha z+\beta)+d(\gamma z+\delta))(\gamma z+\delta)^{-1})^{-1}\\
&= (a(\alpha z+\beta)+b(\gamma z+\delta))(\gamma z+\delta)^{-1}(\gamma z+\delta)(c(\alpha z+\beta)+d(\gamma z+\delta))^{-1}\\
&= ((a\alpha+b\gamma)z+a\beta+b\delta)((c\alpha+d\gamma)z+c\beta+d\delta)^{-1}\\
&= (gh)z.
\end{aligned}$$

Como $z \to g(hz)$ y $z \to (gh)z$ son transformaciones continuas que coinciden en un subconjunto denso de $\hat{E}^n$, podemos concluir que coinciden en todo $\hat{E}^n$, es decir, para cualquier $z \in \hat{E}^n$ se tiene que $g(hz) = (gh)z$ y como $g, h \in \mathscr{C}^n$ eran arbitrarios, concluimos que G es en efecto una acción de grupo. □

Ahora veremos que la acción de $\mathscr{C}^n$ en E^n se corresponde con la acción del grupo de transformaciones de Möbius actuando en E^n (véase [4], págs. 20-24). Para demostrar esto, haremos uso del siguiente lema.

Lema 3.0.13 *Para $a \in \Gamma^n$, se tiene que $(a^*)^{-1} = |a|^{-2}a'$.*

Demostración. Sea $a = v_1...v_r \in \Gamma^n$, donde para $j \in \{1, .., r\}$ $v_j \in E^n$ son invertibles. Se tiene que

$$a^*a' = (v_1...v_r)^*(v_1...v_r)' = (v_r...v_1)(-1)^r(v_1...v_r) = (-1)^r q(v_1)...q(v_r).$$

Por otra parte, análogamente a la demostración del Lema 3.0.10 se tiene que

$$|a|^2 = |(v_r^-...v_1^-)(v_1...v_r)| = |(-1)^r q(v_1)...q(v_r)| = |q(v_1)...q(v_r)|.$$

Como para $j \in \{1, ..., r\}$ sucede que $-q(v_j) = |v_j|^2 > 0$, necesariamente $(-1)^r q(v_1)...q(v_r) > 0$, lo que prueba el resultado. □

Teorema 3.0.14 *Para cualquier $g \in \mathscr{C}^n$, la transformación inducida*

$$[g] : \hat{E}^n \to \hat{E}^n, \text{ tal que para } z \in \hat{E}^n \ [g](z) = gz$$

es una transformación de Möbius.

Recíprocamente, cualquier transformación de Möbius de $\hat{E}^n$ se puede escribir como $[g]$ para alguna $g \in \mathscr{C}^n$.

Demostración. Sea

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathscr{C}^n.$$

Si $c = 0$, usando el Lema 3.0.13 y las condiciones $(C1), (C2)$ y $(C3)$ tenemos que

$$ad^* = 1 \Rightarrow d = (a^*)^{-1} = |a|^{-2}a' \text{ y } b = b(a^*a')|a|^{-2} = ab^*(|a|^{-2}a').$$

De manera que

$$\begin{aligned} g &= \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} a & ab^*(|a|^{-2}a') \\ 0 & |a|^{-2}a' \end{pmatrix} = \begin{pmatrix} 1 & ab^* \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & |a|^{-2}a' \end{pmatrix} \\ &= \begin{pmatrix} 1 & ab^* \\ 0 & 1 \end{pmatrix} \begin{pmatrix} |a| & 0 \\ 0 & |a|^{-1} \end{pmatrix} \begin{pmatrix} |a|^{-1}a & 0 \\ 0 & |a|^{-1}a' \end{pmatrix}. \end{aligned}$$

Si $c \neq 0$, usando la expresión de b encontrada en (3.9) en la Proposición 3.0.11 y nuevamente por el Lema 3.0.13 se tiene que

$$b = ac^{-1}d - (c^*)^{-1} = ac^{-1}d - |c|^{-2}c',$$

y por lo tanto,

$$\begin{aligned} g &= \begin{pmatrix} a & ac^{-1}d - |c|^{-2}c' \\ c & d \end{pmatrix} = \begin{pmatrix} a & -|c|^{-2}c' \\ c & 0 \end{pmatrix} \begin{pmatrix} 1 & c^{-1}d \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} |c|ac^{-1} & -|c|^{-1} \\ |c| & 0 \end{pmatrix} \begin{pmatrix} |c|^{-1}c & 0 \\ 0 & |c|^{-1}c' \end{pmatrix} \begin{pmatrix} 1 & c^{-1}d \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} ac^{-1} & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} |c| & 0 \\ 0 & |c|^{-1} \end{pmatrix} \begin{pmatrix} |c|^{-1}c & 0 \\ 0 & |c|^{-1}c' \end{pmatrix} \begin{pmatrix} 1 & c^{-1}d \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & ac^{-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} |c| & 0 \\ 0 & |c|^{-1} \end{pmatrix} \begin{pmatrix} |c|^{-1}c & 0 \\ 0 & |c|^{-1}c' \end{pmatrix} \begin{pmatrix} 1 & c^{-1}d \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

Observamos que las transformaciones que son de la forma

$$\begin{aligned} \begin{pmatrix} 1 & v \\ 0 & 1 \end{pmatrix} z &= z + v \ (v \in E^n), \\ \begin{pmatrix} r & 0 \\ 0 & r^{-1} \end{pmatrix} z &= r^2 z \ (r \in \mathbb{R}), \\ \begin{pmatrix} |a|^{-1}a & 0 \\ 0 & |a|^{-1}a' \end{pmatrix} z &= az(a')^{-1} \ (a \in \Gamma^n), \\ \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} z &= (-1)z^{-1} = -\frac{z}{q(z)} = \frac{z}{|z|^2}, \end{aligned}$$

son traslaciones, homotecias, composición de reflexiones en hiperplanos (debido a la demostración del Teorema 1.0.13) y la inversión respecto a la esfera unitaria, respectivamente, por lo que son todas de Möbius, entonces por lo explicado anteriormente y por la Proposición 3.0.12, se tiene que para cualquier $g \in \mathscr{C}^n$, la transformación inducida $[g] : \hat{E}^n \to \hat{E}^n$ es también de Möbius.

Para demostrar el recíproco, observamos que cualquier transformación de Möbius de $\hat{E}^n$ está generada por elementos de los cuatro tipos descritos anteriormente y que cada una de las matrices que los definen están en $\mathscr{C}^n$ ya que para la composición de reflexiones en hiperplanos se tiene que

$$(|a|^{-1}a)(|a|^{-1}a')^* = |a|^{-2}aa^- = |N(a)|^{-1}N(a) = 1,$$

y para traslaciones, homotecias y la inversión respecto a la esfera unitaria esto se puede verificar fácilmente.

De este hecho se sigue que cualquier transformación de Möbius puede escribirse como $[g]$ para alguna $g \in \mathscr{C}^n$. □

Definición 11 *Denotamos como $M(\hat{E}^n)$ al grupo de transformaciones de Möbius de $\hat{E}^n$, y como $SM(\hat{E}^n)$ al subgrupo de transformaciones de Möbius de $\hat{E}^n$ que preservan la orientación.*

Definición 12 *Definimos a la transformación $\lambda : \mathscr{C}^n \to M(\hat{E}^n)$ tal que para $g \in \mathscr{C}^n$, $\lambda(g) = [g]$, donde $[g]$ es como en la Proposición 3.0.14.*

Proposición 3.0.15 *La transformación λ de la Definición 12 es un epimorfismo de grupos. Además, $ker(\lambda) = \{\pm Id_{\mathscr{C}^n}\}$.*

Demostración. Dadas $g, h \in \mathscr{C}^n$, debido a la Proposición 3.0.12, sucede que para $z \in \hat{E}^n$, $[gh](z) = (gh)z = g(hz) = [g](hz) = [g][h](z)$, es decir,

$$\lambda(gh) = [gh] = [g][h] = \lambda(g)\lambda(h),$$

por lo que λ es un homomorfismo de grupos.

Por el recíproco dado en el Teorema 3.0.14, observamos que λ es suprayectiva y entonces es un epimorfismo.

Finalmente, si $g \in ker(\lambda)$, entonces $[g] = \lambda(g) = Id_{\hat{E}^n}$, es decir, para toda $z \in \hat{E}^n$ se tiene que $gz = z$. En particular, como $g(\infty) = \infty$, usando la notación de la Definición 10, se tiene que $c = 0$. También, $g(0) = 0$ implica que $bd^{-1} = 0$, por lo que debido al Lema 3.0.2, se tiene que $b = 0$.

En consecuencia de lo anterior, para cualquier $z \in E^n$ se tiene que $(az)d^{-1} = z$, y como $ad^* = 1$, se tiene que $d^{-1} = a^*$, por lo que para $z \in E^n$ se tiene que $aza^* = z$ y en particular, $|aza^*| = |z|$, pero por el Lema 3.0.10 tenemos que $|aza^*| = |a|^2|z|$, de manera que $|a| = 1$. Así, usando el Lema 3.0.13, tenemos que $d = (a^*)^{-1} = |a|^{-2}a' = a'$, lo que implica que

$$\forall z \in E^n \; az = za',$$

y por la Proposición 1.0.11, obtenemos que $a \in \mathbb{R}$. Como consecuencia, se tiene que $d = a = \pm 1$. Esto implica que $ker(\lambda) \subseteq \{\pm Id_{\mathscr{C}^n}\}$ y es claro que $\pm Id_{\mathscr{C}^n} \in ker(\lambda)$, por lo que concluimos que

$$ker(\lambda) = \{\pm Id_{\mathscr{C}^n}\}.$$

□

Proposición 3.0.16 $\lambda(\mathscr{C}^n_{par}) = SM(\hat{E}^n)$.

Demostración. Debido a la demostración del Teorema 3.0.14, sabemos que $\mathscr{C}^n$ está generado por las matrices

$$\begin{pmatrix} 1 & v \\ 0 & 1 \end{pmatrix} \in \mathscr{C}^n_{par} \; (v \in E^n),$$
$$\begin{pmatrix} r & 0 \\ 0 & r^{-1} \end{pmatrix} \in \mathscr{C}^n_{par} \; (r \in \mathbb{R}),$$
$$\begin{pmatrix} |a|^{-1}a & 0 \\ 0 & |a|^{-1}a' \end{pmatrix} \in \mathscr{C}^n_{par} \cup \mathscr{C}^n_{impar} \; (a \in \Gamma^n),$$
$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \mathscr{C}^n_{impar}.$$

Es por esto que, debido a las observaciones dadas antes de la Definición 10, se tiene que las matrices en $\mathscr{C}^n_{par}$ pueden escribirse como producto de matrices de las formas anteriores donde exactamente una cantidad par de ellas pertenece a $\mathscr{C}^n_{impar}$.

También sabemos que $M(\hat{E}^n)$ está generado por traslaciones (composición de dos reflexiones en planos), homotecias (composición de dos inversiones en esferas centradas en el origen), composición de reflexiones en hiperplanos y por la inversión respecto a la esfera unitaria. Notamos que, como las reflexiones en esferas o hiperplanos invierten la orientación, entonces las traslaciones,

homotecias y reflexiones en una cantidad par de hiperplanos son elementos de $SM(\hat{E}^n)$, mientras que las reflexiones en una cantidad impar de hiperplanos y la inversión respecto a la esfera unitaria no lo son. De manera que una transformación en $SM(\hat{E}^n)$ puede escribirse como composición de transformaciones de los tipos mencionados anteriormente, donde exactamente una cantidad par de ellas no pertenece a $SM(\hat{E}^n)$.

Por lo explicado anteriormente y como al aplicar λ a cada una de las matrices, obtenemos traslaciones, homotecias, composición de reflexiones en hiperplanos (una cantidad par si $a \in \Gamma^n_{par}$ y una cantidad impar si $a \in \Gamma^n_{impar}$, debido a la demostración del Teorema 1.0.13 y del Corolario 1.0.14) y la inversión en la esfera unitaria, se sigue entonces que $\lambda(\mathscr{C}^n_{par}) \subseteq SM(\hat{E}^n)$.

Por el mismo argumento mencionado en la demostración de la contención anterior y además usando que $ker(\lambda) = \{\pm Id_{\mathscr{C}^n}\}$ y el hecho de que $g \in \mathscr{C}^n_{par}$ si y sólo si $-g \in \mathscr{C}^n_{par}$, se tiene que $SM(\hat{E}^n) \subseteq \lambda(\mathscr{C}^n_{par})$. Con esto concluimos la demostración. □

Debido a las dos proposiciones anteriores obtenemos las siguientes sucesiones exactas cortas de grupos:

$$1 \hookrightarrow \{\pm 1\} \hookrightarrow \mathscr{C}^n \overset{\lambda}{\twoheadrightarrow} M(\hat{E}^n) \twoheadrightarrow 1,$$

$$1 \hookrightarrow \{\pm 1\} \hookrightarrow \mathscr{C}^n_{par} \overset{\lambda}{\twoheadrightarrow} SM(\hat{E}^n) \twoheadrightarrow 1.$$

Bibliografía

[1] Adams, C., *What is a Hyperbolic 3-Manifold?,* Volumen 65, 544-546.

[2] Ahlfors, L. V., *Möbius Transformations and Clifford Numbers, Differential Geometry and Complex Analysis,* Springer-Verlag, 1985.

[3] Ahlfors, L. V., *Möbius Transformations in* $\mathbb{R}^n$ *expressed through* $2x2$ *Matrices of Clifford Numbers,* Mathematics Department, Harvard University 1986.

[4] Beardon, A. F., *The Geometry of Discrete Groups,* Graduate Texts in Mathematics 91, Springer-Verlag, 1995.

[5] Lang, S., *Linear Algebra,* Addison Wesley, 1972.

[6] Porteous, I.R., *Topological Geometry,* Cambridge University Press, Segunda Edición, 1981.

[7] Vahlen, K.Th., Über Bewegungen und Complexe Zahln, *Math. Annalen*, 55, 585-593, 1902.

[8] Wada, M., *Conjugacy Invariants and Normal Forms of Isometries of Hyperbolic Space* Graduate School of Arts and Sciences, Columbia University, 3-26, 1986.

[9] Wada, M., *Conjugacy Invariants of Möbius Transformations* Department of Mathematics, University of Pennsylvania, 1990.