Representaciones de Weil del Grupo $SL_*(2, \mathbb{F}_q[x]/\langle x^m \rangle)$

Tesis
Entregada a la
Universidad de Chile
en cumplimiento parcial de los requisitos
para optar al grado de
Doctor en Ciencias con mención en Matemáticas
Facultad de Ciencias

por

Luis Cristian Gutiérrez Frez
Julio, 2006

Director de Tesis: Dr. José Pantoja Macari

FACULTAD DE CIENCIAS
UNIVERSIDAD DE CHILE

INFORME DE APROBACIÓN
TESIS DE DOCTORADO

Se informa a la Escuela de Postgrado de la Facultad de Ciencias que la Tesis de Doctorado presentada por el candidato

LUIS CRISTIAN GUTIÉRREZ FREZ

Ha sido aprobada por la comisión de Evaluación de la tesis como requisito para optar al grado de Doctor en Ciencias con mención en Matemáticas, en el examen de Defensa de Tesis rendido el día 3 de Julio de 2006.

Director de Tesis

Dr. José Pantoja Macari

Comisión de Evaluación de la Tesis

Dr. Eduardo Friedman (Presidente)

Dr. Roberto Aravire

Dr. Philip Kutzko
Representado por
Dr. Rodrigo Bamon

Agradecimientos

Al finalizar mis estudios de doctorado quiero agradecer a todos los que participaron en mi formación. En especial:

A los profesores guias de esta tesis; José Pantoja Macari y Jorge Soto Andrade por su paciencia y constante apoyo.

A Philip Kutzko, por las sesiones de trabajo que sostuvimos y por su gran disposición.

A mi esposa Teresa Castro, por su cariño y paciencia, a mi esposa, por compartir su alegria.

A mis padres, por su cariño y gran sacrificio. A mis padres; génesis de todos mis pasos.

A mis hermanos, por su ferrea confianza.

A mis compañero y amigos; Jaime Conejeros y Pablo Figueroa, por todo el apoyo en el transcurso del doctorado.

A mi amigo Cristian Reyes, por su amistad

A mis amigos Carolina Achiardi y Pablo Navarro, por la dedicación en la escritura de esta tesis.

A la comisión Nacional de Investigación en Ciencia y Tecnología, CONICY, por la beca otorgada en mis primeros cuatro años de doctorado.

Al Programa de Mejoramiento de la Calidad y la Equidad de la Educación Superio, Mecesup, por la beca de termino de tesis obtenida en mi quinto año de doctorado.

Abstract

Let A be a unitary ring with involution $*$. The groups $SL_*(2, A)$ were defined by J. Pantoja and J. Soto Andrade in [4]. These groups are a non-conmutative version of the special linear groups $SL(2, F)$, defined over a commutative base field F. In particular, if A is the full matrix ring $M(2, F)$ endowed with the trasposition as involution, then $SL_*(2, A)$ coincides with the symplectic group $Sp(2n, F)$ in $2n$ variables. In this thesis we study the truncated polinomial rings $A_m = \mathbb{F}_q[x]/\langle x^m \rangle)$ with k a finite field of odd characteritic p, for any positive integer m endowed with the natural involution given $x \mapsto -x$. These rings, reminiscent of algebras de m-jets, appear when m is a power of p, with a different involution as polinomial models for the non- semi-simple modular group algebras $k[C_m]$ over a base field of characteristic p, whose involution is given by inversion in the group. We obtain a full characterization of all the involutions in the ring A_m, for any m and the fact that there is only one isomorphism type of non trivial involutions in A_m. Moreover we obtain a representation of the $SL_*(2, A_m)$ in terms of the so called "Bruhat generator" and a complete set of relations among them. The order of the group $SL_*(2, A_m)$ is also calculated. Finally we construct a remarkable linear complex representation of the group $SL_*(2, A_m)$, for odd m, which generalizes the classical constructionof the Weil representation of the group $SL(2, F)$, defined over a finite base field F of odd characteristic, associated to a non degenerate quadratic space over F. A first decomposition of the Weil representation is indicated .

« Ella está en el horizonte. Me acerco dos pasos, ella se aleja dos pasos. Camino diez pasos y el horizonte se corre diez pasos más allá, por mucho que yo camino, nunca la alcanzaré. ¿Para qué sirve la utopía? Para eso sirve: para caminar. »

"Ventana sobre la utopía", Palabras andantes.
Eduardo Galeano.

Índice

Introducción **10**

1. Anillos involutivos **11**
1.1. Anillos Involutivos 11
1.2. Caracterización de las involuciones en $A_m = k[x]/\langle x^m \rangle$ 13

2. Sumas de Gauss sobre A-módulos cuadráticos **21**
2.1. Sumas de Gauss sobre cuerpos finitos 21
2.2. A-módulos cuadráticos no degenerados 27
2.3. Cálculo de la Suma de Gauss 30

3. El grupo $SL_*(2, A)$, $(A, *)$ anillo involutivo unitario **35**
3.1. Definición del grupo $SL_*(2, A)$. 35
3.1.1. Generadores de Bruhat para $SL_*(2, A)$ 37
3.2. Una presentación del grupo $SL_*(2, A_m)$ 37
3.2.1. El orden de $SL_*(2, A_m)$ 40

4. Representación de Weil de $SL_*(2, A_m)$ **43**
4.1. Preliminares
Representaciones lineales de grupos 43
4.2. Definición de la Representación de Weil de $SL_*(2, A_m)$ 45
4.3. Estructura del grupo ortogonal O(Q) 50
4.4. Descomposición de la Representación de Weil según $O(Q) \simeq \mathcal{U}_m$ 51

Bibliografia **53**

Introducción

Un fenómeno notable en la teoría de representaciones lineales de grupos es la existencia de una cierta representación del grupo $SL(2,F)$, donde F es un cuerpo localmente compacto, no discreto, o finito.

La construcción de esta representación aparece por primera vez, en forma explícita, en el artículo célebre "Sur certains groupes d'opérateurs unitaires" de André Weil [9], en el cual se construye más generalmente una representacion del grupo simpléctico $Sp(2n,F)$ en $2n$ variables. La construcción de A. Weil se apoya en la teoría de representaciones unitarias del grupo de Heisenberg $\mathcal{H}_n$ en n grados de libertad, descrita por el Teorema de Stone-von Neumann. De hecho, el grupo simpléctico $Sp(2n,F)$ actúa por automorfismos de grupos en el grupo de Heisenberg $\mathcal{H}_n$ y como éste posee esencialmente una sola representación unitaria irreductible de dimensión infinita (la representación de Schrödinger, en $L^2(\mathbb{R}^n)$ según el Teorema de Stone-von Neumann), entonces cada elemento de $Sp(2n,F)$ define un operador de entrelazamiento de esta representación dando así origen a una representación, proyectiva en general, de $Sp(2n,F)$ en el mismo espacio $L^2(\mathbb{R}^n)$ de la representación de Schrödinger. Esta representación se llama hoy día "representación de Weil" de $Sp(2n,F)$ en la literatura. Como caso particular se tiene, una representación de Weil para $Sp(2,F) = SL(2,F)$ en, $L^2(\mathbb{R})$.

P. Cartier observó en los años 70, que esta representación puede ser recuperada dando simplemente los operadores asociados a los generadores clásicos de $SL(2,F)$ y verificando que las relaciones de conmutación entre ellos son respetadas. Al proceder de esta manera, aparece claramente que los operadores de Weil están definidos a partir de la forma cuadrática $x \mapsto x^2$ en $\mathbb{R}$.

Más generalmente, es posible construir de este modo una " representación de Weil" para el grupo $SL(2,F)$ a partir de cualquier forma cuadrática no degenerada sobre F, con ayuda de la presentación bien conocida de $SL(2,F)$ a la Bruhat-Tits, definiendo operadores asociados a los generadores del grupo de modo que verifiquen las relaciones de conmutacion entre éstos.

Es un hecho notable que tomando un representante de cada tipo de isomorfía de formas cuadráticas de rango 2 sobre F y descomponiendo las representaciones de Weil asociadas, se obtiene en total todas las representaciones lineales unitarias irreducibles de $SL(2,F)$ (salvo que F sea un cuerpo 2-ádico). Se obtiene así un método uniforme y universal para construir todas las representaciones unitarias del grupo $SL(2,F)$.

Cabe señalar que J. Soto Andrade, en [7] extendió esta construcción al grupo $Sp(2n, F)$ mirándolo como un $SL(2)$ con coeficientes en el anillo de matrices $M(n, F)$ para obtener una nueva presentación de este grupo.

Así construyó las representaciones de Weil de $Sp(2n, F)$, asociadas a formas cuadráticas sobre un cuerpo de base F *finito* y obtuvo todas las representaciones irreductibles del grupo $Sp(4, F)$ al descomponer las representaciones de Weil asociadas a las 2 formas cuadraticas posibles de rango 4, a menos de isomorfía.

En forma natural, surge entonces la idea de reemplazar el cuerpo F por un anillo unitario A no necesariamente conmutativo y así definir un análogo "no conmutativo" de $SL(2, F)$. Para esto queremos definir una función determinante sobre $M(2, A)$ para un anillo A no conmutativo.

Ahora bien, J. Pantoja y J. Soto Andrade, en [5], consideran un anillo unitario A dotado de una involución $*$ y definen un $\det_*$ sobre el conjunto $M_*(2, A) \subset M(2, A)$ y luego $SL_*(2, A) = \{g \in M_*(2, A) : \det_*(g) = 1\}$. En el caso del anillo de matrices $A = M(n, F)$ dotado de la traspuesta como involución $*$ se tiene que $SL_*(2, A) = Sp(2n, F)$.

La introducción adecuada de un signo en la definición de los grupos anteriores y la elección de otros anillos involutivos permite recuperar otros grupos clásicos, como los grupos ortogonales, ver [8].

Por otra parte, se obtiene también ejemplos novedosos mediante la elección de anillos involutivos apropiados. Tal es el caso de esta tesis, donde se considera el caso de las álgebras de grupo no semi-simples, como anillos involutivos.

Los autores mencionados estudian el caso en que A es un anillo artiniano involutivo, demostrando la existencia de un conjunto de "generadores de Bruhat" para $SL_*(2, A)$ o de ciertos de sus subgrupos. Además el primer autor demuestra en [4] que los generadores mencionados, junto con ciertas relaciones "universales" determinan una presentación del grupo $SL_*(2, A)$.

El estudio de estos grupos es muy distinto, según sean semi-simples o no. En el primer caso, en particular para anillos simples artinianos involutivos se cuenta con teoremas de estructura como en [3] lo que puede permitir un estudio más sencillo de estos grupos, por el contrario, si los anillos involutivos considerados no son semi-simples, su estudio deviene en general más complicado.

Esta teoría resulta importante, entonces, pues, para comenzar, existe una gran variedad de anillos involutivos a considerar. Por ejemplo, las k-álgebras de grupo $k[G]$, dotada de la inversión en G como involución $*$. Una pregunta, interesante en sí misma, es qué grupo resulta ser $SL_*(2, k[G])$. Si k es un cuerpo finito, esta colección de anillos involutivos se divide según el teorema

de Maschke, en dos clases: semi-simples o no.

Ahora, si k es un cuerpo finito de característica p y si G es el grupo cíclico de orden p^n entonces el álgebra de grupo $k[G]$ es isomorfa a $k[x]/\left\langle x^{p^n}\right\rangle$. Este isomorfismo de anillos motiva el estudio de los anillos de polinomios "truncados" $k[x]/\langle x^m\rangle$. Podemos notar de inmediato que en $k[x]/\langle x^m\rangle$ el $k-$automorfimo de álgebras determinado por $x \mapsto -x$ es una involución. Preguntas naturales, por cierto, son: ¿Cómo son las involuciones en estos anillos y cuántos tipos de isomorfia de involuciones existen?.

En esta tesis consideramos, k es un cuerpo finito de característica impar,

$$A_m = k[x]/\langle x^m\rangle = \left\{ \sum_{i=0}^{m-1} a_i \overline{x}^i : a_i \in k, \overline{x}^m = 0 \right\}$$

y denotemos por $*$ a la involución ($k-$isomorfismo de álgebras de cuadrado la identidad) de A_m determinada por

$$* : \overline{x} \mapsto -\overline{x}.$$

Los objetivos de este trabajo son:

1. Determinar todos los tipos de isomorfía de involuciones en A_m.
2. Estudiar en estos casos, si el conjunto de generadores de Bruhat, introducido en 2 da una presentación de $SL_*(2, A_m)$.
3. Construir generalizaciones de las representaciones de Weil de $SL(2, F)$ para los grupos $SL_*(2, A_m)$.
4. Investigar además una primera descomposicion de las representaciones asi construidas.

Esta tesis esta dividida en cuatro capítulos;

En el capítulo 1, se presenta algunas nociones básicas sobre anillos involutivos y se obtiene el primer resultado de la tesis, en el cual se da una caracterización de las involuciones en el anillo de polinomios truncados A_m sobre un cuerpo de base k, finito, de característica impar. Además, en este mismo teorema, se establece la existencia de un solo tipo de isomorfía de involuciones no triviales en A_m. Por último, se obtiene el mismo resultado en el anillo de series formales $k[[x]]$.

En el capítulo 2, se presenta algunos resultados clásicos sobre sumas de Gauss sobre cuerpos finitos. También se da algunas nociones de A-módulos cuadráticos no degenerados, entre ellas, la definición de suma de Gauss de

un módulo cuadrático no degenerado. En la sección 2.3, se calcula la suma de Gauss $S_{\psi \circ Q}$ asociada al módulo cuadrático no degenerado (A_m, Q, B).

En el capitulo 3 se define el grupo $SL_*(2, A)$, donde A es un anillo unitario con una involución $*$. Se define también los generadores de Bruhat de $SL_*(2, A)$. Aquí se da (en el Teorema 5) una presentación de $SL_*(2, A_m)$, via los generadores de Bruhat y las relaciones universales entre ellos. También se calcula, en el Teorema 6 parte 2, el orden de $SL_*(2, A_m)$.

Finalmente, en el capítulo 4, se presenta algunas nociones de la teoría de representaciones lineales de grupos. Aquí se construye una representación lineal $(\mathbb{W}, \rho)$ de $SL_*(2, A_m)$ asociada al A_m-módulo cuadrático no degenerado (A_m, Q, B), que llamamos representación de Weil generalizada de $SL_*(2, A)$. Además se estudia el grupo ortogonal $O(Q)$ asociado a (A_m, Q, B) determinándose su estructura en ciertos casos. Este grupo actua en el espacio $\mathbb{W}$ de la representación de Weil, conmutando con la acción de ρ. Tal accion de $O(Q)$ permite en la sección 4.4 obtener una descomposición de la representación $(\mathbb{W}, \rho)$ de $SL_*(2, A_m)$.

Capítulo 1

Anillos involutivos

1.1. Anillos Involutivos

Definición 1. *Una involución* $* : a \mapsto a^*$ *en un anillo* A *es un anti-automorfismo de orden dos del anillo* A*, es decir, un automorfismo del grupo abeliano* A *tal que*

$$\begin{aligned} (ab)^* &= b^*a^*, \\ *^2 = * \circ * &= \mathrm{Id}_A\,. \end{aligned}$$

Diremos que una involución $*$ es no trivial en A, si $*$ no es el automorfismo identidad en A. Además, en ocasiones denotaremos $(A, *)$ al anillo A dotado de una involución $*$.

Ejemplo 1. *Consideremos el anillo* A *de matrices de orden* n *por* n *sobre el cuerpo* k*, y la involución dada por*

$$a^* = a^t, \text{ donde } a^t \text{ es la traspuesta de } a.$$

Entonces $(A, *)$ *es un anillo unitario involutivo.*

Ejemplo 2. *Sea* k *un cuerpo y* G *un grupo finito. Consideremos* $k[G]$ *el álgebra de grupo de* G *sobre* k*. Si definimos* $* : k[G] \to k[G]$ *mediante*

$$\left(\sum_{g\in G} a_g g\right)^* = \sum_{g\in G} a_g g^{-1}.$$

Se tiene que $(k[G], *)$ *es un anillo involutivo.*

Definición 2. *Sean $(A_1, *_1)$ y $(A_2, *_2)$ dos anillos involutivos. Diremos que $(A_1, *_1)$ es isomorfo a $(A_2, *_2)$ (y escribimos $(A_1, *_1) \cong (A_2, *_2)$) si existe un isomorfismo de anillos $\varphi : A_1 \to A_2$ tal que el siguiente diagrama*

$$\begin{array}{ccc} A_1 & \xrightarrow{\varphi} & A_2 \\ {\scriptstyle *_1}\downarrow & & \downarrow{\scriptstyle *_2} \\ A_1 & \xrightarrow{\varphi} & A_2 \end{array}$$

es conmutativo.

Proposición 1. *Sea k un cuerpo finito de característica p, $m = p^r$ y C_m el grupo cíclico de orden m. Entonces $k[C_m]$ dotado de la involución $*_1$ (k-automorfismo de álgebra) $g \mapsto g^{-1}$ es isomorfo a $A_m = k[x]/\langle x^m \rangle$ dotado de la involución $*_2$ ($k-$ automorfismo de álgebra) dado por $x \mapsto \frac{-x}{1-x}$.*

Demostración. Denotemos por g un generador del grupo C_m. Si

$$\begin{array}{rccc} \varphi & : & k[C_m] & \to & A_m \\ & & \sum_{i=0}^{m-1} a_i g^i & \mapsto & \sum_{i=0}^{m-1} a_i (1-x)^i. \end{array}$$

$$\begin{array}{rccc} \tilde{\varphi} & : & A_m & \to & k[C_m] \\ & & \sum_{i=0}^{m-1} a_i x^i & \mapsto & \sum_{i=0}^{m-1} a_i (1-g)^i, \end{array}$$

Entonces φ y $\tilde{\varphi}$ son k-homorfismos de álgebras. En efecto, de la definición es claro que φ y $\tilde{\varphi}$ son k-lineales. Veamos que φ y $\tilde{\varphi}$ respetan el producto. Basta verificar que φ y $\tilde{\varphi}$ respetan las relaciones sobre los generadores de estas álgebras,

$$\text{Como } g^m = 1, \text{ entonces } \varphi(g)^m = (1-x)^m = 1.$$
$$\text{Como } x^m = 0, \text{ entonces } \tilde{\varphi}(x)^m = (1-g)^m = 0$$

Así, φ y $\tilde{\varphi}$ son k-homorfismos de k-álgebras. Además, se tiene que

$$\begin{aligned} \tilde{\varphi} \circ \varphi &= \mathrm{Id}_{A_m}. \\ \varphi \circ \tilde{\varphi} &= \mathrm{Id}_{k[C_m]}. \end{aligned}$$

Por último se comprueba directamente que

$$\tilde{\varphi} \circ *_2 \circ \varphi(g) = g^{*_1}$$

De aquí la proposición. ∎

1.2. Caracterización de las involuciones en $A_m = k[x]/\langle x^m \rangle$

Sean $k = \mathbb{F}_q = \mathbb{F}_{p^n}$ el cuerpo finito de $q = p^n$ elementos, p primo impar y m un natural cualquiera. Sea

$$A_m = k[x]/\langle x^m \rangle \cong \left\{ \sum_{i=0}^{m-1} a_i \bar{x}^i : a_i \in k, \bar{x}^m = 0 \right\}.$$

En lo que sigue, denotaremos simplemente por x a $\bar{x}$, así el anillo A_m se presenta como

$$A_m = k[x]/\langle x^m \rangle \cong \left\{ \sum_{i=0}^{m-1} a_i x^i : a_i \in k, x^m = 0 \right\}.$$

Las involuciones que consideramos en A_m satisfacen

$$a^* = a, \text{ para todo } a \in k.$$

Notemos que como la k-álgebra A_m está generada por x, se tiene que todo endomorfismo $*$ de la k-álgebra A_m está determinada por la imagen que asigna a x. Un ejemplo de una involución no trivial en A_m está dada por:

$$* : x \mapsto x^* = -x.$$

El siguiente teorema, en 1, da una caracterización de las involuciones en A_m. En 2, se demuestra la existencia de un solo tipo de isomorfía de involuciones no triviales en A_m.

Teorema 1. *1. Sea $\tilde{*}$ una involución no trivial en A_m. Entonces*

$$x^{\tilde{*}} = \frac{-x}{1 + xq(x)} \tag{1.1}$$

$$\left(\sum_{i=0}^{m-1} a_i x^i \right)^{\tilde{*}} = \sum_{i=0}^{m-1} a_i x^{\tilde{*}i} \tag{1.2}$$

donde $q(x) \in A_m$ satisface $x^2 q(x) = x^2 q\left(\frac{-x}{1+xq(x)}\right)$ y recíprocamente, es decir, dado $q(x) \in A_m$ tal que $x^2 q(x) = x^2 q\left(\frac{-x}{1+xq(x)}\right)$ y definiendo $\tilde{*} : A_m \to A_m$ mediante (1.1) y (1.2), se tiene que $\tilde{*}$ es una involución en A_m.

2. *Toda involución no trivial de A_m es isomorfa a la involución $*$ determinada por*

$$* : x \mapsto x^* = -x.$$

Demostración.

1. Sea $\tilde{*}$ una involución en A_m. Escribamos

$$x^{\tilde{*}} = \sum_{i=1}^{m-1} a_i x^i.$$

Como $\tilde{*}^2 = \mathrm{Id}$, se tiene que $a_1^2 = 1$. Luego $a_1 = 1$ o bien $a_1 = -1$.

a) Si $a_1 = 1$, entonces $a_i = 0$, para todo $i = 2, 3, \ldots, m-1$. En efecto, procedamos por inducción sobre i. Para $i = 2$.

$$(x^{\tilde{*}})^{\tilde{*}} = x \text{ implica } 2a_2 = 0, \text{ así } a_2 = 0.$$

Supongamos ahora que $a_j = 0$ para $j = 1, ..., i$. Entonces

$$(x^{\tilde{*}})^{\tilde{*}} = x + 2a_{i+1}x^{i+1} + f_{i+2}(x),$$

donde $f_{i+2}(x) \in x_{i+2}A_m$ agrupa los términos de grado mayor o igual a $i+2$ en la expansión de $(x^{\tilde{*}})^{\tilde{*}}$. Por lo tanto $(x^{\tilde{*}})^{\tilde{*}} = x$ implica $a_{i+1} = 0$. De aquí $\tilde{*} = \mathrm{Id}_{A_m}$.

b) Si $a_1 = -1$, entonces

$$\begin{aligned} x^{\tilde{*}} &= -x + \sum_{i=2}^{m-1} a_i x^i \\ &= -x + x^2 h(x), \end{aligned}$$

donde $h(x) = \sum_{i=2}^{m-1} a_i x^{i-2}$. Como $1 - xh(x)$ es invertible, podemos tomar $q(x) \in A_m$ tal que $(1 - xh(x))(1 + xq(x)) = 1$. Por lo tanto

$$x^{\tilde{*}} = \frac{-x}{1 + xq(x)}.$$

Ahora, calculando $\tilde{*}^2$, se tiene que

$$
\begin{aligned}
(x^{\tilde{*}})^{\tilde{*}} &= \left(\frac{-x}{1+xq(x)}\right)^{\tilde{*}} \\
&= \frac{-x^{\tilde{*}}}{1+x^{\tilde{*}}q(x^{\tilde{*}})} \\
&= \frac{\frac{x}{1+xq(x)}}{\frac{1+xq(x)-xq\left(\frac{-x}{1+xq(x)}\right)}{1+xq(x)}} \\
&= \frac{x}{1+xq(x)-xq\left(\frac{-x}{1+xq(x)}\right)}.
\end{aligned}
$$

Así, $(x^{\tilde{*}})^{\tilde{*}} = x$ implica $x^2q(x) = x^2q\left(\frac{-x}{1+xq(x)}\right)$.

Recíprocamente, si $q(x) \in A_m$ satisface la relación anterior. Se define $\tilde{*} : A_m \to A_m$, mediante (1.1) y (1.2), es decir,

$$x^{\tilde{*}} = \frac{-x}{1+xq(x)}.$$

Se afirma que $\tilde{*}$ es una involución en A_m. En efecto

$$(x^{\tilde{*}})^{\tilde{*}} = \left(\frac{-x}{1+xq(x)}\right)^{\tilde{*}} = \frac{x}{1+xq(x)-xq\left(\frac{-x}{1+xq(x)}\right)}.$$

Por hipótesis, $q(x)$ satisface $x^2q(x) = x^2q\left(\frac{-x}{1+xq(x)}\right)$, luego $x = x + x^2q(x) - x^2q(1+xq(x))$. Reescribiendo la igualdad anterior, se tiene

$$\frac{x}{1+xq(x)-xq\left(\frac{-x}{1+xq(x)}\right)} = x.$$

De aquí se obtiene (1).

2. Sea $\tilde{*}$ una involución no trivial en A_m. Escribamos $x^{\tilde{*}} = -x + a_lx^l + h_{l+1}(x)$, donde $h_{l+1}(x) \in x^{l+1}A_m$. Entonces, se afirma que:

   - La primera potencia l de x, de $x^{\tilde{*}}$, es par.
   - Existe $f : A_m \to A_m$ automorfismo, tal que

   $$\left(f^{-1} \circ \tilde{*} \circ f\right)(x) = -x + a_{l+2}x^{l+2} + h_{l+3}(x)$$

   donde $h_{l+3}(x) \in x^{l+3}A_m$.

En efecto, para demostrar la primera afirmación, supongamos que l es impar, se tiene que

$$\begin{aligned}\left(x^{\tilde{*}}\right)^{\tilde{*}} &= \left(-x + a_l x^l + h_{l+1}(x)\right)^{\tilde{*}} \\ &= -x^{\tilde{*}} + a_l x^{\tilde{*}^l} + h_{l+1}^{\tilde{*}}(x) \\ &= -\left(-x + a_l x^l + h_{l+1}(x)\right) + a_l \left(-x + a_l x^l + h_{l+1}(x)\right)^l + h_l(x)^{\tilde{*}}.\end{aligned}$$

Si $\overline{h}_{l+1}(x)$ agrupa, en el segundo sumado de la expresión anterior, todos los polinomios de grado mayor o igual que $l+1$, entonces

$$\begin{aligned}\left(x^{\tilde{*}}\right)^{\tilde{*}} &= x - a_l x^l - h_{l+1}(x) - a_l x^l + a_l \overline{h}_{l+1}(x) + h_{l+1}^{\tilde{*}}(x) \\ &= x - 2a_l x^l + \left(a_l \overline{h}_{l+1}(x) + h_{l+1}^{\tilde{*}}(x) - h_{l+1}(x)\right).\end{aligned}$$

Luego $\left(x^{\tilde{*}}\right)^{\tilde{*}} \neq x$, pues $-2a_l \neq 0$ y $\left(a_l \overline{h}_{l+1}(x) + h_{l+1}^{\tilde{*}}(x) - h_{l+1}(x)\right)$ pertenece a $x^{l+1}A_m$, lo cual es una contradicción. Por lo tanto, l es par. Ahora, para demostrar a segunda afirmación, consideremos los siguientes isomorfismos (de k-álgebras) de A_m dados por

$$\begin{aligned}f(x) &= x - \frac{a_l}{2}x^l \\ f^{-1}(x) &= x + \frac{a_l}{2}x^l + t_{l+1}(x),\ t_{l+1}(x) \in x^{l+1}A_m\end{aligned}$$

Así, se tiene que

$$\begin{aligned}\left(f^{-1} \circ \tilde{*} \circ f\right)(x) &= \left(f^{-1} \circ \tilde{*}\right)\left(x - \frac{a_l}{2}x^l\right) \\ &= f^{-1}\left(x^{\tilde{*}} - \frac{a_l}{2}x^{\tilde{*}^l}\right) \\ &= f^{-1}\left(-x + a_l x^l + h_{l+1}(x) - \frac{a_l}{2}\left(-x + a_l x^l + h_{l+1}(x)\right)^l\right).\end{aligned}$$

Si $\tilde{t}_{l+1}(x)$ agrupa, en el argumento de f^{-1}, de la expresión anterior, todos los polinomios de grado mayor o igual que $l+1$, entonces

$$\begin{aligned}\left(f^{-1} \circ \tilde{*} \circ f\right)(x) &= f^{-1}\left(-x + \frac{a_l}{2}x^l + \tilde{t}_{l+1}(x)\right) \\ &= -f^{-1}(x) + \frac{a_l}{2}f^{-1}(x)^l + f^{-1}\left(\tilde{t}_{l+1}(x)\right) \\ &= -\left(x + \frac{a_l}{2}x^l + t_{l+1}(x)\right) + \frac{a_l}{2}\left(x + \frac{a_l}{2}x^l + t_{l+1}(x)\right)^l + f^{-1}\left(\tilde{t}_{l+1}(x)\right).\end{aligned}$$

Si $\tilde{h}_{l+1}(x)$ agrupa, en la expresión anterior, todos los polinomios de grado mayor o igual a $l+1$, entonces

$$\left(f^{-1} \circ \tilde{*} \circ f\right)(x) = -x + \tilde{h}_{l+1}(x).$$

De la primera observación, se tiene que $\tilde{h}_{l+1}(x) \in x^{l+2}A_m$, pues $f^{-1} \circ * \circ f$ es una involución. Por lo tanto

$$\left(f^{-1} \circ \tilde{*} \circ f\right)(x) = -x + a_{l+2}x^l + h_{l+2}(x),$$

donde $\tilde{h}_{l+1}(x) = a_{l+2}x^l + h_{l+2}(x)$, luego procediendo inductivamente, se obtiene, finalmente un automorfismo $f : A_m \to A_m$, tal que

$$\left(f^{-1} \circ \tilde{*} \circ f\right)(x) = -x.$$

De aquí, toda involución no trivial de A_m es isomorfa a la involución dada por $x \to -x$.

■

Caso del anillo de las series formales $k[[x]]$

Cabe señalar que el resultado anterior también es válido en el anillo de series formales $k[[x]]$. Para establecer la validez de tal afirmación, comencemos estudiando los k-automorfismos en $k[[x]]$. Sea $g(x) \in k[[x]]$ y consideremos la siguiente función

$$\begin{array}{rccl} \varphi_g & : & k[[x]] & \to k[[x]] \\ & : & f & \mapsto \varphi_g(f) = f \circ g. \end{array}$$

Entonces φ_g es un k-homomorfismo de $k[[x]]$. Con estas notaciones, se tiene el siguiente

Lema 1. *Un k-homorfismo φ de $k[[x]]$ es un k-isomorfismo si y sólo si existe una serie formal $g(x) \in xk[[x]]$, $g(x) \notin x^2k[[x]]$ tal que $\varphi = \varphi_g$.*

Demostración. Sea φ un k-isomorfismo de $k[[x]]$. Sea $g(x) = \varphi(x)$ y $f(x) = \sum_{i=0}^{\infty} b_i x^i$

una serie formal arbitraria. Así

$$\begin{aligned}\varphi(f)(x) &= \varphi\left(\sum_{i=0}^{\infty} b_i x^i\right)\\ &= \sum_{i=0}^{\infty} b_i \varphi(x)^i\\ &= \sum_{i=0}^{\infty} b_i g(x)^i\\ &= \varphi_g(f)(x).\end{aligned}$$

Además, como φ es un isomorfismo de $k[[x]]$, explicitando $(\varphi \circ \varphi)(x) = x$ se obtiene que $g(x) = \varphi(x) \in xk[[x]]$ y que $g(x) = \varphi(x) \notin x^2k[[x]]$. Recíprocamente, sea $g(x) \in xk[[x]]$ y $g(x) \notin x^2k[[x]]$. Escribamos

$$g(x) = \sum_{i=1}^{\infty} a_i x^i,\ a_1 \neq 0.$$

Directamente de la definición, se tiene que φ_g es un k-homorfismo de k[[x]]. Además, escribiendo en forma explícita $\varphi_g(f_1) = \varphi_g(f_2)$ se concluye que $f_1 = f_2$, es decir, φ_g es inyectiva. Por otro lado se tiene que

$$\text{existe } h(x) \in k[[x]] \text{ tal que } (g \circ h)(x) = x \text{ si y sólo si } a_1 \neq 0,$$

pues $\left\{\sum_{i=0}^{\infty} a_i x^i :\ a \neq 0\right\}$ es, de hecho, un grupo bajo composición. Entonces tenemos que $(g \circ h)(x) = (h \circ g)(x) = x$. Luego $\varphi_g \circ \varphi_h = \varphi_h \circ \varphi_g = \mathrm{Id}$. De aquí el lema ■

Ahora estamos en condiciones de demostrar el siguiente

Teorema 2. *1. Sea $\tilde{*}$ una involución no trivial en $k[[x]]$. Entonces*

$$x^{\tilde{*}} = \frac{-x}{1 + xq(x)} \tag{1.3}$$

$$\left(\sum_{i=0}^{\infty} a_i x^i\right)^{\tilde{*}} = \sum_{i=0}^{\infty} a_i x^{\tilde{*}^i} \tag{1.4}$$

donde $q(x) \in k[[x]]$ satisface $x^2q(x) = x^2q\left(\frac{-x}{1+xq(x)}\right)$ y recíprocamente, es decir, dado $q(x) \in k[[x]]$ tal que $x^2q(x) = x^2q\left(\frac{-x}{1+xq(x)}\right)$, y definiendo $\tilde{*} : k[[x]] \to k[[x]]$ mediante (1.3) y (1.4), se tiene que $\tilde{*}$ es una involución en $k[[x]]$.

2. *Toda involución no trivial de $k[[x]]$ es isomorfa a la involución $\bar{*}$ determinada por*

$$\bar{*} : x \mapsto x^{\bar{*}} = \frac{-x}{1-x}.$$

Demostración.

1. Se procede como en 1 del Teorema 1.

2. A diferencia de la parte 2 del Teorema 1, podemos aquí, establecer explícitamente un isomorfismo entre una involución no trivial $\tilde{*}$ y la involución dada por $\bar{*}$. Sea $\tilde{*}$ una involución no trivial en $k[[x]]$, entonces por (1), existe $q(x) \in k[[x]]$ tal que,

$$x^{\tilde{*}} = \frac{-x}{1+xq(x)},$$

con $q(x)$ satisfaciendo la relación anterior. Definamos el k-homomorfimo $\varphi : k[[x]] \to k[[x]]$ mediante $\varphi(\sum a_i x^i) = \sum a_i(\varphi(x))^i$, donde $\varphi(x) = \frac{2x}{2+xq(x)+x}$.

Del lema 1, tenemos que φ es un k-automorfismo de $k[[x]]$. Además se afirma que φ satisface

$$\varphi\left(\frac{-x}{1-x}\right) = (\varphi(x))^{\tilde{*}}.$$

En efecto

$$\begin{aligned}
\varphi\left(\frac{-x}{1-x}\right) &= \frac{-\varphi(x)}{1-\varphi(x)} \\
&= \frac{-\frac{2x}{2+xq(x)+x}}{1-\frac{2x}{2+xq(x)+x}} \\
&= \frac{-2x}{2+xq(x)-x}.
\end{aligned}$$

Por otra parte

$$\begin{aligned}
(\varphi(x))^{\tilde{*}} &= \left(\frac{2x}{2+xq(x)+x}\right)^{\tilde{*}} \\
&= \frac{2x^{\tilde{*}}}{2+x^{\tilde{*}}q(x^{\tilde{*}})+x^{\tilde{*}}} \\
&= \frac{2\frac{-x}{1+xq(x)}}{2+\left(\frac{-x}{1+xq(x)}\right)q\left(\frac{-x}{1+xq(x)}\right)+\left(\frac{-x}{1+xq(x)}\right)} \\
&= \frac{-2x}{2+xq(x)-x}.
\end{aligned}$$

Lo que demuestra el teorema.

■

Observación 1. *Es importante señalar que se podría haber tomado un punto de vista diferente al aquí tratado. Explícitamente, se podría haber demostrado primero el teorema de clasificación y tipo de isomorfía en el anillo de series formales $k[[x]]$, de aquí haber observado que toda involución $*$ en $k[[x]]$ provee una involución $\tilde{*}$ en A_m y que toda involución $\tilde{*}$ en A_m puede ser extendida a una involución $*$ en $k[[x]]$, tal que el siguiente diagrama*

$$\begin{array}{ccc} k[[x]] & \xrightarrow{*} & k[[x]] \\ {\scriptstyle pr}\downarrow & & \downarrow{\scriptstyle pr} \\ A_m & \xrightarrow{\tilde{*}} & A_m \end{array}$$

es conmutativo. De aquí, entonces, haber obtenido el teorema 1. Sin embargo, este punto de vista no fue considerado, pues el interés estaba centrado en estudiar anillos involutivos finitos. No obstante, tal punto de vista puede ser, en un futuro próximo, investigado en relación a ver si los resultados en esta tesis obtenidos, siguen siendo válidos al considerar el anillo involutivo de las series formales $k[[x]]$.

Capítulo 2

Sumas de Gauss sobre A-módulos cuadráticos

2.1. Sumas de Gauss sobre cuerpos finitos

Definición 3. *Sea k un cuerpo finito de $q = p^n$ elementos, ψ un carácter de k^+ y (V, Q) un espacio cuadrático de dimensión finita sobre k. Se define la suma de Gauss $S_{\psi \circ Q}$ asociada a ψ y a Q por*

$$S_{\psi \circ Q} = \sum_{v \in V} \psi(Q(v)) \in \mathbb{C}.$$

Un resultado importante en la teoría de formas cuadráticas sobre un cuerpo finito k (ver, por ejemplo, [2]), es la existencia de, exactamente, dos formas cuadráticas no degeneradas no isomorfas de rango dos sobre k, a saber:

- En k^2 se define la forma cuadrática (no degenerada)$(x, y) \mapsto xy$, llamada usualmente forma cuadrática hiperbólica o isótropa, que anotaremos, con cierto abuso de notación, por (k^2, xy).
- Sea K la única extensión cuadrática de k y N es la norma de la extensión K sobre k llamada forma cuadrática anisótropa, que anotaremos con cierto abuso de notación, por (K, N).

Con estas notaciones, se tiene el siguiente

Teorema 3. *Sea k un cuerpo finito de característica p impar y ψ un carácter no trivial de k^+. Entonces*

1. $S_{\psi \circ xy} = q$.

2. $S_{\psi \circ N} = -q$.

Demostración. Ver [7], proposición 2, (iii) y (iv).

Lema 2. *Sea ψ un carácter no trivial de k^+ y (V,Q), (V',Q') espacios cuadráticos de dimensión finita sobre k.*

1. *Si $(V,Q) \simeq (V',Q')$ entonces $S_{\psi \circ Q} = S_{\psi \circ Q'}$.*

2. *Si (V,Q) es no degenerado, se tiene que el módulo $|S_{\psi \circ Q}|$ de $S_{\psi \circ Q}$ es $|V|^{\frac{1}{2}}$.*

3. *Para el espacio cuadrático k con la forma cuadrática $x \mapsto x^2$, se tiene que*

$$S_{\psi \circ tx^2} = \alpha(t) S_{\psi \circ x^2}, \text{ para todo } t \in k^\times,$$

donde α es el carácter "signo" en $k^\times$, es decir,

$$\begin{array}{rccl} \alpha: & k^\times & \to & \mathbb{C} \\ & t & \mapsto & \alpha(t) = \begin{cases} 1 & t \in k^{\times 2} \\ -1 & t \notin k^{\times 2}. \end{cases} \end{array}$$

Demostración. 1. Como $(V,Q) \simeq (V',Q')$ existe un isomorfismo $\varphi : V \to V'$ tal que

$$Q'(\varphi(v)) = Q(v), \text{ para todo } v \in V.$$

Así

$$\begin{aligned} S_{\psi \circ Q} &= \sum_{v \in V} \psi(Q(v)) \\ &= \sum_{v \in V} \psi(Q'(\varphi(v))) \\ &= \sum_{v' \in V'} \psi(Q'(v')) \\ &= S_{\psi \circ Q'}. \end{aligned}$$

2. Sea B la forma bilineal asociada a la forma cuadrática Q sobre V, es decir, la forma bilineal B tal que

$$B(x,y) = Q(x+y) - Q(x) - Q(y), \text{ donde } x, y \in V.$$

Calculemos $|S_{\psi \circ Q}|^2$.

$$\begin{aligned} |S_{\psi \circ Q}|^2 &= \Big(\sum_{v \in V} \psi(Q(v))\Big) \cdot \overline{\Big(\sum_{w \in V} \psi(Q(w))\Big)} \\ &= \sum_{v \in V} \sum_{w \in V} \psi(Q(v) - Q(w)) \end{aligned}$$

Si $w = z - v$, entonces

$$|S_{\psi \circ Q}|^2 = \sum_{z \in V} \psi(-Q(z)) \sum_{v \in V} \psi(B(v,z)).$$

Como la forma B es no degenerada, se tiene que para todo $z \neq 0$;

$$\sum_{v \in V} \psi(B(v,z)) = 0.$$

Por lo tanto

$$\begin{aligned} |S_{\psi \circ Q}|^2 &= \sum_{z \in V} \psi(-Q(z)) \sum_{v \in V} \psi(B(v,z)) \\ &= \sum_{v \in V} \psi(-Q(0)) \psi(B(v,0)) \\ &= |V|. \end{aligned}$$

Así

$$|S_{\psi \circ Q}| = |V|^{\frac{1}{2}}.$$

3. Sea $t \in k^\times$. Se distingue dos casos

   a) Si $t = c^2$, $c \in k^\times$, entonces

$$\begin{aligned} S_{\psi \circ t x^2} &= \sum_{y \in k} \psi(t y^2) \\ &= \sum_{y \in k} \psi((cy)^2) \\ &= \sum_{\tilde{y} \in k} \psi(\tilde{y}^2) \\ &= S_{\psi \circ x^2}. \end{aligned}$$

b) En el caso en que t es un no cuadrado, notemos que se tiene

$$S_{\psi o x^2} + S_{\psi o t x^2} = 2 \sum_{y \in k} \psi(y) = 0.$$

Por lo tanto $S_{\psi o t x^2} = -S_{\psi o x^2} = \alpha(t) S_{\psi o t x^2}$. De aquí el teorema.

■

Observación 2. *Se obtiene, de la parte 3 del lema anterior, que*

$$\alpha(t) = \frac{S_{\psi o t x^2}}{S_{\psi o x^2}}, \quad \textit{para todo } t \in k^{\times}.$$

En general, si (V, Q) es un espacio cuadrático no degenerado sobre k, entonces la aplicación de k en $\mathbb{C}$ dada por $t \mapsto \frac{S_{\psi o t Q}}{S_{\psi o Q}}$ es el carácter trivial o el carácter signo de k. Para verificar esta afirmación se distinguen dos casos:

- *Si (V, Q) es de rango par, entonces $Q \simeq tQ$. Así, de la parte 1, del lema anterior, se tiene que la aplicación es el carácter trivial en k.*
- *Ahora, si (V, Q) es de rango impar, digamos $2n + 1$, entonces*

  $$V = (U, \tilde{Q}) \oplus (k, rx^2),$$

  donde $(U, \tilde{Q})$ es la suma de n espacios cuadráticos de rango 2 y $\oplus$ es suma directa ortogonal . Así,$(U, t\tilde{Q}) \simeq (U, \tilde{Q})$, para $t \in k^{\times}$. Luego

  $$\frac{S_{\psi o t Q}}{S_{\psi o Q}} = \frac{S_{\psi o t \tilde{Q}} \cdot S_{\psi o t r x^2}}{S_{\psi o \tilde{Q}} \cdot S_{\psi o r x^2}} = \frac{S_{\psi o t r x^2}}{S_{\psi o r x^2}} = \alpha(t).$$

  Por lo tanto, en este caso la aplicación es el carácter signo en k

De aqui la afirmación

Lema 3. *Sea (V, Q) un espacio cuadrático no degenerado de dimensión n sobre el cuerpo finito k. Entonces*

$$\frac{S_{\psi o Q}^2}{|V|} = \alpha(-1)^n.$$

Demostración. Demostraremos el lema nuevamente para el espacio cuadrático (k, rx^2). De la parte 3 del lema anterior, tenemos que

$$S_{\psi \circ rx^2} = \alpha(r) S_{\psi \circ x^2}.$$

De donde

$$S^2_{\psi \circ rx^2} = S^2_{\psi \circ x^2}.$$

Por lo tanto, basta demostrar la igualdad para el espacio cuadrático (k, x^2). Así

$$\begin{aligned} S^2_{\psi \circ x^2} &= \Big(\sum_{x \in k} \psi(x^2)\Big)\Big(\sum_{y \in k} \psi(y^2)\Big) \\ &= \sum_{x \in k} \sum_{y \in k} \psi(x^2)\psi(y^2) \\ &= \sum_{(x,y) \in k^2} \psi(x^2 + y^2). \end{aligned}$$

Notemos que $(k^2, x^2 + y^2)$ es un plano cuadrático no degenerado, luego

$$(k^2, x^2 + y^2) \cong (k^2, x \cdot y) \text{ o bien } (k^2, x^2 + y^2) \cong (K, N).$$

- Si -1 es un cuadrado en k, entonces

$$(k^2, x^2 + y^2) \cong (k^2, x \cdot y).$$

Así, de la parte 1 del lema 2 y el teorema 3, parte 1 , se tiene que

$$S^2_{\psi \circ x^2} = S_{\psi \circ xy} = q.$$

Por lo tanto

$$\frac{S^2_{\psi \circ x^2}}{|k|} = 1 = \alpha(-1).$$

- Por otro lado, si -1 no es un cuadrado, entonces

$$(k^2, x^2 + y^2) \cong (K, N).$$

Usando la parte 1 del lema 2 y teorema 3, parte 2, se tiene que

$$S_{\psi \circ x^2} = S_{\psi \circ N} = -q.$$

Por lo tanto,

$$\frac{S^2_{\psi \circ x^2}}{|k|} = -1 = \alpha(-1).$$

Ahora, dado (V, Q) un espacio cuadrático no degenerado arbitrario, se distingue dos casos;

1. Si (V, Q) es de rango $2n$, entonces (V, Q) es suma de espacios cuadráticos de rango dos. Por lo tanto, usando partes 1 y 2 del teorema 3 se tiene que $S_{\psi \circ Q} = \pm q^n$. Así

$$\frac{S^2_{\psi \circ Q}}{|V|} = 1 = \alpha(-1)^{2n}.$$

2. Por otro lado, si (V, Q) es de rango $2n + 1$, entonces

$$(V, Q) \simeq (k, rx^2) \oplus (U, Q'),$$

donde (U, Q') es un espacio cuadrático no degenerado de rango par. Así, $S_{\psi \circ Q} = S_{\psi \circ rx^2} \cdot S_{\psi \circ Q'}$. Por lo tanto

$$\begin{aligned} \frac{S^2_{\psi \circ Q}}{|V|} &= \frac{S^2_{\psi \circ rx^2} \cdot S^2_{\psi \circ Q'}}{|V|} \\ &= \frac{S^2_{\psi \circ rx^2}}{k} \\ &= \alpha(-1) \\ &= \alpha(-1)^{2n+1}. \end{aligned}$$

■

2.2. A-módulos cuadráticos no degenerados

Definición 4. *Sea $(A,*)$ un anillo involutivo y M un A-módulo derecho. Diremos que (M,Q,B) es un A-módulo cuadrático si $Q : M \to A$ es función y $B : M \times M \to A$ es una A-forma bi-aditiva tal que*

$$\begin{aligned} Q(ma) &= a^*Q(m)a \\ B(m,n) &= Q(m+n) - Q(m) - Q(n) \\ B(ma,n) &= B(m,na^*) \\ B(m,n) &= B(n,m)^* \\ B(ma,n) &= a^*B(m,n), \end{aligned}$$

para todo $m,n \in M$ y para todo $a \in A$.

Definición 5. *Diremos que una A-forma B es no degenerada si se cumple que:*

Si $B(m,n) = 0$ para todo $m \in M$, entonces $n = 0$.

Definición 6. *Diremos que el A-módulo cuadrático es no degenerado, si la A-forma B es no degenerada.*

Definición 7. *Sea (M,Q,B) un A-módulo cuadrático no degenerado. Se define el grupo ortogonal $O(Q)$, como el grupo de los isomorfismos A-lineales $\varphi : M \to M$ tales que*

$$Q(\varphi(a)) = Q(a), \text{ para todo } a \in A.$$

Definición 8. *Sea (M,Q,B) un A-módulo cuadrático no degenerado y sea θ un caracter no trivial de A^+ tal que $\theta(ab) = \theta(ba)$, para todo $a,b \in A$. La suma de Gauss $S_{\theta \circ Q}$ asociada a Q y θ está definida por:*

$$S_{\theta \circ Q}(a) = \sum_{x \in M} \theta(aQ(x)) .$$

Notación 1. *En todo lo que sigue, anotamos $S_{\theta \circ aQ} = \sum_{x \in M} \theta(aQ(x))$.*

Lema 4. *Sea (M,Q,B) un A-módulo cuadrático no degenerado y sea θ un caracter no trivial de A^+ tal que $\theta(ab) = \theta(ba)$, para todo $a,b \in A$. Entonces*

1. *Si $t \in A$ invertible, entonces*

$$S_{\theta \circ aQ} = S_{\theta \circ tat^* Q},$$

para todo $a \in A$.

2. *Si $t \in A$ invertible, entonces*

$$S_{\theta o tQ} = S_{\theta o t^{*-1} Q}.$$

Demostración.

1. En efecto,

$$\begin{aligned} S_{\theta o tat^* Q} &= \sum_{m \in M} \theta(tat^* Q(m)) \\ &= \sum_{m \in M} \theta(at^* Q(m)t) \\ &= \sum_{m' \in M} \theta(aQ(m')) = S_{\theta o aQ}. \end{aligned}$$

2. En efecto,

$$\begin{aligned} S_{\theta o tQ} &= \sum_{m \in M} \theta(tQ(m)) \\ &= \sum_{m' \in M} \theta(tQ(t^{-1}m')) \\ &= \sum_{m' \in M} \theta(tt^{*-1} Q(m')t^{-1}) \\ &= \sum_{m' \in M} \theta(t^{*-1} Q(m')) \\ &= S_{\theta o t^{*-1} Q}. \end{aligned}$$

■

Definición 9. *Un morfismo entre dos A-módulos cuadráticos no degenerados (M_1, Q_1, B_1) y (M_2, Q_2, B_2) es una función $f : M_1 \to M_2$ A-lineal tal que $Q_2 \circ f = Q_1$.*

La clase de todos los A-módulos cuadráticos no degenerados junto con todos los morfismos entre ellos, forma una categoría. La siguiente proposición se verifica de manera inmediata.

Proposición 2. *Sean $(A_1, *_1)$ y $(A_2, *_2)$ anillos involutivos isomorfos. Entonces la categoría de los A_1-módulos cuadráticos no degenerados es isomorfa a la categoría de los A_2-módulos cuadráticos no degenerados.*
□

Consideramos en lo que sigue (A_m, Q, B) el A_m-módulo cuadrático no degenerado, donde $Q : A_m \to A_m$ está definido mediante

$$Q(t(x)) = t^*(x)t(x)$$

y la forma $B : A_m \times A_m \to A_m$ dada por

$$B(t(x), s(x)) = t(x)^* s(x) + t(x)s(x)^*.$$

Definición 10. *Denotemos por* tr *la aplicación de* A_m *en* k *definida por*

$$\mathrm{tr}\left(\sum_{i=0}^{m-1} a_i x^i\right) = a_{m-1}.$$

Lema 5. *La función* tr *es* k*-lineal. Si* m *es un número impar, entonces la función* tr *es invariante por la involución* $*$*, es decir*

$$\mathrm{tr}(t(x)^*) = \mathrm{tr}(t(x)).$$

Demostración. La función tr es, claramente, k-lineal. Recordemos que la involución $*$ está dada por $x^* = -x$, luego si $t(x) = \sum_{i=0}^{m-1} a_i x^i \in A_m$, entonces

$$\mathrm{tr}(t(x)^*) = \mathrm{tr}\left(\sum_{i=0}^{m-1} (-1)^i a_i x^i\right) = a_{m-1} = \mathrm{tr}(t(x)).$$

Por lo tanto, la función tr es invariante por la involución $*$.

■

Lema 6. *Si* m *es un número impar, entonces, la* k*-forma* $\mathrm{tr} \circ B$ *es una forma bilineal simétrica no degenerada.*

Demostración. De la definición de B y $*$, es claro que $\mathrm{tr} \circ B$ es bilineal simétrica, para ver que es no degenerada, notemos que

$$\begin{aligned} \mathrm{tr} \circ B(t(x), s(x)) &= \mathrm{tr}(t(x)^* s(x) + t(x)s(x)^*) \\ &= \mathrm{tr}(t(x)^* s(x)) + \mathrm{tr}(t(x)^* s(x)) \\ &= 2\,\mathrm{tr}(t(x)^* s(x)), \end{aligned}$$

Así, basta demostrar que la k-forma $\widetilde{B} : (t(x), s(x)) \mapsto \mathrm{tr}(t(x)^* s(x))$ es no degenerada. Sea pues $t(x) \in \ker(\widetilde{B})$. Escribamos

$$t(x)^* = \sum_{i=0}^{m-1} a_i x^i.$$

Consideremos $s_j(x) = x^{m-j}$, $j = 1, 2, \ldots, m$. Por lo tanto, $\mathrm{tr}(t^*(x)s_j(x)) = 0$ para todo $j = 1, 2, \ldots, m$. Por otra parte

$$\mathrm{tr}\left(\sum_{i=0}^{m-1} a_i x^i s_j(x)\right) = a_{j-1}.$$

Así se obtiene que $a_{j-1} = 0$, para todo $j = 1, 2, \ldots, m$. Por lo tanto $t^*(x) = 0$, así $t(x) = 0$. De aquí, $\tilde{B}$ es no degenerada. Luego el lema.

■

Del lema anterior, se deduce inmediatamente el siguiente

Lema 7. *Si m es un número impar, entonces el A_m-módulo cuadrático (A_m, Q, B) es no degenerado.*
□

2.3. Cálculo de la Suma de Gauss

Recordemos que la involución $*$ dada por $x \mapsto -x$ y $tr\left(\sum_{i=0}^{m-1} a_i x^i\right) = a_{m-1}$. Sean m un número impar, digamos $m = 2s + 1$, ψ un caracter aditivo no trivial de k y $\underline{\psi} = \psi \circ tr$. A continuación calculamos la suma de Gauss $S_{\underline{\psi} \circ Q}$ asociada al A_m-módulo cuadrático no degenerado (a_m, Q, B). Sea $a = a_0 + a_1 x + \cdots + a_{m-1} x^{m-1}$ en $A_m^\times$. Entonces

$$\begin{aligned} \mathrm{tr}(aa^*) &= a_0 a_{m-1} + \cdots + (-1)^j a_j a_{m-1-j} + \cdots + a_{m-1} a_0 \\ &= \sum_{i=0}^{s-1} 2(-1)^j a_j a_{m-1-j} + (-1)^s a_s^2 \end{aligned}$$

Luego

$$\sum_{a \in A_m} \psi\left(\mathrm{tr}(a^* a)\right) = \sum_{a_0, a_{m-1}} \psi^2\left(a_0 a_{m-1}\right) \sum_{a_1, a_{m-2}} \psi^2\left(a_1 a_{m-2}\right) \cdots \sum_{a_{s-1}, a_{s+1}} \psi\left(a_{s-1} a_{s+1}\right) \sum_{a_s} \psi^2\left(a_s^2\right),$$

donde los a_j y a_{m-1-j} recorren todo k en la cada una de las sumas anteriores. Por lo tanto, usando el teorema 3 se tiene que

$$S_{\underline{\psi} \circ Q} = \sum_{a \in A_m} \psi\left(\mathrm{tr}(a^* a)\right) = q^s \sum_{a_s \in k} \psi^2\left(a_s^2\right).$$

Así el valor la suma de Gauss $S_{\psi \circ Q}$ queda completamente determinada por el valor de la suma de Gauss clásica $\sum_{a_s \in k} \psi^2\left(a_s^2\right)$.

Lema 8. *Para el anillo involutivo $(A_m, *)$ se cumple*

1. *El orden del grupo $A_m^{\times}$ de las unidades de A_m es $(q-1)q^{m-1}$.*
2. *El orden del conjunto A_m^s de elementos simétricos bajo $*$ es $q^{[\frac{m+1}{2}]}$.*
3. *El orden de $A_m^{\times} \cap A_m^s$ es $(q-1)q^{[\frac{m-1}{2}]}$.*

Demostración.

1. Sea $f(x) = \sum_{i=0}^{m-1} a_i x^i \in A_m$. Como $\sum_{i=1}^{m-1} a_i x^i$ es nilpotente en A_m, se tiene que $f(x)$ es unidad si y sólo si $a_0 \neq 0$. De aquí 1.
2. Sea $f(x) = \sum_{i=0}^{m-1} a_i x^i \in A_m$. Entonces

$$f(x)^* = \sum_{i=0}^{m-1} (-1)^i a_i x^i.$$

   Por lo tanto $f(x) = f(x)^*$ si y sólo si $a_i = 0$, para todo i impar con $0 < i \leq m-1$. Así, se tiene 2.
3. De 1 y 2 se tiene de inmediato que

$$\left|A_m^{\times} \cap A_m^s\right| = (q-1)q^{[\frac{m-1}{2}]}.$$

■

Teorema 4. *Un elemento $a = \sum_{i=0}^{m-1} a_i x^i$ es un cuadrado en A_m si y sólo si a_0 es un cuadrado en k.*

Demostración. Notemos que si a es un cuadrado en A_m, entonces es inmediato que a_0 es un cuadrado en k. Recíprocamente, sea $a = \sum_{i=0}^{m-1} a_i x^i \in A_m$ tal que a_0 es un cuadrado en k. Queremos encontrar $b = \sum_{i=0}^{m-1} b_i x^i$, tal que $b^2 = a$. Para ello, notemos que el siguiente sistema de ecuaciones en los b_i

$$\begin{aligned}
b_0^2 &= a_0 \\
b_0 b_1 + b_1 b_0 &= a_1 \\
b_0 b_2 + b_1 b_1 + b_2 b_0 &= a_2 \\
&\vdots \\
b_0 b_i + b_1 b_{i-1} + \cdots + b_{i-1} b_1 + b_i b_0 &= a_i \\
&\vdots \\
b_0 b_{m-1} + b_1 b_{m-2} + \cdots + b_{m-1} b_0 &= a_{m-1},
\end{aligned}$$

tiene solución, procediendo inductivamente. Así, considerando $b = \sum_{i=0}^{m-1} b_i x^i$, se tiene entonces que $b^2 = a$. De aquí el teorema. ■

Proposición 3. *Hagamos actuar el grupo $A_m^\times$ sobre $(A_m^\times \cap A_m^s)$, mediante*

$$\begin{aligned} A_m^\times \times (A_m^\times \cap A_m^s) &\to A_m^\times \cap A_m^s \\ (t(x), s(x)) &\mapsto t(x)s(x)t(x)^* , \end{aligned}$$

entonces la acción tiene exactamente dos órbitas.

Demostración. Para comenzar estudiemos la órbita $\mathrm{Orb}_{A_m^\times}(1)$.

$$\begin{aligned} \mathrm{Orb}_{A_m^\times}(1) &= \left\{a^*a \ : \ a \in A_m^\times\right\} \\ &= \left\{\left(\sum_{i=0}^{m-1}(-1)^i a_i x^i\right)\left(\sum_{i=0}^{m-1} a_i x^i\right) \ : \ a = \sum_{i=0}^{m-1} a_i x^i \in A_m^\times\right\}. \quad (2.1) \end{aligned}$$

Se afirma que

$$\mathrm{Orb}_{A_m^\times}(1) = \left\{a_0 + \sum_{i=1}^{[\frac{m-1}{2}]} a_{2i}x^{2i} \ : \ a_0 \in (k^\times)^2, \ a_{2i} \in k\right\}.$$

En efecto, de (2.1) el término constante de a^*a es un cuadrado (no nulo) en k. Además, como a^*a es un elemento simétrico en A_m, a^*a no tiene términos de grado impar, luego

$$\mathrm{Orb}_{A_m^\times}(1) \subseteq \left\{a_0 + \sum_{i=1}^{[\frac{m-1}{2}]} a_{2i}x^{2i} \ : \ a_0 \in (k^\times)^2, \ a_{2i} \in k\right\}.$$

Por otra parte, dado $a = a_0 + \sum_{i=1}^{[\frac{m-1}{2}]} a_{2i}x^{2i}$ con $a_0 \in (k^\times)^2$, podemos encontrar $b = b_0 + \sum_{i=1}^{[\frac{m-1}{2}]} b_{2i}x^{2i}$ (procediendo como en el Teorema 4) tal que $a = b^2 = b^* \cdot b$, así $a \in \mathrm{Orb}_{A_m^\times}(1)$. Por lo tanto

$$\mathrm{Orb}_{A_m^\times}(1) = \left\{a_0 + \sum_{i=1}^{[\frac{m-1}{2}]} a_{2i}x^{2i} \ : \ a_0 \in (k^\times)^2, \ a_{2i} \in k\right\}.$$

Ahora, si $d \in k$ es un no cuadrado, entonces $d \notin \mathrm{Orb}_{A_m^\times}(1)$. Se afirma que las órbitas $\mathrm{Orb}_{A_m^\times}(1)$ y $\mathrm{Orb}_{A_m^\times}(d)$ son las únicas órbitas de esta acción. Debido a que el anillo A_m es conmutativo, se tiene que $\mathrm{Stab}_{A^\times}(1) = \mathrm{Stab}_{A^\times}(d)$. Así las órbitas $\mathrm{Orb}_{A_m^\times}(1)$ y $\mathrm{Orb}_{A_m^\times}(d)$ tienen la misma cardinalidad, es decir,

$$|\mathrm{Orb}_{A_m^\times}(d)| = |\mathrm{Orb}_{A_m^\times}(1)| = \Big(\frac{q-1}{2}\Big)q^{[\frac{m-1}{2}]}.$$

Por lo que

$$|\mathrm{Orb}_{A_m^\times}(1)| + |\mathrm{Orb}_{A_m^\times}(d)| = |A_m^\times \cap A_m^s|\,.$$

Por lo tanto, las únicas órbitas que deja esta acción, son $\mathrm{Orb}_{A_m^\times}(1)$ y $\mathrm{Orb}_{A_m^\times}(d)$. De aquí la proposición. ■

Corolario 1. *El orden del estabilizador* $\mathrm{Stab}_{A_m^\times}(1)$ *de* 1 *es* $2q^{[\frac{m-1}{2}]}$.

Demostración. De la demostración de la proposición 3 se tiene que

$$|\mathrm{Orb}_{A_m^\times}(1)| = \Big(\frac{q-1}{2}\Big)q^{[\frac{m-1}{2}]}.$$

Por lo tanto

$$\begin{aligned} |\mathrm{Stab}_{A_m^\times}(1)| &= \frac{|A_m^\times|}{|\mathrm{Orb}_{A_m^\times}(1)|} \\ &= 2q^{[\frac{m-1}{2}]}. \end{aligned}$$

■

Corolario 2. *La función*

$$\begin{aligned} \alpha : A_m^\times &\to \mathbb{C} \\ t &\mapsto \alpha(t) = \frac{S_{\underline{\psi} o tQ}}{S_{\underline{\psi} o Q}} \end{aligned}$$

es el carácter signo del grupo $A_m^\times$.

Demostración.

- Si t es un cuadrado en $A_m^\times$, entonces t pertenece a la órbita $\mathrm{Orb}_{A_m^\times}(1)$ de la acción de $A_m^\times$ en $A_m^\times \cap A_m^s$, dada en la proposición 3. Así $ata^* = 1$, para algún en $a \in A_m^\times$. Luego, usando el lema 4, capítulo 2, se tiene que se tiene $S_{\underline{\psi} o tQ} = S_{\underline{\psi} o\, ata^* Q} = S_{\underline{\psi} o\, Q}$. Por lo tanto $\alpha(t) = 1$.
- Por otro lado, si t es un no cuadrado, argumentando como antes, t pertenece a la órbita $\mathrm{Orb}_{A_m^\times}(d)$, con $d \in k$ un no cuadrado, así existe $a \in A_m^\times$ tal que $ata^* = d$. Luego

$$S_{\underline{\psi} o tQ} = S_{\underline{\psi} o ata^* Q} = S_{\underline{\psi} o dQ} = S_{\underline{\psi} o\, d\,\mathrm{tr}\, o Q}.$$

De la observación 2, se tiene que

$$S_{\underline{\psi} \circ d\mathrm{tr} \circ Q} = -S_{\underline{\Psi} \circ Q}.$$

Por lo tanto, $\alpha(t) = -1$.

■

Capítulo 3

El grupo $SL_*(2, A)$, $(A, *)$ anillo involutivo unitario

3.1. Definición del grupo $SL_*(2, A)$.

Sea A un anillo unitario provisto de una involución $a \mapsto a^*$. Se define una involución en $M(2, A)$ (que denotaremos $T \mapsto T^*$), mediante $(T^*)_{ij} = (T_{ji})^*$. Sea $M_*(2, A)$ el conjunto de todas las matrices g en $M(2, A)$ tal que $g^* J g J^{-1} = \lambda_g I_2$, con $\lambda_g \in Z(A)$ e I_2 es la matriz identidad en $M(2, A)$, $J = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \in M(2, A)$ y $Z(A)$ es el centro de A. Notemos que $M_*(2, A)$ es cerrado bajo multiplicación matricial.

Definición 11. *Sea $GL_*(2, A)$ el conjunto de elementos invertibles de $M_*(2, A)$.*

Definición 12. *En $M_*(2, A)$ se define* $\det_*(g) = ad^* - bc^*$, *para* $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_*(2, A)$. *Entonces* $\det_* g = \lambda_g$.

Sea $SL_*(2, A)$ el conjunto de matrices g en $M_*(2, A)$ tales que $\det_*(g) = 1$.

En el siguiente lema, $Z_s(A)^\times$ denota el conjunto de los elementos simétricos invertibles del anillo A.

Lema 9. *$GL_*(2, A)$ es un grupo bajo multiplicación matricial,* $\det_*$ *es un epimorfismo de $GL_*(2, A)$ en $Z_s(A)^\times$ y* $\ker(\det_*) = SL_*(2, A)$.

Demostración. Ver [5], Lema 15. ■

A continuación, damos algunos ejemplos de $SL_*(2, A)$ para ciertos anillos involutivos.

Ejemplo 3. *Consideremos el siguiente anillo involutivo*

$$\begin{aligned} A &= M(n,k) \\ a^* &= a^t, \end{aligned}$$

donde a^t *denota la traspuesta de* a. *Entonces*

$$SL_*(2,A) = Sp(2n,k).$$

Ejemplo 4. *Sea* k *cuerpo,* $n = 2m$ *e* I_m *la matriz identidad en* $M(m,k)$. *Entonces podemos considerar la forma alternada* B, *sobre el espacio de vectores columna* k^n, *dada por*

$$B(v,w) = v^t \begin{pmatrix} 0 & I_m \\ -I_m & 0 \end{pmatrix} w,$$

Si $*$ *denota la adjunta respecto a* B, *entonces*

$$SL_*(2,A) = O(C),$$

donde

$$\begin{aligned} A &= M(n,k), \\ C(v,w) &= v^t \begin{pmatrix} 0 & 0 & 0 & I_m \\ 0 & 0 & -I_m & 0 \\ 0 & -I_m & 0 & 0 \\ I_m & 0 & 0 & 0 \end{pmatrix} w, \end{aligned}$$

y $O(C)$ *el grupo de isometrías de la forma bilineal simétrica* C.

Lema 10. *Sean* $(A_1, *_1)$ *y* $(A_2, *_2)$ *anillos involutivos isomorfos. Entonces*

$$SL_{*_1}(2,A_1) \simeq SL_{*_2}(2,A_2)\,.$$

Demostración. Por hipótesis, existe un isomorfismo de anillos $\varphi : (A_1, *_1) \to (A_2, *_2)$ tal que $\varphi(a_1^{*_1}) = \varphi(a_1)^{*_2}$, para todo $a_1 \in A_1$. Entonces, definimos

$$\begin{array}{rccc} \widetilde{\varphi}: & SL_{*_1}(2,A_1) & \to & SL_{*_2}(2,A_2) \\ & \begin{pmatrix} a & b \\ c & d \end{pmatrix} & \mapsto & \begin{pmatrix} \varphi(a) & \varphi(b) \\ \varphi(c) & \varphi(d) \end{pmatrix} \end{array}$$

Se verifica directamente que $\widetilde{\varphi}$ es un isomorfismo de grupos. ■

3.1.1. Generadores de Bruhat para $SL_*(2, A)$

Sea A un anillo con identidad provisto de una involución $*$. Sean

$$h(t) = \begin{pmatrix} t & 0 \\ 0 & t^{*^{-1}} \end{pmatrix}, \quad u(b) = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}, \quad w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

El conjunto de matrices $h(t)$, $t \in A^\times$, $u(b)$, $b \in A^s$, w es llamado el conjunto de generadores de Bruhat para $SL_*(2, A)$. Las matrices $h(t)$, $u(b)$ y w satisfacen las siguientes relaciones "universales"

$$\begin{aligned} h(t_1)h(t_2) &= h(t_1t_2) \\ u(b_1)u(b_2) &= u(b_1 + b_2) \\ h(t)u(b) &= u(tbt^*)h(t) \\ w^2 &= h(-1) \\ wh(t) &= h(t^{*^{-1}})w \\ u(t)wu(t^{-1})wu(t) &= wh(-t^{-1}). \end{aligned}$$

Sean

$$\begin{aligned} B &= \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in SL_*(2, A) \right\}, \\ D &= \{h(t) \in B : t \in A^\times\}, \\ N &= \{u(b) \in B : b \in A^s\}. \end{aligned}$$

Se tiene que B, D, N son subgrupos de $SL_*(2, A)$ y $B = DN$.

3.2. Una presentación del grupo $SL_*(2, A_m)$

Para establecer que los generadores de Bruhat y sus relaciones determinan una presentación del grupo seguiremos los pasos que son usados por J. Pantoja en [4]. Los siguientes dos lemas establecen hechos que se cumplen de manera inmediata en los anillos A_m.

Lema 11. *Sean $a, c \in A_m$ tales que a o c son invertibles y $a^*c = c^*a$. Entonces existe $s \in A_m^s$ tal que $a + sc \in A_m^\times$.* □

Lema 12. *Si $a, b \in A_m^s$ son no invertibles, entonces existe $x \in A_m^\times \cap A_m^s$ tal que $a - x^{-1}$ y $b + x$ son simétricos invertibles.* □

Lema 13. *El grupo $SL_*(2, A_m)$ es generado por el conjunto de generadores de Bruhat.*

Demostración. Sea $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_*(2, A_m)$. Si $c = 0$, entonces $g = h(a)u(a^{-1}b)$. Si c es invertible, entonces $g = h(-c^{*^{-1}})u(c^*a)wu(c^{-1}d)$. Por ultimo, si $c \notin A_m \cup \{0\}$, entonces a y c cumplen con las hipótesis del lema 11, así sea $s \in A_m^s$ tal que $a + sc \in A_m^\times$. Luego tenemos que

$$g = u(-s)h(-a - sc)wu(-a^* - c^*s)wu((a + sc)^{-1}(b + sd))$$

■

Lema 14. *En el grupo $SL_*(2, A_m)$ se cumple*

1. *Si $h(t)u(a)wu(b)wu(c) = 1$, entonces $t = -1$, $a = -c$ y $b = 0$.*

2. *1 no pertenece a BwB.*

3. *Si $h(t)u(a) = 1$, entonces $t = 1$ y $a = 0$.*

Demostración. Supongamos que $h(t)u(a)wu(b)wu(c) = 1$. por lo tanto $h(t)u(a)w = -u(-c)wu(-b)$, asi explicitando esta igualdad se tiene 1. Por ultimo, un cálculo directo muestra 2 y 3. ■

Definición 13. *Sea H el grupo abstracto generado por los objetos $h(t), u(b)$ y w con $t \in A^\times$, $b \in A^s$ sujeto a las relaciones*

$$\begin{aligned} h(t_1)h(t_2) &= h(t_1t_2) \\ u(b_1)u(b_2) &= u(b_1 + b_2) \\ h(t)u(b) &= u(tbt^*)h(t) \\ w^2 &= h(-1) \\ wh(t) &= h(t^{*^{-1}})w \\ u(t)wu(t^{-1})wu(t) &= wh(-t^{-1}). \end{aligned}$$

Observación 3. *En lo que sigue, usaremos los misms símbolos $h(t), u(b)$ y w para denotar matrices en $SL_*(2, A_m)$ o elementos en H, los cuales son parametrizados por elementos en el anillo A_m. Al igual que en el grupo $SL_*(2, A)$, denotemos por B el subgrupo de H generado por los elementos $h(t)$ y $u(b)$, con $t \in A_m^\times, b \in A_m^s$.*

Definición 14. *El w-largo de un elemento $g \in H$ es el menor entero positivo j tal que $g \in (BwB)^j$, donde $B^0 = B$. Análogamente, se define el w-largo de un elemento $g \in SL_*(2, A_m)$.*

Lema 15. *En el grupo H, todo elemento tiene a w-largo a lo más 2.*

Demostración. Sea $g_1g_2t = g_3t'$, para $g_i \in BwB$, $i = 1,2,3$ y t, t' son elementos arbitrarios de H. Usando las relaciones que definen a H, esta expresión es equivalente a $wu(a)wt'' = u(b)w$, para algun $t'' \in H$. Para demostrar este lema, demostraremos que esta expresión es equivalente a una que envuelve un w menos.

Si a o bien b son invertibles, entonces, sin pérdida de generalidad, supongamos que a es invertible. Luego usando la relación $wu(t^{-1})wu(t)wu(t^{-1}) = h(t)$ para $t = a$ se tiene que $wu(a)w = -u(-a^{-1})wh(a)u(-a^{-1})$. Así $wu(b) = wu(a)wt'' = -u(-a^{-1})wh(a)u(-a^{-1})t''$.

Por otra parte, si a y b son no invertibles, entonces usando el lema 11, existe $x \in A_m^{\times} \cap A_m^s$ tal que $a - x^{-1}, b + x \in A_m^{\times}$. Luego multiplicando $wu(a)wt'' = u(b)w$ por $u(x)$, se tiene que $u(x)wu(a)wt'' = u(b+x)w$. Trabajando con las relaciones que definen a H se tiene

$$\begin{aligned}
u(x)wu(a)wt'' &= -w(wu(x)w)u(a)wt'' \\
&= -w(-u(-x^{-1})wh(x)u(-x^{-1}))u(a)wt'' \\
&= wu(-x^{-1})wh(x)u(-x^{-1}+a)wt'' \\
&= wu(-x^{-1})h(x^{-1})wu(-x^{-1}+a)wt'' \\
&= wu(-x^{-1})h(x^{-1})(u(-(a-x^{-1})^{-1})wh(a-x^{-1})u(-(a-x^{-1})^{-1}w)wt'' \\
&= -wu(-x^{-1})h(x^{-1})u(-(a-x^{-1})^{-1})wh(a-x^{-1})u(-(a-x^{-1})^{-1}t''.
\end{aligned}$$

Luego

$$wu(b+x)w = u(-x^{-1})h(x^{-1})u(-(a-x^{-1})^{-1})wh(a-x^{-1})u(-(a-x^{-1})^{-1}t''.$$

Usando nuevamente $wu(t^{-1})wu(t)wu(t^{-1}) = h(t)$, para $t = b + x$ tenemos que $wu(b+x)w = -u(-(b+x)^{-1})wh(b+x)u(-(b+x)^{-1})$. Por lo tanto la ecuación original se reduce a

$$-u(-(b+x)^{-1})wh(b+x)u(-(b+x)^{-1}) = u(-x^{-1})h(x^{-1})u(-(a-x^{-1})^{-1})wh(a-x^{-1})u(-(a-x^{-1})^{-1}t''.$$

Así la expresión equivalente envuelve un w menos. Por último, el resultado sigue por inducción sobre el w-largo de los elementos en H. ■

Finalmente podemos establecer el siguiente

Teorema 5. *El conjunto de generadores de Bruhat*

$$h(t) = \begin{pmatrix} t & 0 \\ 0 & t^{*^{-1}} \end{pmatrix}, \quad u(b) = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}, \quad w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Con $t \in A_m^{\times}$ y $b \in A_m^s$ junto con las relaciones

$$\begin{aligned} h(t_1)h(t_2) &= h(t_1t_2) && (3.1)\\ u(b_1)u(b_2) &= u(b_1+b_2) && (3.2)\\ h(t)u(b) &= u(tbt^*)h(t) && (3.3)\\ w^2 &= h(-1) && (3.4)\\ wh(t) &= h(t^{*^{-1}})w && (3.5)\\ u(t)wu(t^{-1})wu(t) &= wh(-t^{-1}) && (3.6) \end{aligned}$$

determina una presentación para $SL_*(2, A_m)$.

Demostración. Notemos de inmediato que, usando el lema 13, la función natural $\varphi : H \to SL_*(2, A)$ es un epimorfismo. Por lo tanto, solo debemos demostrar que φ es inyectiva. Por lema 15 todo elemento de H es de una de las siguientes formas; $h(t)u(a)$, $h(t)u(a)wu(b)$, o bien $h(t)u(a)wu(b)wu(c)$. Ahora, del lema 14 se tiene que $\varphi(g) = 1$, implica $g = 1$. De aquí el teorema ■

3.2.1. El orden de $SL_*(2, A_m)$

Teorema 6. *Si $SL_*(2, A_m)$ actúa en $A_m \times A_m$ mediante multiplicación a la izquierda sobre $M_{2\times 1}(A_m)$, entonces*

1. *La cardinalidad $\left|\mathrm{Orb}_{\mathrm{SL_*(2,A_m)}}\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)\right|$ es $(q-1)q^{m+[\frac{m+1}{2}]-2}(q+1)$.*
2. *La cardinalidad $|SL_*(2, A_m)|$ es $(q-1)q^{m+2[\frac{m+1}{2}]-2}(q+1)$.*

Demostración.

1. De la definición, se tiene que

$$\mathrm{Orb}_{\mathrm{SL_*(2,A_m)}}\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right) = \left\{\left(\begin{smallmatrix}a\\c\end{smallmatrix}\right) : \left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right) \in SL_*(2, A)\right\}.$$

   Luego, si $\left(\begin{smallmatrix}a\\c\end{smallmatrix}\right) \in \mathrm{Orb}_{\mathrm{SL_*(2,A_m)}}\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)$, así se tiene que $a \in A_m^{\times}$ o bien $c \in A_m^{\times}$. Entonces, definamos

$$\begin{aligned} O_1 &= \left\{\left(\begin{smallmatrix}a\\c\end{smallmatrix}\right) : \left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right) \in SL_*(2, A), a \in A_m^{\times}\right\}.\\ O_2 &= \left\{\left(\begin{smallmatrix}a\\c\end{smallmatrix}\right) : \left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right) \in SL_*(2, A), a \notin A_m^{\times}\right\}. \end{aligned}$$

Por lo tanto,

$$\mathrm{Orb}_{\mathrm{SL}_*(2,\mathrm{A_m})}\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right) = O_1 \cup O_2.$$

Además estos dos últimos conjuntos son disjuntos, así la cardinalidad $\left|\mathrm{Orb}_{\mathrm{SL}_*(2,\mathrm{A_m})}\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)\right|$ es $|O_1| + |O_2|$. Para calcular tales cardinalidades, notemos lo siguiente:

- Sea $\left(\begin{smallmatrix}a\\c\end{smallmatrix}\right) \in O_1$. Como $\left(\begin{smallmatrix}a\\c\end{smallmatrix}\right)$ es primera columna de una matriz en $SL_*(2, A_m)$, se tiene que $a^*c = c^*a$. Luego $(\frac{c}{a})^* = \frac{c}{a}$, es decir, $\frac{c}{a}$ es simétrico en A_m. Así $c = ua$, $u \in A_m^s$. Por lo tanto,

  $$O_1 \subseteq \left\{\left(\begin{smallmatrix}a\\ua\end{smallmatrix}\right) : a \in A_m^\times,\ u \in A_m^s\right\}.$$

  Por otro lado, para todo $a \in A_m^\times$ y $u \in A_m^s$, se tiene que $\left(\begin{smallmatrix}a\\ua\end{smallmatrix}\right) \in \mathrm{Orb}_{\mathrm{SL}_*(2,\mathrm{A_m})}\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)$. En efecto,

  $$\begin{pmatrix} a & 0 \\ ua & a^{*-1} \end{pmatrix} \in SL_*(2, A_m)$$

  $$\begin{pmatrix} a & 0 \\ ua & a^{*-1} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ ua \end{pmatrix}.$$

  Así

  $$O_1 = \left\{\left(\begin{smallmatrix}a\\ua\end{smallmatrix}\right) : a \in A_m^\times,\ u \in A_m^s\right\}.$$

- Por último, sea $\left(\begin{smallmatrix}a\\c\end{smallmatrix}\right) \in O_2$. Como $\left(\begin{smallmatrix}a\\c\end{smallmatrix}\right)$ es primera columna de una matriz en $SL_*(2, A_m)$, se tiene que $a^*c = c^*a$. Luego $(\frac{a}{c})^* = \frac{a}{c}$, es decir, $\frac{a}{c}$ es simétrico en A_m. Así $a = uc$, donde $u \in A_m^s - A_m^\times$. Por lo tanto

  $$O_2 \subseteq \left\{\left(\begin{smallmatrix}uc\\c\end{smallmatrix}\right) : c \in A_m^\times,\ u \in A_m^s - A_m^\times\right\}.$$

  Por otra parte, para todo $c \in A_m^\times$ y $u \in A_m^s - A_m^\times$, se afirma que

  $$\left(\begin{smallmatrix}uc\\c\end{smallmatrix}\right) \in \mathrm{Orb}_{\mathrm{SL}_*(2,\mathrm{A_m})}\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right).$$

  En efecto,

  $$\begin{pmatrix} uc & -c^{*-1} \\ c & 0 \end{pmatrix} \in SL_*(2, A_m),$$

  $$\begin{pmatrix} uc & -c^{*-1} \\ c & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} uc \\ c \end{pmatrix}.$$

  Así $O_2 = \left\{\left(\begin{smallmatrix}uc\\c\end{smallmatrix}\right) : c \in A_m^\times,\ u \in A_m^s - A_m^\times\right\}$.

De lo anterior, tenemos que

$$\begin{aligned} |O_1| &= \left|\left\{\binom{a}{ua} : a \in A_m^{\times},\ u \in A_m^s\right\}\right| \\ &= (q-1)q^{m-1}q^{[\frac{m+1}{2}]} \\ &= (q-1)q^{m+[\frac{m+1}{2}]-1}. \end{aligned}$$

$$\begin{aligned} |O_2| &= \left|\left\{\binom{uc}{c} : c \in A_m^{\times},\ u \in A_m^s - A_m^{\times}\right\}\right| \\ &= (q-1)q^{m-1}q^{[\frac{m+1}{2}]-1} \\ &= (q-1)q^{m+[\frac{m+1}{2}]-2}. \end{aligned}$$

Por lo tanto,

$$\begin{aligned} |\mathrm{Orb}_{\mathrm{SL}_*(2,\mathrm{A_m})}\binom{1}{0}| &= |O_1| + |O_2| \\ &= (q-1)q^{m+[\frac{m+1}{2}]-1} + (q-1)q^{m+[\frac{m+1}{2}]-2} \\ &= (q-1)q^{m+[\frac{m+1}{2}]-2}(q+1). \end{aligned}$$

2. Notemos que

$$|SL_*(2,A_m)| = |\mathrm{Orb}_{\mathrm{SL}_*(2,\mathrm{A_m})}\binom{1}{0}| \cdot |\mathrm{Stab}_{\mathrm{SL}_*(2,\mathrm{A_m})}\binom{1}{0}|.$$

Así, en virtud de 1, basta saber la cardinalidad del estabilizador $\mathrm{Stab}_{\mathrm{SL}_*(2,\mathrm{A_m})}\binom{1}{0}$.

$$\begin{aligned} \mathrm{Stab}_{\mathrm{SL}_*(2,\mathrm{A_m})}\binom{1}{0} &= \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_*(2,A) : \begin{pmatrix} a & b \\ c & d \end{pmatrix}\binom{1}{0} = \binom{1}{0}\right\} \\ &= \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_*(2,A) : \binom{a}{c} = \binom{1}{0}\right\} \\ &= \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_*(2,A) : a = 1,\ c = 0\right\} \\ &= \left\{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in A_m^s\right\}. \end{aligned}$$

Por lo tanto,

$$\begin{aligned} |SL_*(2,A_m)| &= (q-1)q^{m+[\frac{m+1}{2}]-2}(q+1)q^{[\frac{m+1}{2}]} \\ &= (q-1)q^{m+2[\frac{m+1}{2}]-2}(q+1). \end{aligned}$$

Así, la demostración está completa.

■

Capítulo 4

Representación de Weil de $SL_*(2, A_m)$

4.1. Preliminares
Representaciones lineales de grupos

Definición 15. *Sea G un grupo. Diremos que el par (V, ρ) es una representación lineal (compleja) de G si V es un espacio vectorial complejo y ρ es un homomorfismo de G en el grupo de automorfismos lineales $Aut_{\mathbb{C}}(V)$. Denotemos por $\rho(g) = \rho_g$ la imagen de g mediante ρ.*

En ocasiones, el par (V, ρ) será denotado sólo por ρ o sólo por V. Además diremos que la representación (V, p) tiene dimensión finita n o es de grado n, si la dimensión del espacio vectorial V es n.

Ejemplo 5. *Un ejemplo importante de representaciones lineales de un grupo finito G se tiene cuando G actúa a la izquierda sobre un conjunto finito X por $(g, x) \mapsto g \cdot x$ $(x \in X, g \in G)$. Entonces se puede construir una representación (V, π) de G, definiendo $V = \mathbb{C}^X$ (el espacio de funciones de X en $\mathbb{C}$) y definiendo la acción π mediante*

$$\pi(g)(f)(x) = f(g^{-1}x).$$

La representación lineal (V, π) de G se llama representación natural de G asociada a la acción de G sobre X.

Definición 16. *Sea (V, ρ) una representación lineal de G. Se dice que (V, ρ) es una representación reducible si existe un subespacio W de V, no nulo y distinto de V, tal que*

$$\rho(g)(W) \subset W, \text{ para todo } g \in G.$$

En tal caso, el par (W, ρ_W), donde ρ_W está definido por $\rho_W(g) = \rho_g|_W$ para todo $g \in G$, es, en sí misma, una representación de G, denominada subrepresentación de (V, ρ). Por otra parte, se dice que el par (V, ρ) es una representación irreducible si (V, ρ) es no reducible.

Definición 17. *Sean (V, ρ) y (U, π) dos representaciones de G. Una función lineal f de V en U es un operador de entrelazamiento (o un G-homomorfismo) entre ρ y π si para todo g, el siguiente diagrama*

$$\begin{array}{ccc} V & \xrightarrow{f} & U \\ {\scriptstyle \rho_g}\downarrow & & \downarrow{\scriptstyle \pi_g} \\ V & \xrightarrow{f} & U \end{array}$$

es conmutativo.

El espacio de todos los operadores de entrelazamientos entre ρ y π será denotado por $\mathrm{Hom}_G(\rho, \pi)$.

Definición 18. *Un carácter (lineal) ψ del grupo G es una representación lineal de G de dimensión 1. Diremos que el caracter ψ es trivial en G si $\psi(g) = 1$, para todo $g \in G$.*

Teorema 7 (Teorema de Maschke). *Sea $k[G]$ el álgebra de grupo de un grupo finito G sobre un cuerpo k, entonces $k[G]$ es semisimple si y sólo si, la característica de k no divide al orden $|G|$ del grupo G.*

Demostración. Ver, por ejemplo, [1], proposición 5.8, capítulo 9.

Definición 19. *Diremos que (V, ρ) es isomorfa a (U, π) (y anotaremos $(V, \rho) \simeq (U, \pi)$) si existe un operador de entrelazamiento biyectivo entre ρ y π.*

Lema 16 (Lema de Schur). *Sean (V, ρ) y (U, π) dos representaciones lineales de G y f un operador de entrelazamiento entre ρ y π. Entonces*

1. *Si $(V, \rho) \not\simeq (U, \pi)$, entonces $f \equiv 0$.*
2. *Si $V = U$ y $\rho = \pi$, se tiene que f es una homotecia.*

Demostración. Ver, por ejemplo, [6], proposición 4, capítulo 2.

4.2. Definición de la Representación de Weil de $SL_*(2, A_m)$

Como antes, $k = \mathbb{F}_q$ el cuerpo finito de $q = p^n$ elementos, p primo impar, m un número impar,

$$A_m = \left\{ \sum_{i=0}^{m-1} a_i x^i : a_i \in k,\ x^m = 0 \right\},$$

con la involución $*$ dada por $x \mapsto -x$ y la traza $\mathrm{tr} : A_m$ en k dada por

$$\mathrm{tr}\left(\sum_{i=0}^{m-1} a_i x^i \right) = a_{m-1}.$$

Recordemos que si ψ un caracter no trivial de k^+, $\underline{\psi} = \psi \circ \mathrm{tr}$ y $S_{\underline{\psi} \circ Q}$ denota la suma de Gauss asociada a Q, calculada en la sección 2.3, entonces la función

$$\begin{aligned} \alpha : A_m^\times &\to \mathbb{C} \\ t &\mapsto \alpha(t) = \frac{S_{\underline{\psi} \circ tQ}}{S_{\underline{\psi} \circ Q}} \end{aligned}$$

es el carácter signo del grupo $A_m^\times$, corolario 2 del capítulo 2. Con estas notaciones, se tiene el siguiente

Teorema 8. *Sea $\mathbb{W} = \{f : A_m \to \mathbb{C} / f \text{ función}\}$, hagamos actuar los generadores de Bruhat de $SL_*(2, A_m)$ en $\mathbb{W}$ mediante*

- $\rho(h(t))(f)(a) = \alpha(t) f(at)$
- $\rho(u(b))(f)(a) = \underline{\psi}(bQ(a)) f(a)$
- $\rho(w)(f)(a) = \frac{\alpha(-1)}{S_{\underline{\psi} \circ Q}} \sum_{a \in A_m} \underline{\psi}(B(a, c)) f(c)$

Entonces se puede extender ρ a todo $SL_*(2, A_m)$, obteniendo que $(\mathbb{W}, \rho)$ es una representación lineal de $SL_*(2, A_m)$.Llamaremos al par $(\mathbb{W}, \rho)$, asi construida, reresentación de Weil generalizada de $SL_*(2, A_m)$.

Demostración. *En virtud del teorema 5, para demostrar que ρ está bien definido, basta verificar que ρ satisface las relaciones*

$$\rho(h(t_1)) \circ \rho(h(t_2)) = \rho(h(t_1 t_2)) \quad (4.1)$$

$$\rho(u(b_1)) \circ \rho(u(b_2)) = \rho(u(b_1 + b_2)) \quad (4.2)$$

$$\rho(h(t)) \circ \rho(u(b)) = \rho(u(tbt^*)) \circ \rho(h(t)) \quad (4.3)$$

$$\rho(w) \circ \rho(w) = \rho(h(-1)) \quad (4.4)$$

$$\rho(w) \circ \rho(h(t)) = \rho(h(t^{*^{-1}})) \circ \rho(w) \quad (4.5)$$

$$\rho(u(t)) \circ \rho(w) \circ \rho\left(u(t^{-1})\right) \circ \rho(w) \circ \rho(u(t)) = \rho(w) \circ \rho\left(h(-t^{-1})\right) \quad (4.6)$$

- *Con un cálculo directo, se demuestran las relaciones* (4.1), (4.2) *y* (4.3).

- *Para la relación* (4.4), *se tiene*

$$\begin{aligned}(\rho(w) \circ \rho(w))(f)(a) &= \rho(w)(\rho(w)(f))(a) \\ &= \frac{\alpha(-1)}{S_{\underline{\psi} \circ Q}} \sum_{b \in A_m} \underline{\psi}(B(a,b)) \rho(w)(f)(b) \\ &= \frac{1}{S^2_{\underline{\psi} \circ Q}} \sum_{b \in A_m} \sum_{c \in A_m} \underline{\psi}(B(a,b)) \underline{\psi}(B(b,c)) f(c) \\ &= \frac{1}{S^2_{\underline{\psi} \circ Q}} \sum_{b \in A_m} \sum_{c \in A_m} \underline{\psi}(B(a+c,b)) f(c).\end{aligned}$$

Como ψ es un carácter no trivial de k^+ y B es una A_m-forma no degenerada, se tiene que

$$\sum_{b \in A_m} \underline{\psi}(B(r,b)) = 0,$$

para todo $r \neq 0$. Luego

$$\begin{aligned}(\rho(w) \circ \rho(w))(f)(a) &= \frac{1}{S^2_{\underline{\psi} \circ Q}} \sum_{b \in A_m} \sum_{c \in A_m} \underline{\psi}(B(a+c,b)) f(c) \\ &= \frac{1}{S^2_{\underline{\psi} \circ Q}} \sum_{c \in A_m} f(c) \sum_{b \in A_m} \underline{\psi}(B(a+c,b)) \\ &= \frac{1}{S^2_{\underline{\psi} \circ Q}} \sum_{b \in A_m} \underline{\psi}(B(0,b)) f(-a) \\ &= \frac{|A_m|}{S^2_{\underline{\psi} \circ Q}} f(-a).\end{aligned}$$

Como m es impar, usando el lema 3, se tiene que $\frac{|A_m|}{S^2_{\underline{\psi}\circ Q}} = \alpha(-1)$. *Así,*

$$\begin{aligned}(\rho(w)\circ\rho(w))(f)(a) &= \alpha(-1)f(-a)\\ &= \rho(h(-1))f(a).\end{aligned}$$

Por lo tanto ρ satisface la relación (4.4).

- *Para la relación* (4.5), *se tiene*

$$\begin{aligned}(\rho(w)\circ\rho(h(t)))(f)(a) &= \rho(w)(\rho(h(t))(f))(a)\\ &= \tfrac{\alpha(-1)}{S_{\underline{\psi}\circ Q}}\sum_{b\in A_m}\underline{\psi}(B(a,b))\rho(h(t))(f)(b)\\ &= \tfrac{\alpha(-1)\alpha(t)}{S_{\underline{\psi}\circ Q}}\sum_{b\in A_m}\underline{\psi}(B(a,b))(f(bt))\\ &= \tfrac{\alpha(-1)\alpha(t)}{S_{\underline{\psi}\circ Q}}\sum_{b'\in A_m}\underline{\psi}(B(a,b't^{-1}))(f)(b')\\ &= \tfrac{\alpha(-1)\alpha(t)}{S_{\underline{\psi}\circ Q}}\sum_{b'\in A_m}\underline{\psi}(B(at^{*^{-1}},b'))(f)(b').\end{aligned}$$

Del lema 3, parte 2 se tiene que $S_{\underline{\psi}\circ tQ} = S_{\underline{\psi}\circ t^{*^{-1}}Q}$. *Así* $\alpha(t) = \alpha\left(t^{*^{-1}}\right)$. *Luego,*

$$\begin{aligned}(\rho(w)\circ\rho(h(t)))(f)(a) &= \alpha(-1)\alpha(t^{*^{-1}})\sum_{b'\in A_m}\underline{\psi}(B(at^{*^{-1}},b'))(f(b'))\\ &= (\rho(h(t^{*^{-1}}))\circ\rho(w))(f)(a)\,.\end{aligned}$$

Por lo tanto, ρ satisface la relación (4.5).

- *La relación* (4.6) *es equivalente a la siguiente relación*

$$\rho(w)\circ\rho(u(t))\circ\rho(w) = \rho(h(-t^{-1}))\circ\rho(u(-t))\circ\rho(w)\circ\rho(u(-t^{-1})). \quad (4.7)$$

Por lo tanto, esta última igualdad es la que vamos a verificar. Por una

parte

$$\begin{aligned}(\rho(w)\circ\rho(u(t))\circ\rho(w))(f)(a) &= \tfrac{\alpha(-1)}{S_{\underline{\psi}\circ Q}}\sum_{b\in A_m}\underline{\psi}(B(a,b))(u(t)\circ\rho(w))(f)(b)\\ &= \tfrac{\alpha(-1)}{S_{\underline{\psi}\circ Q}}\sum_{b\in A_m}\underline{\psi}(B(a,b))\underline{\psi}(tQ(b))\rho(w)(f)(b)\\ &= \tfrac{1}{S^2_{\underline{\psi}\circ Q}}\sum_{b\in A_m}\underline{\psi}(B(a,b))\underline{\psi}(tQ(b))\sum_{z\in A_m}\underline{\psi}(B(b,c))f(c)\\ &= \tfrac{1}{S^2_{\underline{\psi}\circ Q}}\sum_{b\in A_m}\sum_{c\in A_m}\underline{\psi}(B(a,b)+tQ(b)+B(b,c))f(c)\,.\end{aligned}$$

Sea $b = t^{-1}\tilde{b}$, *entonces*

$$\begin{aligned}B(a,b)+tQ(b)+B(b,c) &= t^{-1}\left(B(a,\tilde{b})+Q(\tilde{b})+B(\tilde{b},c)\right)\\ &= t^{-1}\left(B(a+c,\tilde{b})+Q(\tilde{b})\right)\\ &= t^{-1}\left(Q(a+c+\tilde{b})-Q(a+c)\right).\end{aligned}$$

Luego,

$$\begin{aligned}(\rho(w)\circ\rho(t)\circ\rho(w))(f)(a) &= \tfrac{1}{S^2_{\underline{\psi}\circ Q}}\sum_{c\in A_m}\sum_{\tilde{b}\in A_m}\underline{\psi}(t^{-1}(B(a+c,\tilde{b})+Q(\tilde{b}))f(c)\\ &= \tfrac{1}{S^2_{\underline{\psi}\circ Q}}\sum_{c\in A_m}\sum_{\tilde{b}\in A_m}\underline{\psi}(t^{-1}(Q(a+c+\tilde{b})-Q(a+c)))f(c)\\ &= \tfrac{1}{S^2_{\underline{\psi}\circ Q}}\sum_{c\in A_m}\underline{\psi}(-t^{-1}(Q(a+c)))f(c)\sum_{\tilde{b}\in A_m}\underline{\psi}(t^{-1}(Q(a+c+\tilde{b}))).\end{aligned}$$

Notemos que para todo $c\in A_m$ *se tiene que*

$$S_{\underline{\psi}\circ t^{-1}Q} = \sum_{\tilde{b}\in A_m}\underline{\psi}(t^{-1}(Q(a+c+\tilde{b}))).$$

Por lo tanto

$$(\rho(w)\circ\rho(t)\circ\rho(w))(f)(a) = \tfrac{S_{\underline{\psi}\circ t^{-1}Q}}{S^2_{\underline{\psi}\circ Q}}\sum_{c\in A_m}\underline{\psi}(-t^{-1}Q(a+c))f(c).$$

Ahora bien, por otra parte,

$$\rho(h(-t^{-1}))\circ\rho(u(-t))\circ\rho(w)\circ\rho(u(-t^{-1}))(f)(a)=$$

$$\begin{aligned}
&= \frac{\alpha(t^{-1})\underline{\psi}(-t^{-1}Q(a))}{S_{\underline{\psi}\circ Q}}\sum_{b\in A_m}\underline{\psi}(B(-at^{-1},b))(\rho(u(-t^{-1})))(f)(b)\\
&= \frac{\alpha(t^{-1})\underline{\psi}(-t^{-1}Q(a))}{S_{\underline{\psi}\circ Q}}\sum_{b\in A_m}\underline{\psi}(B(-at^{-1},b))\underline{\psi}(-t^{-1}Q(b))f(b)\\
&= \frac{\alpha(t^{-1})\underline{\psi}(-t^{-1}Q(a))}{S_{\underline{\psi}\circ Q}}\sum_{b\in A_m}\underline{\psi}(-t^{-1}(B(a,b)-Q(b)))f(b)\\
&= \frac{\alpha(t^{-1})\underline{\psi}(-t^{-1}Q(a))}{S_{\underline{\psi}\circ Q}}\sum_{b\in A_m}\underline{\psi}(-t^{-1}(Q(a+b)-Q(a)))f(b)\\
&= \frac{\alpha(t^{-1})}{S_{\underline{\psi}\circ Q}}\sum_{b\in A_m}\underline{\psi}(-t^{-1}Q(a+b))f(b).
\end{aligned}$$

Luego se satisface la relación (4.7) *si se cumple*

$$\frac{S_{\underline{\psi}\circ t^{-1}Q}}{S^2_{\underline{\psi}\circ Q}}=\frac{\alpha(t^{-1})}{S_{\underline{\psi}\circ Q}},$$

para todo $t\in A_m^{\times}\cap A_m^{s}$. *Se afirma que se tiene tal igualdad, en efecto, pues*

- *Si* $t\in A_m^{\times}\cap A_m^{s}$ *es un cuadrado, entonces de la demostración de la proposición 3, capítulo 2,* $t\in \mathrm{Orb}_{A_m^{\times}}(1)$. *Luego,* $t^{-1}\in \mathrm{Orb}_{A_m^{\times}}(1)$, *así*

$$\frac{S_{\underline{\psi}\circ t^{-1}Q}}{S^2_{\underline{\psi}\circ Q}}=\frac{S_{\underline{\psi}\circ Q}}{S^2_{\underline{\psi}\circ Q}}=\frac{\alpha(t^{-1})}{S_{\underline{\psi}\circ Q}}.$$

- *Si* $t\in A_m^{\times}\cap A_m^{s}$ *es un no cuadrado, entonces de la demostración de la proposición 3, capítulo 2,* $t\in \mathrm{Orb}_{A_m^{\times}}(d)$ *(*d *en* k *un no cuadrado). Luego,* $t^{-1}\in \mathrm{Orb}_{A_m^{\times}}(d)$, *así*

$$\frac{S_{\underline{\psi}\circ t^{-1}Q}}{S^2_{\underline{\psi}\circ Q}}=-\frac{S_{\underline{\psi}\circ Q}}{S^2_{\underline{\psi}\circ Q}}=\frac{\alpha(t^{-1})}{S_{\underline{\psi}\circ Q}}.$$

Por lo tanto, $(\mathbb{W},\rho)$ *es una representación lineal del grupo* $SL_*(2,A_m)$.

4.3. Estructura del grupo ortogonal O(Q)

Lema 17. *El grupo ortogonal del A_m-módulo cuadrático no degenerado (A_m, Q, B) (definido en el capítulo 2) es isomorfo al grupo $\mathcal{U}_m = \{b \in A_m / b^* b = 1\}$.*

Demostración. Sean T y $\tilde{T}$ dados por

$$\begin{array}{rccl} T & : & O(Q) & \to & \mathcal{U}_m \\ & & \varphi & \mapsto & T(\varphi) = \varphi(1) \end{array}$$

$$\begin{array}{rccl} \tilde{T} & : & \mathcal{U}_m & \to & O(Q) \\ & & u & \mapsto & T_u : A_m \to A_m \\ & & & & \quad a \mapsto T_u(a) = ua \end{array}$$

Se verifica directamente que T y $\tilde{T}$ son homorfismos de grupos tales que

$$\begin{aligned} T \circ \tilde{T} &= \mathrm{Id}_{\mathcal{U}_m} \\ \tilde{T} \circ T &= \mathrm{Id}_{O(Q)} \end{aligned}$$

De aquí el lema. ■

Lema 18. *En $A_m^\times$ existen, exactamente, dos elementos cuyo cuadrado es 1.*

Demostración. Sea $a = a_0 + a_1 x + \cdots + a_{m-1} x^{m-1}$ en $A_m^\times$ tal que $a^2 = 1$. Entonces $a_0^2 = -1$, así $a_0 = 1$ o $a_0 = -1$. Ahora si a posee una potencia positiva de x, sea i el menor entero positivo tal que $a_i \neq 0$, es decir, $a = a_0 + a_i x^i + \cdots + a_{m-1} x^{m-1}$. Entonces $a^2 \neq 0$, pues la potencia x^i aparece en a^2. Así, a^2 no posee potencias positivas de x, por lo tanto $a = 1$ o $a = -1$. De aquí el lema. ■

El conocer la estructura del grupo ortogonal $O(Q)$ permite saber la estructura de su grupo de caracteres, lo cual permite entrelazar la representación lineal $(\mathbb{W}, \rho)$, es decir, notar queel grupo $O(Q)$ actúa en el espacio de representación $\mathbb{W}$ conmutando con la acción de ρ. Tal hecho permite obtener una descomposición de $(\mathbb{W}, \rho)$ a partir de representaciones de $O(Q)$. La estructura del grupo $O(Q) \simeq \mathcal{U}_p$ esta dada en el siguiente

Teorema 9. *Sea $k = \mathbb{F}_q = \mathbb{F}_{p^n}$, p primo impar. Entonces*

$$\mathcal{U}_p = C_2 \times \underbrace{C_p \times \cdots \times C_p}_{\frac{p-1}{2} - veces} .$$

Demostración. Sabemos que $\mathcal{U}_p = \mathrm{Stab}_{A_p^\times}(1)$. Así, del corolario 3

$$|\mathcal{U}_p| = 2p^{\frac{p-1}{2}}.$$

Como $\mathcal{U}_p$ es un grupo abeliano, se tiene una primera descomposición

$$\mathcal{U}_p = C_2 \times P,$$

donde P es el p-subgrupo de Sylow $\mathrm{Syl}_p(\mathcal{U}_p)$. Ahora, dado $a \in \mathcal{U}_p$, entonces $a_0 = 1$ o bien $a_0 = -1$. Entonces $a^p = \pm 1$. Así $a^{2p} = 1$. Por lo tanto $a^p = 1$, para todo $a \in P$. Así,

$$P = \underbrace{C_p \times \cdots \times C_p}_{\frac{p-1}{2}-\text{veces}}.$$

Luego

$$\mathcal{U}_p = C_2 \times \underbrace{C_p \times \cdots \times C_p}_{\frac{p-1}{2}-\text{veces}}.$$

De aquí el teorema. ■

Observación 4. *Siguiendo la demostración del teorema anterior, se puede demostrar, en general, que $a^{2m} = 1$, para todo $a \in \mathcal{U}_m$. Además se comprueba directamente que $-1 + x \in \mathcal{U}_m$ y que su orden es precisamente $2m$. Así, podemos decir que el grupo $\mathcal{U}_m$ es de exponente $2m$.*

4.4. Descomposición de la Representación de Weil según $O(Q) \simeq \mathcal{U}_m$

Proposición 4. *Hagamos actuar $\mathcal{U}_m$ en $\mathbb{W}$ mediante*

$$\pi(b)(f)(a) = f(ba), \ b \in \mathcal{U}_m, \ f \in \mathbb{W}.$$

Entonces $(\mathbb{W}, \pi)$ es una representación lineal de $\mathcal{U}_m$. Además, la acción e $\mathcal{U}_m$ conmuta con la acción de ρ.

Demostración. Es suficiente demostrar que la acción de π conmuta con ρ_w, pues de un cálculo directo e tiene que π conmuta con $\rho_{h(t)}$ y con $\rho_{u(s)}$. Así

$$\begin{aligned}(\rho_w \circ \pi_b)(f)(a) &= \rho_w(\pi_b(f))(a) \\ &= \sum_{c \in A} \underline{\psi}(B(a,c))(\pi_b(f))(c) \\ &= \sum_{c \in A} \underline{\psi}(B(a,c)) f(bc)\end{aligned}$$

$$\begin{aligned}(\rho_w \circ \pi_b)(f)(a) &= \sum_{c' \in A} \underline{\psi}(B(a, b^{-1}c'))f(c') \\ &= \sum_{c' \in A} \underline{\psi}(B(a, b^{*}c'))f(c') \\ &= \sum_{c' \in A} \underline{\psi}(B(ba, c'))f(c') \\ &= (\pi_b \circ \rho_w)(f)(a)\,.\end{aligned}$$

■

De esta proposición se obtiene directamente el siguiente

Corolario 3. *Sea α un caracter del grupo $\mathcal{U}_m$. Se define*

$$\mathbb{W}_\alpha = \{f \in \mathbb{W} / f(ba) = \alpha(b)f(a),\ \textit{para todo}\ b \in \mathcal{U}_m,\ \textit{para todo}\ a \in A\}\,.$$

Entonces $(\mathbb{W}_\alpha, \rho|_{\mathbb{W}_\alpha})$ es una subrepresentación de $(\mathbb{W}, \rho)$.

Demostración. Sean $f \in W_\alpha$ y $g \in SL_*(2, A)$. Entonces $\pi(b)(f) = \alpha(b)f$. Como la proposición 4 establece que la acción de $\mathcal{U}_m$ conmuta con la acción de ρ, así

$$\begin{aligned}\rho_g(f)(ua) &= \pi_u(\rho_g(f))(a) \\ &= \rho_g(\pi_u(f))(a) \\ &= \rho_g(\alpha(u)f)(a) \\ &= \alpha(u)(\rho_g(f))(a).\end{aligned}$$

Por lo tanto, $(\mathbb{W}_\alpha, \rho|_{\mathbb{W}_\alpha})$ es una subrepresentación de $(\mathbb{W}, \rho)$.

■

El corolario anterior permite la siguiente

Proposición 5. *Se tiene la siguiente descomposición de la representación de Weil*

$$(\mathbb{W}, \rho) = \bigoplus_{\alpha \in \widehat{\mathcal{U}_m}} (\mathbb{W}_\alpha, \rho|_{\mathbb{W}_\alpha})\,.$$

Así se obtiene una primera descomposición de la representación de Weil $(\mathbb{W}, \rho)$. A partir de ésta, se puede estudiar una futura descomposición de la representación de Weil $(\mathbb{W}, \rho)$ en un subrepresentaciones irreducibles.

Bibliografía

[1] Thomas W. Hungerford. *Algebra.* Springer-Verlag, New York, 1974.

[2] Dieudonne J.A. *La géométrie des groupes classiques.* Springer-Verlag, 1963.

[3] Nathan Jacobson. *Finite Dimensional Division Algebra Over Fields.* Springer-Verlag, 1996.

[4] José Pantoja. *A presentation of the group $SL_*(2, A)$, A simple artinian ring with involution.* A ser publicado en Manuscripta Mathematica.

[5] José Pantoja and Jorge Soto-Andrade. *A Bruhat descomposition of the group $SL_*(2, A)$.* Journal of Algebra, 262 : p. 401-412, 2003.

[6] Jean Pierre Serre. *Linear Representations of Finite Groups.* Springer-Verlag, New York, Berlin, 1977.

[7] Jorge Soto-Andrade. *Représentations de certains groupes symplectiques finis.* Bull. Soc. Math. France, Mémoire 55-56, 1978.

[8] Pantoja, J. & Soto-Andrade, J. *The groups $GL^{\varepsilon}_*(2, A)$, $SL^{\varepsilon}_*(2, A)$ and the ε-determinant.* Preprint.

[9] André Weil. *Sur certains groupes d'opérateurs unitaires.* Acta Math. 111: p. 143-211, 1964.