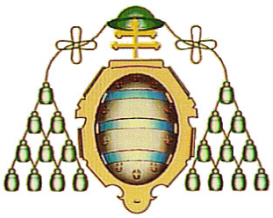


UNIVERSIDAD DE OVIEDO

Departamento de Matemáticas

Alejandro Piñera Nicolás

SUPER-CARACTERES DE GRUPOS DE ÁLGEBRA. APLICACIONES A LA TEORÍA CUÁNTICA DE CÓDIGOS

TESIS DOCTORAL DIRIGIDA POR

Consuelo Martínez López

Universidad de Oviedo

Reservados todos los derechos
© El autor

Edita: Universidad de Oviedo
Biblioteca Universitaria, 2008
Colección Tesis Doctoral-TDR nº 26

ISBN: 978-84-691-5126-6
D.L.: AS.03586-2008

Memoria para optar al grado de Doctor
bajo la dirección de la profesora Consuelo
Martínez López.

Agradecimientos

Es mi deseo agradecer a la profesora Consuelo Martínez López el haberme dado la oportunidad de realizar este trabajo. Gracias por el tiempo dedicado durante estos últimos cinco años.

Asimismo, quiero agradecer al Ministerio de Educación y Ciencia la concesión de una beca para la Formación del Personal Investigador (FPI) que me permitió tener financiación durante este periodo y realizar estancias de investigación en el IAKS de Karlsruhe y en el Centro de Estruturas Lineares e Combinatórias (CELC) da Universidade de Lisboa.

Gracias también al profesor Santos González Jiménez por haberme acogido en su grupo de investigación y a todos los compañeros que allí he tenido. En especial a Ignacio Fernández Rúa, Sergio Martínez Fernández, Ignacio Cascudo Pueyo, Concepción López Diaz con quienes he compartido despacho, charlas, congresos...

Por otra parte, quiero también agradecer al profesor Markus Grassl del IAKS de la Universidad de Karlsruhe el haber aceptado trabajar conmigo y el haber propuesto algunos de los problemas que se han intentado resolver en esta tesis.

Quero agradecer também ao professor Carlos André por me ter acolhido no Centro de Estruturas Lineares e Combinatórias da Universidade de Lisboa, por me ter proposto vários problemas e por me ter dedicado tanto tempo.

Sem ele esta tese não teria sido possível. Obrigado também aos colegas do CELC, com quem sempre me senti como se estivesse em casa. Especialmente quero agradecer à Ana Luísa Correia e à Ana Margarida Neto, que resolveram os meus problemas de alojamento, e ao Henrique Cruz com quem partilhei café e jornal.

Obrigado também à Patrícia, que me falou da hipótese de trabalhar em Portugal e não só... Sem ela este trabalho teria sido bem diferente. Obrigado também à sua família pela forma como me acolheram e ajudaram.

Y por último, y no por ello menos importante, gracias a mi familia y amigos por haberme apoyado durante todo este tiempo y haberme ayudado siempre que lo precisé. A todos ellos, mi más sincera gratitud.

Índice general

Introducción

La Teoría de Representaciones de grupos finitos tiene su origen en los trabajos de Frobenius de finales del siglo XIX y fue desarrollada por Burnside, a quien se debe su primera exposición sistemática, a comienzos del siglo XX. De esta época es el teorema de Burnside que establece que un grupo es resoluble si su orden es divisible, como máximo, por dos primos distintos (ver teorema 34.1 de [24]). Posteriormente, los trabajos de E. Noether y R. Brauer le dieron un enfoque más próximo al actual al introducir en la teoría el lenguaje de módulos y anillos al que ahora estamos acostumbrados.

La evolución de la teoría ha permitido resolver importantes problemas de la Teoría de Grupos. Por ejemplo, en la clasificación de los grupos simples finitos se utilizan técnicas basadas en representaciones de grupos. También encontramos aplicaciones en otras disciplinas como la Física, la Química o la Cristalografía, al constituir la Teoría de Representaciones un modelo natural para el estudio de la simetría.

El grupo de las matrices triangulares es un objeto fundamental dentro de las Matemáticas (ver [49]). Por ello, el conocimiento de sus representaciones tiene una relevancia especial. Este problema, aun en el caso de que el grupo sea nilpotente (lo que equivale a considerar matrices estrictamente superiores) no tiene una solución sencilla. El método de las órbitas de Kirillov (ver [48], [50]) permitió resolver el problema para el grupo $U_n(\mathbb{R})$, es decir, el grupo

de las matrices unitriangulares sobre el cuerpo $\mathbb{R}$. Una adaptación de este método para cuerpos finitos, dada por Kazhdan (ver [47]) durante los años 70, logró la extensión de estos resultados al grupo $\mathbf{U}_n(q)$, esto es, el grupo de las matrices unitriangulares con coeficientes en el cuerpo finito $\mathbb{F}_q$, con $q = p^e$, cuando la característica p es suficientemente grande. Sin embargo, no fue posible resolver el problema para el caso en que la característica de $\mathbb{F}_q$ es arbitraria.

Los super-caracteres, desarrollados por Carlos A. M. André (ver [4], [5], [6], [8] y [9]) y por Ning Yan (ver [82]), suponen una nueva aproximación al problema. A pesar de que los métodos seguidos por cada uno de ellos son diferentes, los resultados a los que llegan son equivalentes. En esencia, lo que se obtiene es una partición del conjunto de caracteres irreducibles del grupo $\mathbf{U}_n(q)$ que conserva alguna de las propiedades de éstos. Así, los super-caracteres son ortogonales dos a dos y descomponen el carácter regular del grupo, por lo que cada super-carácter es constituyente de un único carácter irreducible.

El propósito de esta memoria es extender estos resultados a grupos más generales: los denominados grupos de álgebra, con el fin de avanzar en la determinación de sus caracteres irreducibles (ver [7]). A esto dedicaremos los cuatro primeros capítulos. Finalmente, en el último capítulo procederemos al estudio de una de las aplicaciones de la Teoría de Representaciones: la construcción de códigos cuánticos correctores de errores. Como veremos después, la información cuántica es muy sensible a todo tipo de errores e interacciones con el medio exterior, por lo que es importante desarrollar mecanismos que permitan su protección frente a este tipo de sucesos.

De forma sucinta, el contenido de la memoria se distribuye a lo largo de sus capítulos como se muestra a continuación. El primer capítulo resume los

resultados de André y Yan para el grupo $\mathbf{U}_n(q)$. En él no se aportan resultados nuevos y se incluye con la finalidad de que la memoria sea autocontenida y de que el lector pueda conocer el trabajo de Yan, no fácilmente accesible. El método seguido por André consiste en asociar un carácter especial, llamado carácter básico, a cada elemento de la base canónica de $\mathbf{U}_n(q)$ visto como $\mathbb{F}_q$-espacio vectorial. De esta manera, un super-carácter se define como un producto de caracteres básicos. Por su parte, el método de Yan está más próximo del de Kirillov, pues define cada super-carácter como asociado a un cierto $\mathbb{C}\mathbf{U}_n(q)$-modulo dado por una acción de $\mathbf{U}_n(q)$, denominada acción de cotransición, sobre el espacio dual $\mathbf{U}_n(q)^*$. Probaremos que ambos métodos son equivalentes y por ello, las dos definiciones de super-carácter coinciden.

El grupo $\mathbf{U}_n(q)$ es un caso especial de grupo de álgebra. Esta noción fue introducida por Isaacs en [43] y se refiere a los grupos de la forma $G = 1+J(A)$, donde A es una F-álgebra de dimensión finita y $J(A)$ es su radical de Jacobson. En el segundo capítulo de la memoria extenderemos el concepto de super-carácter para abarcar los $\mathbb{F}_q$-grupos de álgebra finitos. Es importante notar que en nuestro desarrollo no se hace ninguna referencia a la característica del cuerpo $\mathbb{F}_q$, por lo que los resultados son válidos para cualquier valor de ésta. Es debido a una definición conveniente de los super-caracteres que evita el uso de la función exponencial cuando se relacionan las propiedades del grupo G y de la $\mathbb{F}_q$-álgebra $J(A)$ (un ejemplo del uso de la exponencial en grupos de álgebra se puede ver en [33]). Una vez definidos, se estudian sus principales propiedades, que acaban por coincidir con las obtenidas para $\mathbf{U}_n(q)$, y se estudia un caso particular: el álgebra de polinomios de grado menor o igual que n en una única indeterminada.

El capítulo tercero se encarga de estudiar los super-caracteres de una $\mathbb{F}_q$-álgebra nilpotente libre. Para ello, estudiamos la $\mathbb{F}_q$-álgebra de polinomios en

m indeterminadas no conmutativas cuyo grado es menor o igual que n. Puesto que cualquier $\mathbb{F}_q$-álgebra es cociente de un álgebra libre, estos resultados deberían ayudarnos a encontrar los super-caracteres de cualquier $\mathbb{F}_q$-grupo de álgebra. Sin embargo, a pesar de que la forma de los super-caracteres es conocida por los resultados del capítulo anterior, en el caso general, no es posible una descripción sencilla de los mismos. Por ello, acudimos a una aproximación para intentar escribir el super-carácter asociado a un polinomio cualquiera como producto de caracteres asociados a los monomios que lo componen, de forma parecida a lo que se hace en el grupo $\mathbf{U}_n(q)$ con los caracteres básicos. Así, la primera sección se centra en la definición de estos nuevos caracteres, que por analogía con el grupo $\mathbf{U}_n(q)$ reciben el nombre de básicos, y en el estudio de sus propiedades. Posteriormente, probaremos que se pueden descomponer en una suma de super-caracteres, y prestaremos especial atención a aquellos que sólo poseen un único constituyente: los completamente ramificados. Por último, terminamos con un ejemplo: el álgebra de polinomios en m indeterminadas conmutativas de grado menor o igual que n.

Abordamos en el cuarto capítulo una extensión de la teoría de super-caracteres cuando la $\mathbb{F}_q$-álgebra A se sustituye por un R-módulo nilpotente con R un anillo conmutativo finito. La elección del anillo R es importante, pues de ella dependerá el que se pueda obtener una buena parametrización de los super-caracteres en función de los elementos del módulo dual A^*, tal como sucede en el capítulo 2. No todos los anillos finitos son apropiados, como veremos en la primera sección, sino sólo aquellos que son admisibles, lo que según la definición de Claasen (ver [23]) equivale a que el módulo de los caracteres aditivos de R sea cíclico. En la segunda sección, analizamos con más detalle esta propiedad y caracterizamos los anillos finitos que la satisfacen:

los anillos Frobenius (ver [80]), para estudiar el caso particular de los anillos de Galois (ver [17]). A lo largo de lo que resta de capítulo, impondremos que el anillo R es un anillo de Galois y construiremos, en la tercera sección, los super-caracteres del grupo adjunto asociado al módulo nilpotente A, que es el sustituto natural del grupo de álgebra. Por último, estudiamos un ejemplo sencillo: la R-álgebra de los polinomios en una indeterminada de grado menor que n y sin término independiente, con R un anillo de Galois. Construimos una parte de los super-caracteres y los comparamos con los que obtuvimos en el capítulo segundo. La diferencia más significativa es el incremento en el grado de dificultad de la descripción. Mientras que en el capítulo 2 se conseguía una descripción completa de todos ellos, en este caso sólo conseguimos dar una expresión simple de los más sencillos.

La memoria termina con una aplicación de la Teoría de Representaciones a la Teoría de Codificación: la construcción de códigos cuánticos correctores de errores. Para ello, nos hemos basado en los trabajos de Martin Roettler y Andreas Klappanecker (ver [51], [52], [53], [54] y [55]) y hemos intentado construir nuevos códigos cuánticos de forma similar a como se hace con los clásicos. Los errores cuánticos se modelan como operadores que actúan sobre un espacio de Hilbert que representa el sistema de trabajo. Estos errores se pueden generar a partir de nice error bases que, tal como están descritas en la primera sección, constituyen una representación proyectiva de un grupo G llamado grupo de error. La segunda sección se dedica a la descripción de los códigos cuánticos más usuales: los códigos estabilizadores y los códigos de Clifford y se estudian sus propiedades correctoras en términos de la Teoría de Representaciones. Finalmente, procedemos a dar una caracterización de los códigos Clifford no estabilizadores en términos de caracteres completamente ramificados y a la construcción de nuevos códigos Clifford a partir

del producto de varios grupos de error, para concluir con el análisis de sus propiedades correctoras.

Capítulo 1

Preliminares. Super-caracteres del grupo $\mathbf{U}_n(q)$

Sea p un primo y $q = p^e$, $e > 1$ una cierta potencia suya. Si $\mathbb{F}_q$ es el cuerpo finito de q elementos, denotaremos por $\mathbf{U}_n(q)$ el grupo de todas las matrices unitriangulares, es decir, matrices triangulares superiores con 1 en su diagonal principal, cuyas entradas son elementos de $\mathbb{F}_q$.

La determinación de los caracteres irreducibles del grupo $\mathbf{U}_n(q)$ es un problema difícil. Para abordarlo, Carlos A. M. André y Ning Yan introdujeron, de forma independiente, el concepto de super-carácter (ver [4]-[7] para el primero y [82] para el segundo). En esencia, constituyen una partición del conjunto de caracteres irreducibles $Irr(\mathbf{U}_n(q))$ que conserva algunas de sus propiedades: son ortogonales dos a dos, descomponen el carácter regular y son constantes sobre las super-clases, una generalización de las clases de conjugación del grupo.

A pesar de que el objeto definido por André y por Yan es el mismo, sus enfoques son diferentes. Para el primero, los super-caracteres se definen de forma puramente combinatoria, a partir de los caracteres básicos. Para

Yan, más próximo al método de las órbitas de Kirillov (ver [48]), cada super-carácter está asociado a la órbita de una acción de $\mathbf{U}_n(q)$.

En este capítulo trataremos de hacer una revisión de ambas formulaciones para probar que ambas son equivalentes para el grupo $\mathbf{U}_n(q)$. Así, comenzaremos por una sección introductoria donde revisaremos conceptos básicos de la teoría de caracteres que se utilizarán con frecuencia en la tesis. Las dos secciones siguientes se ocupan del trabajo de Carlos A. M. André. En la primera se expone el concepto de funciones de Kirillov para un grupo de álgebra, ver [7] y en la segunda estudiaremos la noción de carácter básico. Las ideas fueron desarrolladas en [9]. La última sección explora el método de Yan y la construcción de los caracteres de transición para terminar probando la equivalencia de ambas formulaciones. Esta última sección pretende ser un resumen de [82]. Dado que esta referencia puede no ser fácilmente accesible, se incluyen algunas demostraciones por completitud y para facilitar la lectura de la memoria.

1.1. Preliminares

A continuación intentaremos revisar algunos de los conceptos que aparecerán a lo largo de esta tesis y que deberían ser familiares. Dentro de este apartado se encuadran las definiciones de representaciones, caracteres y fórmulas de ortogonalidad. Los resultados, que se presentarán sin demostración, están extraídos de [24], [25] y [41], donde se remite al lector para una lectura más detallada.

Definición 1.1.1 *Sean F un cuerpo y G un grupo. Una F-representación de grado n de G es un homomorfismo $\mathfrak{X} : G \to GL(n, F)$, con $GL(n, F)$ el grupo general lineal de grado n sobre el cuerpo F.*

Sea M un F-espacio vectorial, diremos que M es un G-módulo si se puede definir un producto $G \times M \to M$ de forma que para todo $g, g' \in G$ y todo $m, m' \in M$ se verifiquen las siguientes propiedades:

$$\begin{cases} g(m+m') = gm + gm', \\ (gg')m = g(g'm), \\ 1\, m = m. \end{cases} \tag{1.1}$$

Si la dimensión de M es n, el grupo $GL(n,F)$ se identifica de forma natural con el grupo de F-automorfismos de M, denotado por $GL(M)$. Entonces, dada una F-representación de G, $\mathfrak{X} : G \to GL(n,F)$, podemos definir el producto $gm = \mathfrak{X}(g)\, m$, que claramente satisface las propiedades (1.1) y convierte a M en el G-módulo asociado a la F-representación $\mathfrak{X}$. Recíprocamente, si M es un G-módulo, la F-representación $\mathfrak{X} : G \to GL(n,F)$ definida por $\mathfrak{X}(g)(m) = gm$ es la F-representación asociada al módulo M. De esta forma, a cada G-módulo se le asocia una única F-representación y viceversa.

Definición 1.1.2 *Sean $\mathfrak{X}$ y $\mathfrak{D}$ dos F-representaciones de un grupo G. Diremos que son equivalentes si ambas tienen el mismo grado y además existe una matriz $P \in GL(n,F)$ tal que $\mathfrak{X}(g) = P^{-1}\mathfrak{D}(g)\, P$ para todo $g \in G$.*

En el lenguaje de módulos, dos representaciones $\mathfrak{X}$ y $\mathfrak{D}$, con módulos asociados M y N respectivamente, se dicen equivalentes si existe un G-isomorfismo de módulos $\varphi : M \to N$. Recordemos que φ es un G-isomorfismo de módulos si es un isomorfismo de espacios vectoriales y además satisface $\varphi(gm) = g\varphi(m)$ para todo $g \in G$ y $m \in M$.

Definición 1.1.3 *Sean $\mathfrak{X}$ una F-representación y M su módulo asociado. Se dice que $\mathfrak{X}$ es irreducible si el módulo M es irreducible, es decir, si sus únicos submódulos propios son 0 y M.*

Un módulo M se dice *completamente reducible* si para cualquier submódulo suyo V se puede encontrar otro W de forma que $M = V \oplus W$. El Teorema de Maschke (ver teorema 1.9 de [41]) garantiza que si la característica de F no divide al orden de G (en particular, si es cero), todo G-módulo es completamente reducible. En términos de F-representaciones esta propiedad se traduce en que cualquier representación de G se puede escribir como suma directa de representaciones irreducibles.

Aunque una parte de los resultados que recogemos a continuación son ciertos siempre que F sea un cuerpo cuya característica no divide al orden de G, en adelante consideraremos que F es el cuerpo $\mathbb{C}$ de los complejos.

Definición 1.1.4 *Sea $\mathfrak{X}$ una $\mathbb{C}$-representación de un grupo G. El $\mathbb{C}$-carácter χ asociado a $\mathfrak{X}$ es la aplicación $\chi : G \to \mathbb{C}$ definida por $\chi(g) = tr(\mathfrak{X}(g))$, para todo $g \in G$.*

Dado un G-módulo M, su carácter asociado será el de la $\mathbb{C}$-representación dada por M. Es decir, se tiene la siguiente definición:

Definición 1.1.5 *Sean M un G-módulo y $\mathfrak{X}$ su $\mathbb{C}$-representación asociada. Diremos que χ es el carácter asociado a M si χ es el carácter asociado a $\mathfrak{X}$, es decir si $\chi(g) = tr(\mathfrak{X}(g))$, para todo $g \in G$.*

Nota 1.1.6 *Los caracteres asociados a una F-representación de G (respect. de un G-módulo M) reciben el nombre de F-caracteres. En lo que sigue, puesto que trabajaremos sólo con $\mathbb{C}$-representaciones, entenderemos que los caracteres de un grupo G (respect. de un G-módulo M) son los $\mathbb{C}$-caracteres de G (respect. de M).*

Si dos $\mathbb{C}$-representaciones de G son equivalentes, entonces los G-módulos asociados a cada una de ellas son G-isomorfos, de donde se sigue que los caracteres han de ser iguales.

Definición 1.1.7 *Sean $\mathfrak{X}$ una $\mathbb{C}$-representación de G y χ su carácter asociado, entonces χ es irreducible si y sólo si la representación $\mathfrak{X}$ es irreducible.*

Denotaremos por $Irr(G)$ al conjunto de todos los caracteres irreducibles de G. Se puede probar (ver 27.22 de [24]) que el cardinal $|Irr(G)|$ es igual al número de clases de conjugación del grupo. Los caracteres de grado uno, que claramente son irreducibles, reciben el nombre especial de caracteres lineales.

Si G es abeliano, cada elemento coincide con su clase de conjugación y entonces $|Irr(G)| = |G|$. Así pues, todos los caracteres de G son lineales. El recíproco también es cierto, de hecho, se tiene la siguiente caracterización (ver corolario 2.6 de [41] para los detalles).

Proposición 1.1.8 *Un grupo G es abeliano si y sólo si todos sus caracteres son lineales, en cuyo caso $|G| = |Irr(G)|$.*

Es fácil ver que los caracteres son constantes sobre las clases de conjugación del grupo. Este tipo de funciones se conocen como *funciones de clase* de G, forman un $\mathbb{C}$-espacio vectorial, denotado por $\mathrm{cf}(G)$, y su base es el conjunto $Irr(G)$. Así pues, cada función $\varphi \in \mathrm{cf}(G)$ se puede escribir de forma única como $\varphi = \sum_{\chi \in Irr(G)} a_\chi \chi$. Los elementos $\chi \in Irr(G)$ para los que $a_\chi \neq 0$ reciben el nombre de *constituyentes irreducibles* de φ.

En caso que G sea finito (en lo que sigue siempre lo será), denotamos por $\mathbb{C}G$ el conjunto de todas las sumas formales $\{\sum_{g \in G} a_g g : a_g \in \mathbb{C}\}$. Claramente, $\mathbb{C}G$ es un $\mathbb{C}$-espacio vectorial, pero también un G-módulo si consideramos el producto $ha = h(\sum_{g \in G} a_g\, g) = \sum_{g \in G} a_g\, hg$, para todo $h \in G$, $a \in \mathbb{C}G$. La representación asociada a este módulo recibe el nombre de *representación regular* de G. Su carácter suele representarse como ρ_G.

Proposición 1.1.9 *Sea G un grupo y sea ρ_G su carácter regular, entonces*

$$\rho_G(g) = \begin{cases} |G| & si\ g = 1, \\ 0 & en\ otro\ caso. \end{cases}$$

Este carácter tiene la siguiente descomposición como suma de irreducibles :

$$\rho_G = \sum_{\chi \in Irr(G)} \chi(1)\chi.$$

Sea $\mathbb{C}[G] = \{f : G \to \mathbb{C}\}$ el $\mathbb{C}$-espacio vectorial de las funciones complejas definidas sobre G. Este espacio puede dotarse de un producto escalar mediante la siguiente definición.

Definición 1.1.10 (Producto de Frobenius) *Sean φ, θ funciones complejas sobre G, entonces*

$$\langle \varphi, \theta \rangle_G = \frac{1}{|G|} \sum_{g \in G} \varphi(g)\overline{\theta(g)}$$

es el producto de Frobenius de φ y θ.

El conjunto $Irr(G)$ es una base ortogonal respecto al producto de Frobenius del espacio vectorial $\mathrm{cf}(G)$. Este resultado se conoce como *primera relación de ortogonalidad* de caracteres.

Teorema 1.1.11 (Primera Relación de Ortogonalidad) *Sean χ_i, χ_j caracteres irreducibles de G, entonces su producto de Frobenius*

$$\langle \chi_i, \chi_j \rangle_G = \frac{1}{|G|} \sum_{g \in G} \chi_i(g)\overline{\chi_j(g)} = \delta_{ij}.$$

Los caracteres irreducibles satisfacen también la siguiente relación, conocida como *segunda relación de ortogonalidad.*

Teorema 1.1.12 (Segunda Relación de Ortogonalidad) *Sean $g, h \in G$, entonces*

$$\sum_{\chi \in Irr(G)} \chi(g)\overline{\chi(h)} = \begin{cases} |C_G(g)| & \text{si } g \text{ y } h \text{ son } G\text{-conjugados,} \\ 0 & \text{en otro caso,} \end{cases}$$

donde $C_G(g) = \{x \in G : xg = gx\}$ es el centralizador de g en G.

Nota 1.1.13 *Nótese que los órdenes $|C_G(g)|$ y $|C_G(h)|$ coinciden si g y h son conjugados.*

Por último, introducimos la definición de función inducida y el resultado conocido como reciprocidad de Frobenius (ver lema 5.2 de [41]). Estos conceptos serán de utilidad en los capítulos siguientes.

Definición 1.1.14 *Sea $H \leq G$ y sea $\varphi \in cf(H)$. La función φ^G definida como*

$$\varphi^G(g) = \frac{1}{|H|} \sum_{x \in G} \varphi^\circ(xgx^{-1}),$$

con $\varphi^\circ(h) = \varphi(h)$ si $h \in H$ y $\varphi^\circ(t) = 0$ si $t \notin H$, recibe el nombre de función inducida sobre G.

Proposición 1.1.15 (Reciprocidad de Frobenius) *Sea $H \leq G$ un subgrupo de G. Supongamos que φ es una función de clase de H y que θ es una función de clase de G, entonces se cumple*

$$\langle \varphi, \theta \rangle_H = \frac{1}{|H|} \sum_{h \in H} \varphi(h)\overline{\theta(h)} = \langle \varphi^G, \theta \rangle.$$

1.2. Grupos de álgebra. Generalidades

Comenzamos esta sección con la definición de grupo de álgebra. Este concepto fue introducido por Isaacs en [42] tal como aparece a continuación:

Definición 1.2.1 *Sean F un cuerpo de característica p y A una F-álgebra finito dimensional. Si $J = J(A)$ es su radical de Jacobson, entonces el conjunto $1 + J = \{1 + a : a \in J\}$ es un p-subgrupo de las unidades de A que recibe el nombre de F-grupo de álgebra.*

Sea $\psi : \mathbb{F}_q^+ \to \mathbb{C}$ un $\mathbb{C}$-carácter no trivial[1] cualquiera del grupo aditivo $\mathbb{F}_q^+$ y sea J^* el espacio dual de J. Para cada elemento $f \in J^*$, definimos la aplicación

$$\begin{aligned} \psi_f : (J,+) &\longrightarrow (\mathbb{C},\cdot) \\ a &\longrightarrow \psi(f(a)) \end{aligned}$$

Las funciones ψ_f con $f \in J^*$ son homomorfismos y por tanto, caracteres del grupo aditivo $(J,+)$. El resultado siguiente prueba que todos los caracteres irreducibles de este grupo tienen la forma ψ_f para algún $f \in J^*$.

Proposición 1.2.2 *Existe una aplicación biyectiva entre los elementos de J^* y los caracteres irreducibles del grupo aditivo $(J,+)$. Es más,*

$$Irr(J) = \{\psi_f : f \in J^*\}.$$

Demostración: Puesto que el grupo $(J,+)$ es abeliano, por la proposición 1.1.8 tenemos que $|J^*| = |J| = |Irr(J)| < \infty$; lo que prueba la primera parte del resultado.

Dados dos elementos $f, g \in J^*$, el producto de Frobenius de los caracteres ψ_f y ψ_g verifica

$$\begin{aligned} \langle \psi_f, \psi_g \rangle_{(J,+)} &= \frac{1}{|J|} \sum_{a \in J} \psi_f(a)\overline{\psi_g(a)} = \frac{1}{|J|} \sum_{a \in J} \psi(f(a) - g(a)) \\ &= \langle \psi_{f-g}, 1_J \rangle_J = \begin{cases} 1 & \text{si } f = g \\ 0 & \text{en otro caso} \end{cases} \end{aligned}$$

[1] Los detalles de esta construcción y su generalización a otro tipo de módulos se referirán en la sección 4.1

Por lo tanto, estas funciones forman un conjunto ortonormal de caracteres de $(J,+)$ y se sigue que $\{\psi_f : f \in J^*\} \subseteq Irr(J)$. Puesto que J es finito y $|\{\psi_f : f \in J^*\}| = |J|$, se tiene la igualdad. ■

Sea $G = 1 + J$ un grupo de álgebra cualquiera. Si J^* es el espacio dual de J, el grupo G actúa sobre J^* de la siguiente forma: dados un elemento x de G y un elemento f de J^*, la aplicación lineal f^x es un elemento de J^* definido por $f^x(a) = f(xax^{-1})$ para todo $a \in J$. Esta acción se conoce como *acción coadjunta* de G.

Denotamos por $\mathbf{\Omega}(G)$ al conjunto de todas las G-órbitas coadjuntas de J^*. Dada una órbita cualquiera $\mathcal{O} \in \mathbf{\Omega}(G)$, su cardinal $|\mathcal{O}|$ es una potencia de q^2 (proposición 2.1 de [7]).

Proposición 1.2.3 *Sea $f \in J^*$ un elemento cualquiera. El estabilizador de f para la acción coadjunta de G es el conjunto*

$$C_G(f) = 1 + \{a \in J : f(ab) = f(ba),\ \forall b \in J\}.$$

Si $\mathcal{O}$ es la G-órbita coadjunta que contiene a f, entonces su cardinal $|\mathcal{O}|$ es una potencia de q^2.

Demostración: Dado $f \in J^*$, definimos la forma bilineal B_f como sigue:

$$\begin{aligned} B_f : J \times J &\to \mathbb{C} \\ (a,b) &\to f([a,b]) \end{aligned}$$

con $[a,b] = ab - ba$ el corchete de Lie de a, b.

El radical de la forma B_f es el conjunto

$$\begin{aligned} Rad(f) &= \{a \in J : f([ab]) = 0,\ \forall b \in J\} \\ &= \{a \in J : f(ab) = f(ba),\ \forall b \in J\}. \end{aligned}$$

Claramente $Rad(f)$ es un $\mathbb{F}_q$-subespacio vectorial de J multiplicativamente cerrado. Por tanto, $1 + Rad(f)$ es un subgrupo de G cuyos elementos verifican $f^x = f$. Por otra parte, si $x = 1+a \in G$ es un elemento que satisface $f^x = f$, es fácil comprobar que $a \in Rad(f)$. Así pues, el estabilizador de f para la acción coadjunta será el conjunto $C_G(f) = 1 + Rad(f)$.

En cuanto al cardinal de las órbitas, basta observar que la forma B_f es antisimétrica. Entonces, si $dimJ = n$, se puede encontrar una $\mathbb{F}_q$-base de J, $(e_1, \ldots, e_n)$, en la que la matriz coordenada de B_f es de la forma

$$M(f) = \begin{pmatrix} X & 0 \\ 0 & 0 \end{pmatrix},$$

donde $X = diag(d_1 J, \ldots, d_t J)$ es una matriz diagonal por bloques con $d_i \neq 0$ para todo i y $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Así pues, el rango de $M(f)$ es un número par y si $\mathcal{O}$ es la órbita coadjunta que contiene a f, su cardinal

$$|\mathcal{O}| = q^{dim\, J - dim\, Rad(f)} = q^{rg\,(M(f))}$$

es una potencia de q^2. ■

A cada órbita coadjunta $\mathcal{O} \in \mathbf{\Omega}(G)$ le asociamos la función $\phi_{\mathcal{O}}$ definida como

$$\begin{array}{rcl} \phi_{\mathcal{O}} : G & \longrightarrow & \mathbb{C} \\ 1 + a & \longrightarrow & \dfrac{1}{\sqrt{|\mathcal{O}|}} \displaystyle\sum_{f \in \mathcal{O}} \psi_f(a). \end{array} \tag{1.2}$$

Estas funciones reciben el nombre de *funciones de Kirillov*. Notemos que todas ellas son funciones de clase de G, sin embargo no todas son caracteres (irreducibles). Aún así, constituyen una base ortonormal para el producto de Frobenius del espacio $cf(G)$ y satisfacen una expresión parecida a la Segunda Relación de Ortogonalidad (ver teorema 1.1.12).

Puesto que serán de utilidad más adelante, recogemos aquí estas propiedades tal y como aparecen en las proposiciones 2.2 y 2.3 y en el corolario 2.1 de [7].

Proposición 1.2.4 *El conjunto* $\{\phi_{\mathcal{O}} : \mathcal{O} \in \mathbf{\Omega}(G)\}$ *es una base ortonormal para el producto de Frobenius del* $\mathbb{C}$*-espacio vectorial* $cf(G)$ *de las funciones de clase de* G*. En particular se tiene que*

$$\frac{1}{|G|}\sum_{x\in G}\phi_{\mathcal{O}}(x)\overline{\phi_{\mathcal{O}'}(x)} = \delta_{\mathcal{O},\mathcal{O}'},$$

para todo $\mathcal{O}, \mathcal{O}' \in \mathbf{\Omega}(G)$*.*

Demostración: Sean $\mathcal{O}$ y $\mathcal{O}'$ dos órbitas coadjuntas de J^*. El producto de Frobenius de las funciones $\phi_{\mathcal{O}}$ y $\phi_{\mathcal{O}'}$ será

$$\langle \phi_{\mathcal{O}}, \phi_{\mathcal{O}'} \rangle_G = \frac{1}{\sqrt{|\mathcal{O}|}}\frac{1}{\sqrt{|\mathcal{O}'|}}\sum_{f\in\mathcal{O}}\sum_{f'\in\mathcal{O}'}\langle \psi_f, \psi_{f'}\rangle_J.$$

Puesto que los caracteres ψ_f y $\psi_{f'}$ son irreducibles (ver proposición 1.2.2), se sigue que $\langle \psi_f, \psi_{f'}\rangle_J = \delta_{f,f'}$. Con sólo sustituir en la expresión anterior llegamos a $\langle \phi_{\mathcal{O}}, \phi_{\mathcal{O}'}\rangle_G = \delta_{\mathcal{O},\mathcal{O}'}$.

Ahora sólo resta probar que el conjunto $\{\phi_{\mathcal{O}} : \mathcal{O} \in \mathbf{\Omega}(G)\}$ genera el espacio $cf(G)$. Para ello, basta ver que el cardinal $|\mathbf{\Omega}(G)|$ es igual al número de clases de conjugación de G. La demostración se basa en el teorema de Brauer (teorema 6.25 de [42]) y es similar a la de la proposición 2.4.3, por lo que se omite y se remite al lector interesado a la proposición 2.2 de [7]. ■

Las funciones de Kirillov satisfacen la siguiente relación, similar a la del teorema 1.1.12.

Proposición 1.2.5 *Sean* $x, y \in G$ *arbitrarios, entonces*

$$\sum_{\mathcal{O}\in\mathbf{\Omega}(G)}\phi_{\mathcal{O}}(x)\overline{\phi_{\mathcal{O}}(y)} = \begin{cases} |C_G(x)| & \text{si } x \text{ e } y \text{ son } G\text{-conjugados,} \\ 0 & \text{en otro caso.} \end{cases}$$

Demostración: Sean $a, b \in J$ tales que $x = 1 + a$ e $y = 1 + b$. Notemos que si $z \in G$, entonces $z^{-1}yz = 1 + z^{-1}bz$, puesto que la multiplicación del grupo es la misma que la del álgebra. Así pues, podemos llegar a la siguiente expresión:

$$\begin{aligned}\sum_{\mathcal{O}\in\mathbf{\Omega}(G)} \phi_{\mathcal{O}}(x)\overline{\phi_{\mathcal{O}}(y)} &= \sum_{\mathcal{O}\in\mathbf{\Omega}(G)} \frac{1}{|G|} \sum_{f\in\mathcal{O}} \frac{1}{|C_G(f)|} \sum_{z\in G} \psi_f(a)\overline{\psi_f(z^{-1}bz)} \\ &= \frac{1}{|G|} \sum_{z\in G} \sum_{f\in J^*} \psi_f(a - z^{-1}bz) = \frac{1}{|G|} \sum_{z\in G} \rho_J(a - z^{-1}bz),\end{aligned}$$

con ρ_J el carácter regular de $(J, +)$. Por lo tanto:

$$\sum_{\mathcal{O}\in\mathbf{\Omega}(G)} \phi_{\mathcal{O}}(x)\overline{\phi_{\mathcal{O}}(y)} = \sum_{z\in G} \delta_{a,z^{-1}bz} = |\{z \in G : a = z^{-1}bz\}|.$$

Si x e y no son G-conjugados, claramente $|\{z \in G : a = z^{-1}bz\}| = 0$. Supongamos que lo sean, entonces existe $u \in G$ tal que $u^{-1}bu = a$ y se verifica

$$|\{z \in G : a = z^{-1}bz\}| = |C_G(y)u| = |C_G(y)| = |C_G(x)|.$$

De donde se sigue la fórmula propuesta. ■

Como consecuencia, encontramos la siguiente descomposición para el carácter regular ρ_G que se utilizará en la demostración del teorema 2.3.4.

Corolario 1.2.6 *Sea ρ_G el carácter regular de G, entonces*

$$\rho_G = \sum_{\mathcal{O}\in\mathbf{\Omega}(G)} \phi_{\mathcal{O}}(1)\phi_{\mathcal{O}}.$$

Demostración: Sea $x \in G$ un elemento cualquiera. Por la proposición anterior sabemos que

$$\sum_{\mathcal{O}\in\mathbf{\Omega}(G)} \phi_{\mathcal{O}}(1)\phi_{\mathcal{O}}(x) = \delta_{x,1}\,|G|,$$

que es la definición del carácter regular ρ_G (ver proposición 1.1.9). ■

Por último, añadiremos algunos comentarios sobre las funciones de Kirillov y su relación con los caracteres irreducibles de G. Como se ha dicho, estas funciones no son, en general, caracteres. No obstante, debido a sus propiedades e inspirado en [47], Kirillov llegó a pensar que los caracteres irreducibles de $\mathbf{U}_n(q)$ tendrían esa forma (ver conjetura 2.2.1 de [49]). La conjetura resultó ser falsa, como se puede apreciar en [43] donde Isaacs y Karagueuzian encuentran un contraejemplo.

Sin embargo, a veces es posible encontrar los caracteres irreducibles de G a partir de las funciones $\phi_{\mathcal{O}}$ (para los detalles, consultar [7]). Es el caso cuando la característica de $\mathbb{F}_q$ es suficientemente grande. Entonces, $a^p = 0$ para todo $a \in J$, y así $(1+a)^p = 1$ para todo $a \in J$; por lo que G tiene exponente p. Así pues, podemos definir la función exponencial, $\exp : J \to G$, como la suma finita

$$\exp(a) = 1 + a + \frac{1}{2!}a^2 + \cdots + \frac{1}{(p-1)!}a^{p-1}.$$

Esta función es biyectiva y su inversa viene dada por la función $\ln : J \to G$ definida por

$$\ln(1+a) = a - \frac{1}{2}a^2 + \frac{1}{3}a^3 + \cdots + \frac{(-1)^p}{p-1}a^{p-1}.$$

La función $\theta : J \times J \to J$ dada por $\theta(a,b) = \ln(\exp(a)\exp(b))$ para todo $a, b \in J$, permite escribir $\exp(a)\exp(b) = \exp(\theta(a,b))$. Si la característica p es suficientemente grande podemos aplicar la fórmula de Campbell-Haussdorff (ver [44]) y expresar $\theta(a,b)$ como suma de conmutadores de Lie de los elementos a, b. En estas condiciones, para cada $\mathcal{O} \in \mathbf{\Omega}(G)$ la aplicación

$$\begin{aligned} \chi_{\mathcal{O}} : G &\longrightarrow \mathbb{C} \\ x &\longrightarrow \phi_{\mathcal{O}}(1 + \ln(x)) \end{aligned}$$

es un carácter irreducible de G. Es más, se puede deducir el siguiente resultado (teorema 6.1 de [7]).

Teorema 1.2.7 *La aplicación $\mathcal{O} \mapsto \chi_{\mathcal{O}}$ define una correspondencia biyectiva entre el conjunto $\mathbf{\Omega}(G)$ de todas las órbitas coadjuntas de G y el conjunto de los caracteres irreducibles de G. Para cada $\mathcal{O} \in \mathbf{\Omega}(G)$, se tiene que $\chi_{\mathcal{O}} \in Irr(G)$ tiene grado $\sqrt{|\mathcal{O}|}$. Además, cada carácter irreducible de G es inducido por un carácter lineal de un subgrupo de álgebra del grupo G.*

1.3. Caracteres básicos

En esta sección estudiaremos los caracteres básicos del grupo $\mathbf{U}_n(q)$. Si $\mathfrak{u}_n(q)$ es el $\mathbb{F}_q$-espacio vectorial de todas las matrices nilpotentes de grado n sobre $\mathbb{F}_q$ que son triangulares superiores, es claro que $J(\mathbf{U}_n(q)) = \mathfrak{u}_n(q)$ y puesto que

$$\mathbf{U}_n(q) = 1 + \mathfrak{u}_n(q) = \{1 + a : a \in J(\mathbf{U}_n(q))\},$$

deducimos que $\mathbf{U}_n(q)$ es un grupo de álgebra de acuerdo con 1.2.1.

Sea $\Phi(n) = \{(i,j) : 1 \leq i < j \leq n\}$, para cada elemento $(i,j) \in \Phi(n)$ denotaremos por e_{ij} a la matriz elemental $e_{ij} = (\delta_{ki}\delta_{lj})_{1\leq k,l,\leq n}$. Claramente, el conjunto $\{e_{ij} : (i,j) \in \Phi(n)\}$ es una base del $\mathbb{F}_q$-espacio vectorial $\mathfrak{u}_n(q)$.

Si $\mathfrak{u}_n(q)^*$ es el espacio dual de $\mathfrak{u}_n(q)$, a partir de la base anterior podemos definir la correspondiente base dual $\{e_{ij}^* : (i,j) \in \Phi(n)\}$. Cada elemento e_{ij}^* satisface $e_{ij}^*(e_{kl}) = \delta_{ik}\delta_{jl}$, para todo $(k,l) \in \Phi(n)$. En consecuencia, si a es un elemento cualquiera de $\mathfrak{u}_n(q)$, $e_{ij}^*(a) = a_{ij}$.

De acuerdo con lo expuesto en la sección anterior, consideramos ψ un carácter no trivial del grupo aditivo $\mathbb{F}_q^+$. Por la proposición 1.2.2, los caracteres irreducibles del grupo aditivo $\mathfrak{u}_n(q)^+$ son

$$Irr(\mathfrak{u}_n(q)^+) = \{\psi_f : f \in \mathfrak{u}_n(q)^*\},$$

con $\psi_f : \mathfrak{u}_n(q) \to \mathbb{C}$ dado por $\psi_f(a) = \psi(f(a))$ para todo $a \in \mathfrak{u}_n(q)$.

Sea $(i,j) \in \Phi(n)$ y sea α un elemento no nulo cualquiera de $\mathbb{F}_q$. Si $\mathcal{O}_{ij}(\alpha)$ es la órbita coadjunta que contiene al elemento αe_{ij}^*, probaremos que la función de Kirillov $\phi_{\mathcal{O}_{ij}(\alpha)}$ asociada a esta órbita es un carácter irreducible de $\mathbf{U}_n(q)$ llamado *carácter elemental*. Cada uno de estos caracteres se denota como $\xi_{ij}(\alpha)$ con $(i,j) \in \Phi(n)$, $\alpha \in \mathbb{F}_q^*$, y es inducido por un carácter lineal de un cierto subgrupo de $\mathbf{U}_n(q)$. Este resultado constituye el lema 2 de [9] que reproducimos a continuación.

Lema 1.3.1 *Sea $(i,j) \in \Phi(n)$ y sea $\alpha \in \mathbb{F}_q^*$. La función de Kirillov $\xi_{ij}(\alpha)$ es un carácter irreducible de $\mathbf{U}_n(q)$. Es más, si $\mathbf{U}_{ij}(q) = \{X \in \mathbf{U}_n(q) : x_{ik} = 0,\ i < k < j\} \leq \mathbf{U}_n(q)$ y si $\lambda_{ij}(\alpha) : \mathbf{U}_{ij}(q) \to \mathbb{C}$ es la función definida como $\lambda_{ij}(\alpha)(x) = \psi(\alpha\, x_{ij})$ para todo $X \in \mathbf{U}_{ij}(q)$, entonces $\lambda_{ij}(\alpha)$ es un carácter lineal de $\mathbf{U}_{ij}(q)$ y $\xi_{ij}(\alpha) = \lambda_{ij}(\alpha)^{\mathbf{U}_n(q)}$ es el carácter inducido por este carácter lineal.*

Demostración: Puesto que las funciones de Kirillov son una base ortonormal de $cf(G)$, proposición 1.2.4, $\langle \xi_{ij}(\alpha), \xi_{ij}(\alpha) \rangle = 1$, por lo que bastará probar que la función $\xi_{ij}(\alpha)$ es un carácter de $\mathbf{U}_n(q)$.

Sean X, Y dos elementos cualesquiera de $\mathbf{U}_{ij}(q)$. Puesto que $x_{ik} = 0$ (resp. y_{ik}) para $i < k < j$, se sigue que $(XY)_{ij} = x_{ij} + y_{ij}$, y entonces

$$\lambda_{ij}(\alpha)(XY) = \psi(\alpha\,(x_{ij} + y_{ij})) = \psi(\alpha\, x_{ij})\,\psi(\alpha\, y_{ij}),$$

de donde se deduce que $\lambda_{ij}(\alpha)$ es un carácter lineal de $\mathbf{U}_{ij}(q)$.

El carácter inducido $\lambda_{ij}(\alpha)^{\mathbf{U}_n(q)}$ será una combinación lineal con coeficientes complejos de las funciones de clase $\phi_{\mathcal{O}}$ con $\mathcal{O} \in \mathbf{\Omega}_n(q)$. La proposición 2 de [9] nos permite garantizar que estos coeficientes son enteros no negativos.

Denotaremos por $\mathfrak{u}_{ij}(q)$ el $\mathbb{F}_q$-subespacio vectorial de $\mathfrak{u}_n(q)$ formado por aquellas matrices de la forma $X - 1$ con $X \in \mathbf{U}_{ij}(q)$, es decir, $\mathbf{U}_{ij}(q) =$

$1+\mathfrak{u}_{ij}(q)$. Sea $f=\alpha e_{ij}^* \in \mathfrak{u}_n(q)^*$ y sea $f_0 \in \mathfrak{u}_{ij}(q)^*$ su restricción a $\mathfrak{u}_{ij}(q)$. Puesto que $f(ab)=0$ para todo $a,b \in \mathfrak{u}_{ij}(q)$, $\{f_0\}$ es una $\mathbf{U}_{ij}(q)$-órbita coadjunta en $\mathfrak{u}_{ij}(q)^*$ y $\lambda_{ij}(\alpha)$ es la función de Kirillov asociada a la órbita $\{f_0\}$ en $\mathfrak{u}_n(q)^*$. A partir de la reciprocidad de Frobenius (proposición 1.1.15) y de la proposición 2 de [9] se sigue que

$$\langle \lambda_{ij}(\alpha)^{\mathbf{U}_n(q)}, \xi_{ij}(\alpha)\rangle_{\mathbf{U}_n(q)} = \langle \lambda_{ij}(\alpha), \xi_{ij}(\alpha)\rangle_{\mathbf{U}_{ij}(q)} \neq 0.$$

Por último sólo falta comprobar que $\lambda_{ij}(\alpha)^{\mathbf{U}_n(q)}(1) = \xi_{ij}(\alpha)(1)$. Ahora bien, puesto que $\lambda_{ij}(\alpha)^{\mathbf{U}_n(q)}(1) = |\mathbf{U}_n(q) : \mathbf{U}_{ij}(q)| = q^{j-i-1}$ y $\xi_{ij}(\alpha)(1) = \sqrt{|\mathcal{O}_{ij}(\alpha)|}$, sólo es preciso ver que $|\mathcal{O}_{ij}(\alpha)| = q^{2(j-i-1)}$.

El estabilizador de f en $\mathbf{U}_n(q)$, $C_{\mathbf{U}_n(q)}(f)$, está formado por todas aquellas matrices que satisfacen $x_{ik}=x_{kj}$ con $i<k<j$. Entonces $|\mathcal{O}_{ij}(\alpha)| = |\mathbf{U}_n(q) : C_{\mathbf{U}_n(q)}(f)| = q^{2(j-i-1)}$. ■

Definición 1.3.2 *El (i,j)-carácter elemental de $\mathbf{U}_n(q)$ asociado a α es el carácter irreducible $\xi_{ij}(\alpha)$.*

Una parte de los caracteres irreducibles de $\mathbf{U}_n(q)$ se puede obtener como producto de caracteres inducidos (ver [63]). Inspirados en esta propiedad, definiremos los *caracteres básicos* como productos de *caracteres elementales*. Como paso preliminar, introducimos la noción de *conjunto básico*.

Definición 1.3.3 *Un subconjunto $D \subseteq \Phi(n)$ se dice básico si satisface estas dos propiedades:*

- $|D \cap \{(i,j) : i<j\leq n\}| \leq 1$, *para todo* $1 \leq i < n$;
- $|D \cap \{(i,j) : 1 \leq i < j\}| \leq 1$ *para todo* $1 < j \leq n$.

Es fácil ver que el conjunto vacío es un conjunto básico. Por otra parte, si $a \in \mathfrak{u}_n(q)$ es una matriz que tiene a lo sumo un elemento diferente de cero en cada fila y en cada columna, el conjunto D de sus posiciones no nulas es un conjunto básico. Es más, todo conjunto básico es de esta forma.

Definición 1.3.4 *Sean D un conjunto básico y $\varphi : D \to \mathbb{F}_q^*$ una aplicación arbitraria. El carácter básico $\xi_D(\varphi)$ es el producto de caracteres básicos indicados por el conjunto D. Es decir,*

$$\xi_D(\varphi) = \prod_{(i,j)\in D} \xi_{ij}(\alpha_{ij}), \tag{1.3}$$

con $\alpha_{ij} = \varphi(i,j)$ para todo $(i,j) \in D$.

Notemos que el carácter trivial $1_{\mathbf{U}_n(q)}$ es también un carácter básico, pues se corresponde con $D = \emptyset$ y con la función vacía.

Los caracteres básicos poseen dos propiedades fundamentales: por una parte, su definición es puramente combinatoria, y por otra, determinan una partición de los caracteres irreducibles de $\mathbf{U}_n(q)$. De hecho, es posible probar el siguiente resultado (teorema 1 de [9]).

Teorema 1.3.5 *Sea χ un carácter irreducible de $\mathbf{U}_n(q)$. Entonces χ es constituyente de un único carácter básico de $\mathbf{U}_n(q)$, es decir, existe un único conjunto básico D y una única función $\varphi : D \to \mathbb{F}_q^*$ tal que χ es constituyente de $\xi_D(\varphi)$.*

La demostración de este resultado se encuentra en [9], por lo que sólo la esbozaremos. Aún así, intentaremos poner de relieve aquellas técnicas que servirán para demostrar resultados parecidos en otras secciones de esta tesis.

El teorema se demuestra si se consigue probar que los caracteres básicos son ortogonales dos a dos y si se puede escribir el carácter regular $\rho_{\mathbf{U}_n(q)}$ como una combinación lineal de ellos.

Dados un conjunto básico D y una función cualquiera $\varphi : D \to \mathbb{F}_q^*$, la subvariedad básica de $\mathfrak{u}_n(q)^*$ asociada al par (D, φ), se define como la suma de órbitas coadjuntas (ver [5])

$$\mathcal{O}_D(\varphi) = \sum_{(i,j)\in D} \mathcal{O}_{ij}(\alpha_{ij}),$$

con $\alpha_{ij} = \varphi(i,j)$ para todo $(i,j) \in D$. Notemos que un elemento de la subvariedad básica es una suma de $|D|$ elementos, cada uno de ellos en una órbita $\mathcal{O}_{ij}(\alpha_{ij})$. En el caso en que (D, φ) sea el par formado por el conjunto vacío y la función vacía, la subvariedad $\mathcal{O}_D(\varphi) = 0$.

Puesto que la subvariedad básica $\mathcal{O}_D(\varphi)$ es invariante para la acción coadjunta de $\mathbf{U}_n(q)$, está constituida por unión de órbitas coadjuntas. El interés en considerar este tipo de variedades se centra en que permite relacionar los constituyentes del carácter básico $\xi_D(\varphi)$ con las órbitas coadjuntas contenidas en la variedad básica $\mathcal{O}_D(\varphi)$. Esta relación queda patente en el corolario 1 de [9] que recogemos a continuación

Corolario 1.3.6 *Sean D un subconjunto básico de $\Phi(n)$ y $\varphi : D \to \mathbb{F}_q^*$ una función. Sea $\mathcal{O} \in \mathbf{\Omega}_n(q)$ una órbita coadjunta arbitraria. Entonces la función de Kirillov $\phi_{\mathcal{O}}$ es un constituyente del carácter básico $\xi_D(\varphi)$ si y sólo si $\mathcal{O} \subseteq \mathcal{O}_D(\varphi)$. Es más, el producto escalar $\langle \phi_{\mathcal{O}}, \xi_D(\varphi) \rangle_{\mathbf{U}_n(q)}$ es un entero no negativo.*

Por tanto, el problema de establecer la ortogonalidad de los caracteres básicos queda reducido a la descomposición de las subvariedades básicas en órbitas coadjuntas. Por otra parte, el espacio $\mathfrak{u}_n(q)^*$ se puede escribir como una unión disjunta de subvariedades básicas tal como se puede encontrar en el teorema 1 de [5]. Así,

$$\mathfrak{u}_n(q)^* = \bigcup_{D,\varphi} \mathcal{O}_D(\varphi), \tag{1.4}$$

donde D recorre todos los posibles subconjuntos básicos de $\Phi(n)$ y φ todas las posibles funciones $\varphi : D \to \mathbb{F}_q^*$.

La ortogonalidad de los caracteres básicos se prueba en el resultado siguiente (proposición 4 de [9]).

Proposición 1.3.7 *Sean D y D' subconjuntos básicos de $\Phi(n)$, y $\varphi : D \to \mathbb{F}_q$ y $\varphi' : D' \to \mathbb{F}_q^*$ funciones cualesquiera. Entonces, el producto escalar $\langle \xi_D(\varphi), \xi_{D'}(\varphi') \rangle \neq 0$ si y sólo si $D = D'$ y $\varphi = \varphi'$.*

Demostración: Si D es un conjunto básico y $\varphi : D \to \mathbb{F}_q^*$ es una función cualquiera, denotaremos por $\mathbf{\Omega}_D(\varphi)$ al conjunto de órbitas coadjuntas $\mathcal{O}$ contenidas en $\mathcal{O}_D(\varphi)$. Por tanto, el carácter básico $\xi_D(\varphi)$ se podrá descomponer de la siguiente forma:

$$\xi_D(\varphi) = \sum_{\mathcal{O} \in \mathbf{\Omega}_D(\varphi)} n_{\mathcal{O}}\, \phi_{\mathcal{O}},$$

donde, por el corolario 1.3.6, cada escalar $n_{\mathcal{O}}$ es un entero positivo. Así pues,

$$\langle \xi_D(\varphi), \xi_{D'}(\varphi') \rangle_{\mathbf{U}_n(q)} = \sum_{\mathcal{O} \in \mathbf{\Omega}_D(\varphi)} n_{\mathcal{O}}\, \langle \phi_{\mathcal{O}}, \xi_{D'}(\varphi') \rangle_{\mathbf{U}_n(q)}$$

y entonces $\langle \xi_D(\varphi), \xi_{D'}(\varphi') \rangle_{\mathbf{U}_n(q)} \neq 0$ si y sólo si el producto de Frobenius $\langle \phi_{\mathcal{O}}, \xi_{D'}(\varphi') \rangle \neq 0$ para algún $\mathcal{O} \in \mathbf{\Omega}_D(\varphi)$. Por el corolario 1.3.6, se cumple que $\langle \xi_D(\varphi), \xi_{D'}(\varphi') \rangle \neq 0$ si y sólo si $\mathbf{\Omega}_D(\varphi) \cap \mathbf{\Omega}_{D'}(\varphi') \neq \emptyset$. Puesto que la unión de (1.4) es disjunta, el resultado se sigue. ■

La descomposición del carácter regular $\rho_{\mathbf{U}_n(q)}$ como suma de caracteres básicos viene dada por el teorema 2 de [9] y es una generalización de los resultados obtenidos para $p \geq n$ en [6] y [8]. La incluimos sin demostración.

Teorema 1.3.8 *Sea $\rho_{\mathbf{U}_n(q)}$ el carácter regular de $\mathbf{U}_n(q)$. Entonces*

$$\rho_{\mathbf{U}_n(q)} = \sum_{D,\varphi} \frac{q^{s(D)}}{\xi_D(\varphi)(1)}\, \xi_D(\varphi),$$

la suma se extiende sobre todos los conjuntos básicos D *de* $\Phi(n)$ *y sobre todas las funciones* $\varphi : D \to \mathbb{F}_q^*$. *Para cada conjunto básico* D, $s(D)$ *representa la cardinalidad del subconjunto de* $\Phi(n)$ *definido como* $S(D) = \bigcup_{(i,j)\in D}\{(i,k) : i < k < j\}$.

Por último, sólo falta probar que estas dos condiciones bastan para demostrar el teorema 1.3.5. Supongamos que χ es un carácter irreducible cualquiera de $\mathbf{U}_n(q)$. Entonces, χ es un constituyente del carácter regular $\rho_{\mathbf{U}_n(q)}$. Del teorema 1.3.8 se sigue que χ debe ser constituyente de uno de los caracteres básicos $\xi_D(\varphi)$. La unicidad de $\xi_D(\varphi)$ se desprende de la ortogonalidad de los caracteres básicos demostrada en la proposición 1.3.7.

1.4. Caracteres de transición

En la última parte de este capítulo revisaremos brevemente el método de los caracteres de transición desarrollado por Yan (ver [82]). Está basado en el método de las órbitas de Kirillov (ver [48] y [50]) y es equivalente al método de los caracteres básicos que se ha desarrollado en la sección anterior.

El punto de partida es considerar las acciones del grupo $\mathbf{U}_n(q)$ sobre el álgebra $\mathfrak{u}_n(q)$ y sobre el espacio dual $\mathfrak{u}_n(q)^*$. Así, para todo $X \in \mathbf{U}_n(q)$, $a \in \mathfrak{u}_n(q)$ las operaciones

$$\begin{aligned} X \cdot a &\to Xa \quad && \textit{acción de transición izquierda}, \\ a \cdot X &\to aX \quad && \textit{acción de transición derecha}, \\ a^X &\to X^{-1}aX \quad && \textit{acción adjunta}, \end{aligned} \tag{1.5}$$

definen tres acciones del grupo $\mathbf{U}_n(q)$ sobre el álgebra $\mathfrak{u}_n(q)$. Nótese que la operación implicada es el producto ordinario de matrices. Las dos primeras acciones conmutan entre sí y definen una acción doble de $\mathbf{U}_n(q)$ sobre $\mathfrak{u}_n(q)$

que recibirá el nombre de acción de transición. Si $a \in \mathfrak{u}_n(q)$ es un elemento cualquiera, la órbita de transición que lo contiene es el conjunto

$$\mathbf{U}_n(q) \cdot a \cdot \mathbf{U}_n(q) = \{X\, a\, Y : X, Y \in \mathbf{U}_n(q)\},$$

que es estable para la acción adjunta de $\mathbf{U}_n(q)$ y por tanto, es unión de órbitas adjuntas.

De forma similar, $\mathbf{U}_n(q)$ actúa sobre el dual $\mathfrak{u}_n(q)^* = Hom_{\mathbb{F}_q}(\mathfrak{u}_n(q), \mathbb{F}_q)$ de tres formas diferentes. Así, para todo $f \in \mathfrak{u}_n(q)^*$, $X \in \mathbf{U}_n(q)$, $a \in \mathfrak{u}_n(q)$, las operaciones

$$\begin{aligned} &(X \cdot f)(a) = f(aX) \quad \textit{acción de cotransición izquierda},\\ &(f \cdot X)(a) = f(Xa) \quad \textit{acción de cotransición derecha},\\ &f^X(a) = f(XaX^{-1}) \quad \textit{acción coadjunta}, \end{aligned} \tag{1.6}$$

definen tres acciones del grupo $\mathbf{U}_n(q)$ sobre el dual $\mathfrak{u}_n(q)^*$. Las acciones de cotransición derecha e izquierda conmutan y dan lugar a una acción doble de $\mathbf{U}_n(q)$ que recibe el nombre de acción de cotransición. Si $f \in \mathfrak{u}_n(q)^*$ es un elemento arbitrario, la órbita de cotransición que contiene a f es el conjunto

$$\mathbf{\Psi}_f = \mathbf{U}_n(q) \cdot f \cdot \mathbf{U}_n(q) = \{X \cdot f \cdot Y : X, Y \in \mathbf{U}_n(q)\},$$

que es estable para la acción coadjunta y que por ello se podrá escribir como unión de órbitas coadjuntas.

Sea $\psi : (\mathbb{F}_q, +) \to (\mathbb{C}^*, \cdot)$ un carácter complejo no trivial del grupo aditivo $(\mathbb{F}_q, +)$ y sea $\mathbb{C}[\mathbf{U}_n(q)]$ el conjunto de todas las funciones complejas definidas sobre $\mathbf{U}_n(q)$. Para cada elemento $f \in \mathfrak{u}_n(q)^*$ consideramos la función $v(f) \in \mathbb{C}[\mathbf{U}_n(q)]$ definida por

$$\begin{aligned} v(f) : \mathbf{U}_n(q) &\longrightarrow \mathbb{C}\\ X &\longrightarrow \psi[f(X - Id)] = \psi_f(X - Id) \end{aligned}$$

Como consecuencia de la proposición 1.2.2, el conjunto $\{v(f) : f \in \mathfrak{u}_n(q)^*\}$ es una base ortonormal de $\mathbb{C}[\mathbf{U}_n(q)]$ como espacio vectorial complejo.

El grupo $\mathbf{U}_n(q)$ actúa sobre el espacio vectorial $\mathbb{C}[\mathbf{U}_n(q)]$ transformándolo en un $\mathbf{U}_n(q)$-módulo por la **izquierda**. Así, para cada $X \in \mathbf{U}_n(q)$ y cada elemento $v \in \mathbb{C}[\mathbf{U}_n(q)]$ la acción $X \curvearrowright v$ se define como

$$\begin{aligned} X \curvearrowright v : \mathbf{U}_n(q) &\longrightarrow \mathbb{C} \\ Y &\longrightarrow v(YX) \end{aligned}$$

El módulo $\mathbb{C}[\mathbf{U}_n(q)]$ está asociado a una representación de $\mathbf{U}_n(q)$ que es equivalente a la representación regular. Su descomposición en términos de la base $\{v(f) : f \in \mathfrak{u}_n(q)^*\}$ nos dará los módulos de transición, que constituyen la parte central de esta sección. En primer lugar estudiamos la acción del grupo sobre los elementos $v(f)$.

Proposición 1.4.1 *Sea $X \in \mathbf{U}_n(q)$ y sea $v(f)$ un elemento de la base de $\mathbb{C}[\mathbf{U}_n(q)]$, entonces*

$$X \curvearrowright v(f) = [v(f)(X)]\, v(X \cdot f).$$

Demostración: Por definición, $v(f)(Y) = \psi_f(Y - Id)$. Por tanto, $X \curvearrowright v(f)(Y) = \psi_f(YX - Id)$. Ahora bien:

$$\begin{aligned} \psi_f(YX - Id) &= \psi_f(YX - X + X - Id) = \psi_f(X - Id)\psi_f((Y - Id)X) \\ &= \psi_f(X - Id)\psi_{X.f}(Y - Id) = [v(f)(X)]v(X \cdot f)(Y). \end{aligned}$$

■

La primera consecuencia que se desprende de esta proposición es que si L es una órbita en $\mathfrak{u}_n(q)$ para la acción de transición **izquierda**, entonces el $\mathbb{C}$-subespacio vectorial de $\mathbb{C}[\mathbf{U}_n(q)]$ generado por el conjunto $\{v(f) : f \in L\}$ es un submódulo de la representación regular de $\mathbf{U}_n(q)$ que denotamos por

$V(L)$ y cuya traza es $\chi(L)$. Por construcción, dim $V(L) = \chi(L)(1)$ es el cardinal de la órbita L. Además

$$\mathbb{C}[\mathbf{U}_n(q)] = \bigoplus_L V(L),$$

donde L recorre todas las órbitas de transición **izquierda** de $\mathfrak{u}_n(q)^*$. Por otra parte, el módulo $V(L)$ está generado como módulo por cualquier $v(f)$ para el que f esté en la órbita L. Por este motivo, en adelante escribiremos $V(f) = V(L)$ y $\chi(f) = \chi(L)$ con independencia del representante elegido. Los módulos $V(f)$ se conocen como *módulos de transición* y los caracteres $\chi(f)$ como *caracteres de transición.*

Proposición 1.4.2 *Sean f y f' dos elementos de $\mathfrak{u}_n(q)^*$ en la misma órbita de transición **derecha**, entonces los módulos de transición $V(f)$ y $V(f')$ son isomorfos.*

Demostración: Sea $X \in \mathbf{U}_n(q)$ tal que $f' = f \cdot X$. Para cada $v \in \mathbb{C}[\mathbf{U}_n(q)]$, la acción **derecha** de X viene dada por $v \curvearrowleft X(Y) = v(XY)$, para todo $Y \in \mathbf{U}_n(q)$. Es fácil ver que la aplicación

$$\begin{aligned} \varphi_X : \mathbb{C}[\mathbf{U}_n(q)] &\longrightarrow \mathbb{C}[\mathbf{U}_n(q)] \\ v &\longrightarrow v \curvearrowleft X \end{aligned}$$

es un isomorfismo de módulos. De forma similar a lo que sucedía para la acción **izquierda** se verifica que

$$\varphi_X(v(f)) = v(f) \curvearrowleft X = [v(f)(X)]\, v(f \cdot X).$$

Así pues, φ_X transforma el módulo $V(f)$ en el módulo $V(f \cdot X) = V(f')$. ■

Corolario 1.4.3 *El carácter de transición $\chi(f)$ sólo depende de la órbita de cotransición $\mathbf{\Psi}_f$ que contiene a f. Es decir, $\chi(f) = \chi(\mathbf{\Psi}_f)$.*

Para cada órbita de cotransición $\mathbf{\Psi}$ el espacio vectorial de $\mathbb{C}[\mathbf{U}_n(q)]$ generado por el conjunto $V(\mathbf{\Psi}) = \{v(f) : f \in \mathbf{\Psi}\}$ es un submódulo de $\mathbb{C}[\mathbf{U}_n(q)]$ cuya dimensión es el cardinal $|\mathbf{\Psi}|$. Por otra parte, podemos escribir $\mathbb{C}[\mathbf{U}_n(q)]$ como suma directa de estos submódulos, con lo que se obtiene:

$$\mathbb{C}[\mathbf{U}_n(q)] = \bigoplus_{\mathbf{\Psi}} V(\mathbf{\Psi}),$$

donde $\mathbf{\Psi}$ recorre todas las órbitas de cotransición de $\mathfrak{u}_n(q)^*$. Por la proposición 1.4.2 cada módulo $V(\mathbf{\Psi})$ es suma directa de copias de módulos de transición isomorfos. Cada una de esas copias se corresponde con una órbita de transición **izquierda** contenida en $\mathbf{\Psi}$ y su traza es el carácter de transición $\chi(\mathbf{\Psi})$. Así pues, su dimensión es $\chi(\mathbf{\Psi})(1)$ y en consecuencia, el número de copias es $|\mathbf{\Psi}|/\chi(\mathbf{\Psi})(1)$. Por otra parte, la representación de $\mathbf{U}_n(q)$ asociada al módulo $\mathbb{C}[\mathbf{U}_n(q)]$ es equivalente a la representación regular y por ello su carácter es el carácter regular $\rho_{\mathbf{U}_n(q)}$. Si reunimos las dos expresiones, obtenemos el siguiente resultado.

Teorema 1.4.4 *El carácter regular* $\rho_{\mathbf{U}_n(q)}$ *se puede escribir como una combinación lineal de caracteres de transición. De hecho*

$$\rho_{\mathbf{U}_n(q)} = \sum_{\mathbf{\Psi}} \frac{|\mathbf{\Psi}|}{\chi(\mathbf{\Psi})(1)}\ \chi(\mathbf{\Psi}),$$

donde $\mathbf{\Psi}$ *recorre todas las órbitas de cotransición de* $\mathfrak{u}_n(q)^*$.

Sea $\mathbf{\Psi}$ una órbita de cotransición y sea L una órbita de cotransición **izquierda** contenida en ella. A partir de la proposición 1.4.1 se deduce que el carácter de transición asociado a $\mathbf{\Psi}$ se puede escribir como

$$\chi(\mathbf{\Psi})(X) = \sum_{X \cdot f = f} v(f)(X),$$

con $X \in \mathbf{U}_n(q)$ y la suma extendida a todos los elementos de la órbita L que están fijos por la acción de cotransición **izquierda** de X.

Puesto que el conjunto $\{v(f) : f \in \mathfrak{u}_n(q)^*\}$ forma una base ortonormal de $\mathbb{C}[\mathbf{U}_n(q)]$, también podemos escribir

$$\chi(\mathbf{\Psi})(X) = \sum_{f \in L} \langle v(X \cdot f), v(f) \rangle \; v(f)(X).$$

Si desarrollamos el producto de Frobenius, tras simplificar se llega a

$$\begin{aligned} \chi(\mathbf{\Psi})(X) &= \frac{1}{|\mathbf{U}_n(q)|} \sum_{f \in L} \sum_{Y \in \mathbf{U}_n(q)} [v(X \cdot f - f)(Y)\, v(f)(X)] \\ &= \frac{1}{|\mathbf{U}_n(q)|} \sum_{f \in L} \sum_{Y \in \mathbf{U}_n(q)} \psi_{f.Y}(X - Id). \end{aligned}$$

Notemos que cuando f recorre la órbita L e Y hace lo mismo con el grupo $\mathbf{U}_n(q)$, cada elemento $f \cdot Y \in \mathbf{\Psi}$ aparece con multiplicidad $\frac{|\mathbf{U}_n(q)|\,|L|}{|\mathbf{\Psi}|}$. Puesto que además $\chi(\mathbf{\Psi})(1) = \dim V(\mathbf{\Psi}) = |L|$, podemos escribir

$$\chi(\mathbf{\Psi})(X) = \frac{|L|}{|\mathbf{\Psi}|} \sum_{f \in \mathbf{\Psi}} \psi_f(X - Id) = \frac{\chi(\mathbf{\Psi})(1)}{|\mathbf{\Psi}|} \sum_{f \in \mathbf{\Psi}} \psi_f(X - Id).$$

Con lo que hemos encontrado una expresión para los caracteres de transición que sólo depende de la órbita de cotransición en $\mathfrak{u}_n(q)^*$. Si utilizamos la base ortonormal de $\mathbb{C}[\mathbf{U}_n(q)]$ llegamos a la siguiente expresión:

Teorema 1.4.5 *Sea $f \in \mathfrak{u}_n(q)^*$ un elemento cualquiera y sea $\mathbf{\Psi}$ la órbita de cotransición que lo contiene. El carácter de transición asociado a $\mathbf{\Psi}$ tiene la forma*

$$\chi(\mathbf{\Psi}) = \frac{\chi(\mathbf{\Psi})(1)}{|\mathbf{\Psi}|} \sum_{f \in \mathbf{\Psi}} v(f).$$

Una consecuencia inmediata, que se deriva de la ortonormalidad de la base $\{v(f) : f \in \mathfrak{u}_n(q)^*\}$, es el resultado siguiente.

Corolario 1.4.6 *Sean* $\mathbf{\Psi}$ *y* $\mathbf{\Psi}'$ *dos órbitas de cotransición, entonces el producto de Frobenius de los caracteres de transición asociados es*

$$\langle \chi(\mathbf{\Psi}), \chi(\mathbf{\Psi}') \rangle = \begin{cases} \dfrac{\chi(\mathbf{\Psi})(1)^2}{|\mathbf{\Psi}|} & \text{si } \mathbf{\Psi} = \mathbf{\Psi}', \\ 0 & \text{en otro caso.} \end{cases}$$

Una vez que hemos desarrollado las dos aproximaciones a los super-caracteres, sólo resta ver que son equivalentes. A este punto se dedicará la última parte de esta sección.

En primer lugar estudiaremos las órbitas de cotransición, pues éstas determinan los caracteres de transición. De esta forma veremos que cada una de ellas determina un único conjunto básico D (ver definición 1.3.3) y una única función $\varphi : D \to \mathbb{F}_q^*$. La descomposición del carácter de transición en producto de caracteres asociados a los elementos de D permitirá probar la igualdad entre caracteres de transición y caracteres básicos.

Sea $\{e_{ij} : 1 \leq i < j \leq n\}$ la base canónica de $\mathfrak{u}_n(q)$ y sea $\{e_{ij}^* : 1 \leq i < j \leq n\}$ su correspondiente base dual. Las acciones de cotransición vienen determinadas por la acción de los elementos de la forma $Id + \alpha_{ij}\, e_{ij}$ sobre los de la base dual. Así, la acción de cotransición **izquierda** viene dada por

$$(Id + \alpha_{ij}\, e_{ij}) \cdot e_{kl}^* = \begin{cases} e_{kj}^* + \alpha_{ij}\, e_{ki}^* & \text{si } l = j \text{ y } k < i, \\ e_{kl}^* & \text{en otro caso.} \end{cases} \tag{1.7}$$

Mientras que la de cotransición **derecha** lo hace por

$$e_{kl}^* \cdot (Id + \alpha_{ij}\, e_{ij}) = \begin{cases} e_{il}^* + \alpha_{ij}\, e_{jl}^* & \text{si } k = i \text{ y } l > j, \\ e_{kl}^* & \text{en otro caso.} \end{cases} \tag{1.8}$$

Conviene representar los elementos de $\mathfrak{u}_n(q)^*$ como si fuesen elementos de $\mathfrak{u}_n(q)$. Para ello, definimos la aplicación biyectiva

$$\begin{array}{rcl} \mathfrak{u}_n(q)^* & \longrightarrow & \mathfrak{u}_n(q) \\ f & \longrightarrow & M_f = \displaystyle\sum_{1 \leq i < j \leq n} f(e_{ij}) e_{ij} \end{array}$$

Con este convenio, la acción de cotransición **izquierda** de un elemento $X = Id + \alpha_{ij}\, e_{ij}$ sobre $f \in \mathfrak{u}_n(q)^*$ es una operación en las columnas de M_f que a cada elemento de la columna i por encima de la diagonal principal le suma α_{ij} veces el elemento que se encuentra a su derecha en la columna j.

Por otra parte, la acción de cotransición **derecha** de X sobre f es una operación en las filas de M_f que suma a cada elemento de la fila j a la derecha de la diagonal α_{ij} veces el elemento de la fila i que tiene sobre él.

Definimos el soporte de $f \in \mathfrak{u}_n(q)^*$ como el conjunto de posiciones (i, j) tales que $f(e_{ij}) \neq 0$, es decir, las posiciones no nulas de la matriz M_f y denotamos por $\mathcal{T}_n^*(q)$ el conjunto de elementos de $\mathfrak{u}_n(q)^*$ tales que su soporte contiene como máximo una posición diferente de cero en cada fila y cada columna.

El resultado siguiente es central en la identificación de caracteres básicos y de transición, pues permite encontrar un único representante en $\mathcal{T}_n^*(q)$ para cada órbita. Éste determina un par (D, φ) en las condiciones expresadas anteriormente.

Teorema 1.4.7 *Cada órbita de cotransición contiene un único representante en $\mathcal{T}_n^*(q)$. Es decir, las órbitas de cotransición están indicadas por los elementos de $\mathcal{T}_n^*(q)$.*

Demostración: Dado un elemento $f \in \mathfrak{u}_n(q)^*$, realizaremos operaciones de cotransición de forma que su matriz asociada M_f acabe por tener la forma requerida. Para ello, trabajamos por columnas y nos movemos de derecha a izquierda. Supongamos que ya tenemos reducidas las últimas k columnas de M_f. En la columna $n - k + 1$ podemos eliminar mediante operaciones de columna apropiadas, cotransiciones **izquierdas**, aquellos elementos diferentes de cero que compartan fila con alguno de los que están en las últimas

k columnas. Las restantes posiciones se pueden anular mediante operaciones de filas, cotransiciones **derechas**, a excepción de la primera posición no nula de la columna $n-k+1$ que no se puede alterar.

Sólo resta probar que no podemos tener dos elementos de la misma órbita de cotransición que pertenezcan a $\mathcal{T}_n^*(q)$. En este sentido, basta observar que estas operaciones conservan el rango de la matriz M_f y que no pueden modificar su soporte cuando $f \in \mathcal{T}_n^*(q)$.

Sea $r(i,j,f)$ es el rango de la matriz

$$\sum_{k\leq i<j\leq l} f(e_{kl})\, e_{kl},$$

es claro que si f y f' pertenecen a la misma órbita de cotransición, entonces $r(i,j,f) = r(i,j,f')$ para todo i,j. Así pues, esto implica que si f y f' pertenecen a $\mathcal{T}_n^*(q)$ su soporte debe ser idéntico.

Supongamos que f y f' son dos elementos de $\mathcal{T}_n^*(q)$ que están en la misma órbita, de manera que podemos encontrar elementos X e Y de $\mathbf{U}_n(q)$ tales que $X \cdot f = f' \cdot Y$. Las acciones de cotransición conservan el valor de las posiciones no nulas de M_f y $M_{f'}$ cuando transforman f en $X \cdot f$ y f' en $f' \cdot Y$. Así pues, $M_{X\cdot f} = M_{f'\cdot Y}$ implica $M_f = M_{f'}$ y por tanto, $f = f'$. ■

Para cada uno de los elementos $f \in \mathcal{T}_n^*(q)$ es fácil ver que el conjunto $D = \{(i,j) : f(i,j) \neq 0\}$ es básico. La función $\varphi : D \to \mathbb{F}_q^*$ se consigue si se le asocia a cada $(i,j) \in D$ el valor $f(i,j) \neq 0$. Por tanto, cada órbita de cotransición, y por ello cada carácter de transición, define un único par (D,φ). Recíprocamente, dado un par (D,φ) con D básico y $\varphi : D \to \mathbb{F}_q^*$ una aplicación cualquiera, el elemento $f = \sum_{(i,j)\in D} \varphi(i,j)\, e_{ij}^* \in \mathcal{T}_n^*(q)$. Es decir, existe una aplicación biyectiva entre los caracteres de transición y todos los posibles pares (D,φ) con D básico y $\varphi : D \to \mathbb{F}_q^*$.

Ahora intentaremos descomponer cada carácter de transición en un pro-

ducto de caracteres, tal como sucede en el caso de los caracteres básicos. En primer lugar, introducimos la siguiente definición.

Definición 1.4.8 *Una órbita de cotransición es primaria si contiene a un elemento de la base de* $\mathfrak{u}_n(q)^*$ *o a un múltiplo suyo que sea diferente de cero. El carácter de transición asociado a una órbita primaria se denomina carácter primario.*

A continuación probaremos que cada órbita de cotransición se puede expresar como una suma de órbitas primarias. Denotamos por $\mathbf{\Psi}_{ij}(\alpha)$, con $1 \leq i < j \leq n$, la órbita coadjunta que contiene al elemento $\alpha\, e_{ij}^*$. Si $\alpha \neq 0$, $\mathbf{\Psi}_{ij}(\alpha)$ es una órbita primaria, mientras que si $\alpha = 0$ es la órbita trivial $\mathbf{\Psi} = \{0\}$.

Lema 1.4.9 *Sea* $f \in \mathfrak{u}_n(q)^*$*, si el soporte de* f *no contiene elementos ni en la fila* i *ni en la columna* j*, la órbita de cotransición de* $f + \alpha\, e_{ij}^*$ *es* $\mathbf{\Psi}_f + \mathbf{\Psi}_{ij}(\alpha)$.

Demostración: Supongamos que $\alpha \neq 0$, pues en otro caso el resultado es trivial. Los elementos de $\mathbf{\Psi}_{ij}(\alpha)$ se obtienen mediante cotransiciones a partir del elemento $\alpha\, e_{ij}^*$, de (1.7) y (1.8) obtenemos la siguiente expresión

$$\alpha\, e_{ij}^* + \sum_{i<k<j} \alpha_k\, e_{kj}^* + \sum_{i<l<j} \alpha_l'\, e_{il}^* + \sum_{i<k<l<j} \alpha^{-1}\alpha_k\, \alpha_l'\, e_{kl}^*,$$

con $\alpha_k, \alpha_l' \in \mathbb{F}_q$. Dada la forma del soporte de f, podemos concluir que es posible pasar del elemento $f + \alpha\, e_{ij}^*$ al elemento

$$f + \alpha\, e_{ij}^* + \sum_{i<k<j} \alpha_k\, e_{kj}^* + \sum_{i<l<j} \alpha_l'\, e_{il}^* + \sum_{i<k<l<j} \alpha^{-1}\alpha_k\, \alpha_l'\, e_{kl}^*$$

mediante cotransiciones. Por tanto, concluimos que el conjunto $f + \mathbf{\Psi}_{ij}(\alpha)$ está contenido en la órbita de cotransición del elemento $f + \alpha\, e_{ij}^*$.

Si $f' \in \mathbf{\Psi}_f$, es claro que podemos transformar $f + \mathbf{\Psi}_{ij}(\alpha)$ en el conjunto $f' + \mathbf{\Psi}_{ij}(\alpha)$ mediante una cotransición, lo que implica que la suma de órbitas $\mathbf{\Psi}_f + \mathbf{\Psi}_{ij}(\alpha)$ esté contenida en la órbita de $f + \alpha\, e_{ij}^*$.

Por otra parte, la acción de cotransición es lineal, por lo que la suma es cerrada para las cotransiciones. Así pues, la órbita de $f + \alpha\, e_{ij}^*$ estará contenida en $\mathbf{\Psi}_f + \mathbf{\Psi}_{ij}(\alpha)$, lo que nos asegura la igualdad. ■

Para cada elemento $\tau \in \mathcal{T}_n^*(q)$, denotamos $\mathbf{\Psi}_{ij}(\tau)$ la órbita de cotransición $\mathbf{\Psi}_{ij}(\tau(e_{ij}))$. Con esta notación podemos probar el siguiente resultado que permite expresar cualquier órbita de cotransición como suma de órbitas primarias.

Teorema 1.4.10 *Dado cualquier elemento $\tau \in \mathcal{T}_n^*(q)$ se tiene que*

$$\mathbf{\Psi}_\tau = \sum_{1 \le i < j \le n} \mathbf{\Psi}_{ij}(\tau).$$

Demostración: Por inducción en el cardinal del soporte de τ. Supongamos que $\tau(e_{kl})$ es diferente de cero para algún k y l dados. Sea $\tau' = \tau - \tau(e_{kl})\, e_{kl}^*$; es claro que $\tau' \in \mathcal{T}_n^*(q)$ y que su soporte tiene un cardinal menor que el soporte de τ. Aplicando la hipótesis de inducción se tiene

$$\mathbf{\Psi}_{\tau'} = \sum_{1 \le i < j \le n} \mathbf{\Psi}_{ij}(\tau').$$

Pero el soporte de τ' no contiene elementos ni en la fila k ni en la columna l, por lo que podemos aplicar el lema anterior y así

$$\mathbf{\Psi}_\tau = \mathbf{\Psi}_{\tau'} + \mathbf{\Psi}_{kl}(\tau) = \sum_{1 \le i < j \le n} \mathbf{\Psi}_{ij}(\tau).$$

■

Sea $\chi_{ij}(\alpha)$ al carácter de transición asociado a la órbita $\mathbf{\Psi}_{ij}(\alpha)$. Notemos que en el caso en que $\alpha = 0$ el carácter $\chi_{ij}(0)$ es el carácter trivial $1_{\mathbf{U}_n(q)}$.

Para cada $\tau \in \mathcal{T}_n^*(q)$ definimos el carácter primario $\chi_{ij}(\tau)$ como $\chi_{ij}(\tau(e_{ij}))$. El resultado siguiente nos da la descomposición del carácter de transición como producto de caracteres primarios.

Teorema 1.4.11 *Sea $\tau \in \mathcal{T}_n^*(q)$, entonces*

$$\chi(\tau) = \prod_{1 \leq i < j \leq n} \chi_{ij}(\tau).$$

Demostración: A partir del teorema 1.4.5 podemos expresar el carácter de transición $\chi(\tau)$ como sigue:

$$\chi(\tau) = \frac{\chi(\tau)(1)}{|\mathbf{\Psi}_\tau|} \sum_{f \in \mathbf{\Psi}_\tau} v(f). \tag{1.9}$$

De igual forma, para cada $1 \leq i < j \leq n$ el correspondiente carácter primario puede escribirse como

$$\chi_{ij}(\tau) = \frac{\chi_{ij}(\tau)(1)}{|\mathbf{\Psi}_{ij}(\tau)|} \sum_{g \in \mathbf{\Psi}_{ij}(\tau)} v(g).$$

Dado que $\chi(\tau)(1) = |\mathbf{U}_n(q) \cdot \tau|$ y puesto que soporte de τ tiene a lo sumo un elemento en cada fila y en cada columna, es fácil ver que

$$|\mathbf{U}_n(q) \cdot \tau| = \prod_{1 \leq i < j \leq n} |\mathbf{U}_n(q) \cdot \tau(e_{ij})\, e_{ij}^*|.$$

Así pues,

$$\chi(\tau)(1) = \prod_{1 \leq i < j \leq n} \chi_{ij}(\tau)(1). \tag{1.10}$$

Ahora hacemos uso del lema 2.3.2 que nos da el cardinal de una órbita de cotransición para el caso de un grupo de álgebra cualquiera, de forma que podemos escribir:

$$|\mathbf{\Psi}_\tau| = \frac{|\mathbf{U}_n(q) \cdot \tau|^2}{|\mathbf{U}_n(q) \cdot \tau \cap \tau \cdot \mathbf{U}_n(q)|} = \frac{\chi_\tau(1)^2}{|\mathbf{U}_n(q) \cdot \tau \cap \tau \cdot \mathbf{U}_n(q)|} \tag{1.11}$$

Para cada órbita primaria $\mathbf{\Psi}_{ij}(\tau)$ es fácil ver que

$$|\mathbf{\Psi}_{ij}(\tau)| = \frac{|\mathbf{U}_n(q) \cdot \tau_{ij}|}{|\mathbf{U}_n(q) \cdot \tau_{ij} \cap \tau_{ij} \cdot \mathbf{U}_n(q)|} = \chi_{ij}(\tau)(1)^2, \tag{1.12}$$

con $\tau_{ij} = \tau(e_{ij})\, e_{ij}^*$, pues de (1.7) y de (1.8) se sigue que la intersección de las órbitas de cotransición izquierda y derecha es el elemento τ_{ij}.

Si combinamos las expresiones (1.11) y (1.12) con (1.10) tenemos que

$$|\mathbf{U}_n(q) \cdot \tau \cap \tau \cdot \mathbf{U}_n(q)|\, |\mathbf{\Psi}_\tau| = \prod_{1 \leq i < j \leq n} |\mathbf{\Psi}_{ij}(\tau)|. \tag{1.13}$$

Según el teorema 1.4.10, cada elemento $f \in \mathbf{\Psi}_\tau$ se puede escribir como una suma de funciones, cada una de ellas en una órbita primaria, es decir:

$$f = \sum_{1 \leq i < j \leq n} f_{ij},$$

con $f_{ij} \in \mathbf{\Psi}_{ij}(\tau)$. Si $f' = X \cdot f \cdot Y$, la descomposición de f lleva a la siguiente descomposición de f':

$$f' = \sum_{1 \leq i < j \leq n} X \cdot f_{ij} \cdot Y,$$

por lo que el número de estas descomposiciones es el mismo para cualquier elemento de $\mathbf{\Psi}_\tau$, que por la ecuación (1.13)es precisamente $|\mathbf{U}_n(q) \cdot \tau \cap \tau \cdot \mathbf{U}_n(q)|$. Por otra parte, cada descomposición de f induce una descomposición de la función $v(f)$. De esa forma, $v(f) = \prod_{1 \leq i < j \leq n} v(f_{ij})$, y se sigue que

$$|\mathbf{U}_n(q) \cdot \tau \cap \tau \cdot \mathbf{U}_n(q)| \sum_{f \in \mathbf{\Psi}_\tau} v(f) = \prod_{1 \leq i < j \leq n} \left[\sum_{h \in \mathbf{\Psi}_{ij}(\tau)} v(h) \right]$$

Si sustituimos esta expresión en (1.9) y usamos (1.10) y (1.13) obtenemos el resultado deseado. ■

Por último, sólo nos falta probar que las dos formulaciones coinciden. Es decir, que los caracteres básicos son iguales a los caracteres de transición.

Hemos visto que cada carácter de transición $\chi(\tau)$ viene indicado por un conjunto básico D y por una función $\varphi : D \to \mathbb{F}_q^*$, definida por $\varphi(i,j) = \tau(e_{ij})$, tal como lo hacen los caracteres básicos definidos en (1.3). Por otra parte, acabamos de ver que $\chi(\tau)$ se descompone en un producto de caracteres primarios, cada uno de ellos indicado por un elemento del conjunto básico D de las posiciones del soporte de τ.

Así pues, para probar que $\chi(\tau)$ es un carácter básico, bastará probar que cada carácter primario es un carácter elemental, es decir, que cada uno de ellos es la función de Kirillov asociada a la órbita coadjunta $\mathcal{O}_{ij}(\tau) = \mathcal{O}_{ij}(\tau(e_{ij}))$. Esto es, debe probarse que

$$\chi_{ij}(\tau) = \phi_{\mathcal{O}_{ij}(\tau)} = \frac{1}{\sqrt{|\mathcal{O}_{ij}(\tau)|}} \sum_{f \in \mathcal{O}_{ij}(\tau)} \psi_f. \tag{1.14}$$

Notemos en primer lugar que los caracteres primarios son siempre irreducibles, pues como consecuencia del corolario 1.4.6 y de (1.12)

$$\langle \chi_{ij}(\tau), \chi_{ij}(\tau) \rangle = \frac{\chi_{ij}(\tau)(1)^2}{|\mathbf{\Psi}_{ij}(\tau)|} = 1.$$

Ahora sólo resta probar que la órbita de cotransición $\mathbf{\Psi}_{ij}(\tau)$ se reduce a la órbita coadjunta $\mathcal{O}_{ij}(\tau)$. Para ello, basta aplicar el teorema 3.2 de [11] en el caso $G = \mathbf{U}_n(q)$. De ahí se deduce no sólo la igualdad $\mathbf{\Psi}_{ij}(\tau) = \mathcal{O}_{ij}(\tau)$, sino también que $|\mathbf{\Psi}_{ij}(\tau)| = |\mathcal{O}_{ij}(\tau)| = \chi_{ij}(\tau)(1)^2$. Sustituyendo en la expresión de los caracteres primarios dada por (1.9) llegamos a (1.14). Por tanto, hemos demostrado el siguiente resultado.

Teorema 1.4.12 *Sean τ un elemento de $\mathcal{T}_n^*(q)$ y $\chi(\tau)$ el carácter de transición asociado. Entonces existe un conjunto básico D y una función $\varphi : D \to \mathbb{F}_q^*$ tales que*

$$\chi(\tau) = \xi_D(\varphi).$$

Los caracteres básicos, o de transición, recibirán en adelante el nombre de *super-caracteres* del grupo $\mathbf{U}_n(q)$.

Capítulo 2

Super-caracteres de un grupo de álgebra finito

Conforme a la notación del capítulo anterior, sea p un primo, $q = p^e$ una potencia suya con $e > 1$ y $\mathbb{F}_q$ el cuerpo de q elementos. Sea A una $\mathbb{F}_q$-álgebra asociativa de dimensión finita y $J = J(A)$ su radical de Jacobson. Podemos considerar, sin pérdida de generalidad, que el álgebra A tiene identidad, representada por 1. Según la definición 1.2.1, el conjunto $G = 1 + J$ es un grupo de álgebra finito. El objetivo de este capítulo es extender el concepto de super-carácter al grupo de álgebra G.

Recordemos que en el capítulo anterior los super-caracteres de $\mathbf{U}_n(q)$ se definieron como los caracteres básicos o de transición del grupo. Sin embargo, para un grupo de álgebra cualquiera G, el proceso de construcción es diferente. El teorema 1.2 de [33] establece que cualquier carácter irreducible de G está inducido por un carácter lineal de un subgrupo $H \leq G$. Este hecho ya fue probado por Carlos A. M. André en [7] para el caso en que $J^p = 0$.

A partir de esta propiedad, es posible definir el super-carácter de G asociado a $f \in J^*$ como el carácter inducido por un carácter lineal del estabilizador

de f para una acción de G. De esta forma, nuestra definición se encuentra más próxima a la formulación de Yan (ver [82]) que a la de los caracteres básicos. A estos volveremos en el capítulo siguiente.

2.1. Las acciones del grupo G

De forma similar a lo que sucede en $\mathbf{U}_n(q)$, ver (1.5), el grupo de álgebra G actúa sobre el $\mathbb{F}_q$-espacio vectorial J de tres formas diferentes:

$$\begin{aligned} x \cdot a &\to x\,a \quad && \textit{acción de transición izquierda},\\ a \cdot x &\to a\,x \quad && \textit{acción de transición derecha},\\ a^x &\to x^{-1}a\,x \quad && \textit{acción adjunta}, \end{aligned}$$

donde $a \in J$ y $x \in G$. La operación implicada es la multiplicación del álgebra A. Es fácil ver que las acciones de transición derecha e izquierda conmutan, lo que permite definir una acción doble del grupo G sobre J, conocida como *acción de transición*, dada por $x \cdot a \cdot y = (x \cdot a) \cdot y = x \cdot (a \cdot y)$ para todo $a \in J$ y todo $x, y \in G$. Dado cualquier $a \in J$, la *órbita de transición* que lo contiene se denota como $G\,a\,G = \{x \cdot a \cdot y : x, y \in G\}$. Notemos que estas órbitas son estables para la acción adjunta y por ello son unión de órbitas adjuntas.

De acuerdo con (1.6), el grupo G define sobre $J^* = Hom_{\mathbb{F}_q}(J, \mathbb{F}_q)$ tres acciones diferentes:

$$\begin{aligned} (xf)(a) &= f(a\,x) \quad && \textit{acción de cotransición izquierda},\\ (fx)(a) &= f(x\,a) \quad && \textit{acción de cotransición derecha},\\ f^x(a) &= f(x\,a\,x^{-1}) \quad && \textit{acción coadjunta}, \end{aligned}$$

donde $x \in G$, $f \in J^*$ y $a \in J$. Las acciones de cotransición derecha e izquierda conmutan, por lo que es posible definir la *acción de cotransición* como la

acción doble de G sobre J^* dada por $(xfy)(a) = (xf)y(a) = x(fy)(a) = f(yax)$ para $x, y \in G$, $f \in J^*$ y $a \in J$. La órbita de cotransición que contiene al elemento $f \in J^*$ es el subconjunto $GfG = \{xfy : x, y \in G\}$. Como antes, cada órbita de cotransición es unión de órbitas coadjuntas.

Nota 2.1.1 *Las acciones de transición y cotransición se pueden ver como acciones del grupo $G \times G$ sobre J y J^* respectivamente. Así, si $(x, y) \in G \times G$ definimos $(x, y) \cdot a = xay^{-1}$ para todo $a \in J$ y definimos $(x, y)f = xfy^{-1}$ para todo $f \in J^*$. Con esta notación se tiene que $|GaG| = |G \times G : C_{G\times G}(a)|$ y $|GfG| = |G \times G : C_{G\times G}(f)|$, con $C_{G\times G}(a)$ y $C_{G\times G}(f)$ los respectivos estabilizadores de a y de f.*

En lo que sigue denotaremos por $\mathbf{\Omega}(G)$ el conjunto de todas las órbitas coadjuntas de G, y por $\mathbf{\Psi}(G)$ el de todas las órbitas de cotransición de G.

Lema 2.1.2 *Sea $f \in J^*$, los estabilizadores de f para las acciones de cotransición derecha e izquierda son, respectivamente, los conjuntos $R(f) = 1 + \mathcal{R}(f)$ y $L(f) = 1 + \mathcal{L}(f)$, donde*

$$\mathcal{R}(f) = \{a \in J : f(ab) = 0, \forall b \in J\} \quad \text{y} \quad \mathcal{L}(f) = \{a \in J : f(ba) = 0, \forall b \in J\}.$$

Demostración: Sea $x = 1+a$ un elemento en el estabilizador $R(f)$, entonces $fx(b) = f(b)$ para todo $b \in J$. Es decir, $(fx)(b) = f(xb) = f((1 + a)b) = f(b+ab) = f(b)$ para todo $b \in J$ y por tanto, $f(ab) = 0$ para todo $b \in J$; así pues $a \in \mathcal{R}(f)$.

Recíprocamente, supongamos $x = 1 + a$ con $a \in \mathcal{R}(f)$. En ese caso, $(fx)(b) = f(xb) = f((1 + a)b) = f(b + ab) = f(b)$ y entonces $x \in R(f)$.

El resultado para la acción de cotransición izquierda se obtiene siguiendo un razonamiento análogo. ■

Nota 2.1.3 *Los subgrupos de un grupo de álgebra $G = 1+J$ tienen la forma $H = 1 + Y$, para algún $Y \subseteq J$. En general, el subconjunto Y no satisface ninguna propiedad en especial; sin embargo, cuando es un $\mathbb{F}_q$-subespacio multiplicativamente cerrado de J, $H = 1 + Y$ recibe el nombre especial de* ***subgrupo de álgebra*** *de G (ver [42]).*

Es fácil comprobar que los conjuntos $\mathcal{R}(f)$ y $\mathcal{L}(f)$ son $\mathbb{F}_q$-subespacios multiplicativamente cerrados de J, por la nota anterior los estabilizadores $R(f)$ y $L(f)$ son subgrupos de álgebra de G.

Dados $a \in J$ y $f \in J^*$, definimos el elemento $af \in J^*$ (respec. $fa \in J^*$) por $(af)(b) = f(ba)$ (respec. $(fa)(b) = f(ab)$) para todo $b \in J$. Los conjuntos $Jf = \{af : a \in J\}$ y $fJ = \{fa : a \in J\}$ claramente son subespacios vectoriales de J y se relacionan con $\mathcal{R}(f)$ y $\mathcal{L}(f)$ como se prueba en el siguiente resultado.

Proposición 2.1.4 *Sea $f \in J^*$, entonces*

1. $Jf = (\mathcal{R}(f))^{\perp} = \{g \in J^* : g(a) = 0, \forall a \in \mathcal{R}(f)\}$;
2. $fJ = (\mathcal{L}(f))^{\perp} = \{g \in J^* : g(a) = 0, \forall a \in \mathcal{L}(f)\}$;
3. $|\mathcal{R}(f)| = |\mathcal{L}(f)|$.

Demostración: Dado $f \in J^*$ definimos la aplicación lineal

$$\begin{aligned} \varphi_f : J &\longrightarrow J^* \\ a &\longrightarrow af \end{aligned}$$

cuya imagen es $Im(\varphi_f) = Jf$. La aplicación dual (ver [46]) se define como

$$\begin{aligned} \varphi_f^* : J^{**} &\longrightarrow J^* \\ \omega &\longrightarrow \omega \circ \varphi_f \end{aligned}$$

Puesto que J tiene dimensión finita, existe un isomorfismo canónico de espacios vectoriales $\eta : J \to J^{**}$ dado por $\eta(a)(g) = g(a)$ para todo $a \in J$ y $g \in J^*$. De este modo, dado $\omega = \eta(a) \in J^{**}$, tenemos que

$$\varphi_f^*(\omega)(b) = \omega \circ \varphi_f(b) = \eta(a)(\varphi_f(b)) = \eta(a)(bf) = bf(a) = fa(b),$$

para todo $b \in J$. Por tanto, φ_f^* se puede identificar con la aplicación

$$\begin{array}{rcl} \varphi_f^* : J & \longrightarrow & J^* \\ a & \longrightarrow & fa \end{array}$$

cuya imagen es $Im(\varphi_f^*) = fJ$. Es bien conocido (ver teorema 11 del capítulo II de [46]) que $Ker(\varphi_f^*)^\perp = Im(\varphi_f) = Jf$, y con la identificación que hemos hecho

$$Ker(\varphi_f^*) = \{a \in J : fa = 0\} = \{a \in J : f(ab) = 0, \forall b \in J\} = \mathcal{R}(f),$$

lo que nos da 1.

Para obtener 2 basta observar que $Ker(\varphi_f) = Im(\varphi_f^*)^\perp = (fJ)^\perp$ y que

$$Ker(\varphi_f) = \{a \in J : af = 0\} = \{a \in J : f(ba) = 0, \forall b \in J\} = \mathcal{L}(f).$$

Todos los espacios vectoriales implicados son de dimensión finita y por ello

$$fJ = ((fJ)^\perp)^\perp = \mathcal{L}(f)^\perp.$$

Por último, para probar 3, observemos que $|Jf| = |Im(\varphi_f)| = q^{rg(\varphi_f)}$, mientras que $|fJ| = |Im(\varphi_f^*)| = q^{rg(\varphi_f^*)}$. Por lo que basta probar que $rg(\varphi_f) = rg(\varphi_f^*)$, lo que se sigue del teorema 12 del capítulo II de [46]. ■

Como consecuencia, podemos encontrar las órbitas de cotransición derecha e izquierda que contienen a un elemento $f \in J^*$.

Corolario 2.1.5 *Sea $f \in J^*$, la órbita de cotransición izquierda (respec. derecha) de f es $Gf = f + (\mathcal{R}(f))^\perp$ (respec. $fG = f + (\mathcal{L}(f))^\perp$). Es más, $|Gf| = |fG|$.*

Demostración: A partir de los resultados 1 y 2 del teorema anterior se tiene que

$$Gf = (1+J)f = f + (\mathcal{R}(f))^\perp, \quad fG = f(1+J) = f + (\mathcal{L}(f))^\perp.$$

Por otra parte, de 3 se sigue que $|Gf| = |(\mathcal{R}(f))^\perp| = |(\mathcal{L}(f))^\perp| = |fG|$. ■

2.2. Super-caracteres de G. Definición

Tras estudiar las generalidades de los grupos de álgebra, en esta sección introducimos el concepto de super-carácter. Para ello, partimos de los caracteres irreducibles de J y extendemos su dominio al grupo G. Una restricción adecuada de estas funciones permite definir por inducción el correspondiente super-carácter.

La forma más habitual de extender el dominio de una función definida sobre el álgebra J al grupo de álgebra $G = 1 + J$ es utilizar la función exponencial introducida en (1.2). Notemos que ésta es la técnica utilizada para obtener los caracteres irreducibles de G a partir de las funciones Kirillov (ver teorema 1.2.7) cuando la característica de $\mathbb{F}_q$ es mayor que el grado de nilpotencia de J. No obstante, puesto que la expresión (1.2) no es válida para cualquier valor de la característica, nuestra definición de super-caracteres no debe depender de la exponencial. Así pues, si ψ es un carácter no trivial del grupo $\mathbb{F}_q^+$, para cada $f \in J^*$ definimos la aplicación:

$$\begin{array}{rcl} \lambda_f : G & \longrightarrow & \mathbb{C} \\ 1+a & \longrightarrow & \psi_f(a) \end{array} \tag{2.1}$$

A pesar de que ψ_f es un carácter de J (ver proposición 1.2.2), en general, λ_f no es un carácter de G. Sin embargo, su restricción a $R(f)$ es un carácter lineal.

Lema 2.2.1 *Sea $f \in J^*$, la aplicación $\lambda_f : G \to \mathbb{C}$ es un carácter lineal del grupo $R(f) = 1 + \mathcal{R}(f)$.*

Demostración: Puesto que $\lambda_f(1) = \psi_f(0) = 1$, basta probar que $\lambda_f|_{R(f)}$ es un carácter. Dados $x, y \in R(f) = 1 + \mathcal{R}(f)$, podemos escribir $x = 1 + a$, $y = 1 + b$ con $a, b \in \mathcal{R}(f)$. Por tanto,

$$\begin{aligned} \lambda_f(xy) = \psi_f(a+b+ab) = \psi(f(a)+f(b)+f(ab)) = \\ = \psi(f(a)+f(b)) = \psi_f(a)\psi_f(b) = \lambda_f(x)\lambda_f(y). \end{aligned}$$

pues $a \in \mathcal{R}(f)$ y $f(ab) = 0$ para todo $b \in J$. ■

Nota 2.2.2 *En adelante, entenderemos que λ_f representa el carácter lineal de $R(f)$ dado por la restricción $\lambda_f|_{R(f)}$.*

Definición 2.2.3 *Sea $f \in J^*$, el super-carácter de G asociado a f es el carácter inducido λ_f^G.*

Al igual que en [82], dado un elemento $f \in J^*$, podemos relacionar el super-carácter asociado a dicho elemento con la órbita de cotransición $\mathbf{\Psi} = GfG$ que lo contiene.

Teorema 2.2.4 *Sea $f \in J^*$, el super-carácter de G asociado a f viene dado por la expresión*

$$\lambda_f^G = \frac{|Gf|}{|GfG|} \sum_{g \in GfG} \lambda_g. \tag{2.2}$$

Demostración: Según la definición 1.1.14, el carácter inducido λ_f^G se puede escribir como

$$\lambda_f^G(1+a) = \frac{1}{|R(f)|} \sum_{x \in G} \lambda_f^\circ[x(1+a)x^{-1}],$$

donde λ_f° la aplicación definida como

$$\lambda_f^\circ(1+a) = \begin{cases} \lambda_f(1+a) & \text{si } 1+a \in R(f), \\ 0 & \text{en otro caso.} \end{cases}$$

Por la proposición 1.2.2, ψ_f es un carácter (irreducible) del grupo abeliano J; si restringimos a $\mathcal{R}(f)$ y después inducimos a J se tiene que

$$(\psi_f|_{\mathcal{R}(f)})^J(a) = \begin{cases} |J : \mathcal{R}(f)|\ \psi_f(a) & \text{si } a \in \mathcal{R}(f), \\ 0 & \text{en otro caso.} \end{cases}$$

Expresión que, junto con la ecuación (2.1) y la proposición 1.2.2, nos lleva a la igualdad siguiente:

$$\begin{aligned} \lambda_f^\circ(1+a) &= \frac{1}{|J : \mathcal{R}(f)|}(\psi_f|_{\mathcal{R}(f)})^J(a) \\ &= \frac{1}{|J : \mathcal{R}(f)|} \sum_{g \in J^*} \langle (\psi_f|_{\mathcal{R}(f)})^J, \psi_g \rangle\, \psi_g(a), \end{aligned}$$

para la que se ha utilizado la descomposición del carácter $(\psi_f|_{\mathcal{R}(f)})^J$ en suma de caracteres irreducibles. Los productos escalares se calculan mediante la reciprocidad de Frobenius, proposición 1.1.15. Así se obtiene:

$$\langle (\psi_f|_{\mathcal{R}(f)})^J, \psi_g\rangle = \langle \psi_f, \psi_g\rangle_{\mathcal{R}(f)} = \begin{cases} 1 & \text{si } g \in f + (\mathcal{R}(f))^\perp, \\ 0 & \text{en otro caso.} \end{cases}$$

De forma que el super-carácter asociado a f se puede escribir como

$$\begin{aligned}\lambda_f^G(1+a) &= \frac{1}{|J|}\sum_{x\in G}\sum_{g\in f+(\mathcal{R}(f))^\perp}\psi_g(xax^{-1}) = \frac{1}{|J|}\sum_{x\in G}\sum_{g\in Gf}\psi_g(xax^{-1}) \\ &= \frac{1}{|J|}\sum_{x\in G}\frac{1}{|\mathcal{L}(f)|}\sum_{y\in G}\psi_{yf}(xax^{-1}),\end{aligned}$$

pues del corolario 2.1.5 se sigue que $f+(\mathcal{R}(f))^\perp = Gf$ y el estabilizador para la acción de cotransición izquierda es $\mathcal{L}(f)$. Si desarrollamos esta expresión,

$$\begin{aligned}\lambda_f^G(1+a) &= \frac{1}{|J|\,|\mathcal{L}(f)|}\sum_{x,y\in G}\psi_f(xax^{-1}y) = \frac{1}{|J|\,|\mathcal{L}(f)|}\sum_{x,z\in G}\psi_f(xaz) \\ &= \frac{1}{|J|\,|\mathcal{L}(f)|}\sum_{x,z\in G}\psi_{zfx}(a) = \frac{|C_{G\times G}(f)|}{|G|\,|L(f)|}\sum_{g\in GfG}\psi_g(a).\end{aligned}$$

Ahora bien, por el corolario 2.1.5, $|fG| = |G : L(f)| = |Gf|$ y por la nota 2.1.1, $|GfG| = |G\times G : C_{G\times G}(f)|$. Así pues,

$$\lambda_f^G(1+a) = \frac{|Gf|}{|GfG|}\sum_{g\in GfG}\psi_g(a).$$

■

Nota 2.2.5 *Hemos definido los super-caracteres de G a partir de la acción de cotransición derecha, mediante la inducción del carácter lineal $\lambda_f|_{R(f)}$ a G. De forma análoga, podemos trabajar con la acción de cotransición izquierda e inducir el carácter lineal $\lambda_f|_{L(f)}$. Se puede probar que ambas elecciones producen el mismo resultado, por lo que la definición no depende de la alternativa elegida.*

Corolario 2.2.6 *El super-carácter λ_f^G depende sólo de la órbita de cotransición $\mathbf{\Psi} = GfG$ que contiene a f. En adelante escribiremos $\lambda_f^G = \xi_{\mathbf{\Psi}}$.*

Demostración: Es claro que si $h \in GfG$, las órbitas de cotransición de f y h coinciden. Por tanto, para probar el resultado bastará ver que $|Gh| = |Gf|$. Supongamos que $h = xfy$ con $x, y \in G$ y consideremos la aplicación

$$\begin{aligned} \varphi : Gh &\longrightarrow Gf \\ g &\longrightarrow gy^{-1} \end{aligned}$$

Si $g \in Gh$, entonces existe $z \in G$ tal que $g = zh$, por lo que $\varphi(g) = zhy^{-1} = zxf \in Gf$. Así pues, φ está bien definida.

Dado un elemento $g' \in Gf$ tal que $g' = zf$ con $z \in G$, es claro que $\varphi(zx^{-1}h) = g'$ y por tanto se sigue que φ es suprayectiva. La inyectividad se desprende de las propiedades de la acción de cotransición: si $\varphi(g) = \varphi(g')$, entonces se tiene que $g = \varphi(g)y = \varphi(g')y = g'$. Por tanto, la aplicación φ es biyectiva y así $|Gh| = |Gf|$. ■

Si $\mathbf{\Psi}$ es la órbita de cotransición que contiene a $f \in J^*$, el grado del super-carácter $\xi_{\mathbf{\Psi}}$ será

$$\xi_{\mathbf{\Psi}}(1) = \lambda_f^G(1) = \frac{|Gf|}{|GfG|} \sum_{g \in GfG} \psi_g(0) = |Gf|. \tag{2.3}$$

Con este resultado podemos escribir el super-carácter $\xi_{\mathbf{\Psi}}$ tal como se muestra a continuación:

Corolario 2.2.7 *Sea $\mathbf{\Psi}$ una órbita de cotransición en J^*, entonces el super-carácter $\xi_{\mathbf{\Psi}}$ se puede escribir como*

$$\xi_{\mathbf{\Psi}} = \frac{\xi_{\mathbf{\Psi}}(1)}{|\mathbf{\Psi}|} \sum_{f \in \mathbf{\Psi}} \lambda_f. \tag{2.4}$$

2.3. Super-caracteres de G. Propiedades

Al igual que sucede con el grupo $\mathbf{U}_n(q)$, los super-caracteres de un grupo de álgebra G determinan una partición del conjunto de sus caracteres irreducibles. Para probarlo, seguiremos un proceso análogo al desarrollado en el capítulo 1, es decir, demostraremos que los super-caracteres son ortogonales para el producto de Frobenius y que el carácter regular de G es una combinación lineal de todos ellos.

Teorema 2.3.1 *Sea $SCh(G) = \{\xi_{\mathbf{\Psi}} : \mathbf{\Psi} \in \mathbf{\Psi}(G)\}$ el conjunto de super-caracteres de G. Entonces se verifica:*

$$\langle \xi_{\mathbf{\Psi}}, \xi_{\mathbf{\Psi}'} \rangle_G = \begin{cases} \dfrac{\xi_{\mathbf{\Psi}}(1)^2}{|\mathbf{\Psi}|} & si\ \mathbf{\Psi} = \mathbf{\Psi}', \\ 0 & en\ otro\ caso. \end{cases}$$

Demostración: A partir de la expresión de los super-caracteres dada en el corolario 2.2.7, llegamos a la siguiente expresión para el producto de Frobenius:

$$\langle \xi_{\mathbf{\Psi}}, \xi_{\mathbf{\Psi}'} \rangle_G = \frac{\xi_{\mathbf{\Psi}}(1)}{|\mathbf{\Psi}|} \frac{\xi_{\mathbf{\Psi}'}(1)}{|\mathbf{\Psi}'|} \sum_{f \in \mathbf{\Psi}} \sum_{g \in \mathbf{\Psi}'} \langle \lambda_f, \lambda_g \rangle_G.$$

La definición de las funciones λ_f y λ_g, dada por la expresión (2.1), permite pasar del grupo de álgebra $G = 1 + J$ al grupo aditivo $(J, +)$, de esta forma se puede escribir

$$\begin{aligned} \langle \lambda_f, \lambda_g \rangle_G &= \frac{1}{|G|} \sum_{x \in G} \lambda_f(x) \overline{\lambda_g(x)} = \frac{1}{|J|} \sum_{a \in J} \psi_f(a) \overline{\psi_g(a)} \\ &= \langle \psi_f, \psi_g \rangle_J = \delta_{f,g}. \end{aligned}$$

Las órbitas de cotransición forman una partición de J^*, por ello $\langle \xi_{\mathbf{\Psi}}, \xi_{\mathbf{\Psi}'} \rangle \neq 0$ si y sólo $\mathbf{\Psi} = \mathbf{\Psi}'$, en cuyo caso:

$$\langle \xi_{\mathbf{\Psi}}, \xi_{\mathbf{\Psi}} \rangle = \frac{\xi_{\mathbf{\Psi}}(1)^2}{|\mathbf{\Psi}|^2} \sum_{f \in \mathbf{\Psi}} \sum_{g \in \mathbf{\Psi}} \delta_{f,g} = \frac{\xi_{\mathbf{\Psi}}(1)^2}{|\mathbf{\Psi}|}.$$

■

Una consecuencia de este teorema es la caracterización de los super-caracteres irreducibles. Previamente, necesitamos probar el siguiente resultado.

Lema 2.3.2 *Sea $f \in J^*$ y sea GfG la órbita de cotransición que lo contiene. Entonces, el cardinal de GfG viene dado por la expresión*

$$|GfG| = \frac{|Gf|\,|fG|}{|Gf \cap fG|}.$$

Demostración: Por la nota 2.1.1, el grupo $G \times G$ actúa sobre J^* según la ley $(z,t)f = zft^{-1}$, para todo $(z,t) \in G \times G$ y todo $f \in J^*$. Por tanto, GfG es la órbita de f para esta acción y $|GfG| = |G \times G : C_{G\times G}(f)|$, con $C_{G\times G}(f) = \{(x,y) \in G \times G : xf = fy\} = \Gamma_f$.

Sea $\pi : G \times G \to G$ la proyección sobre la primera componente de $G \times G$ y sea $S_f = \pi(\Gamma_f)$. Supongamos que $(x,y) \in \Gamma_f$ satisface $\pi(x,y) = 1$, entonces $x = 1$ y $f = fy$, por lo que $y \in R(f)$. Así pues, se tiene que $Ker(\pi|_{\Gamma_f}) = \{1\} \times R(f)$ y por tanto, $|S_f| = \dfrac{|\Gamma_f|}{|R(f)|}$.

Además, S_f actúa transitivamente sobre el conjunto $Gf \cap fG$ mediante la acción de cotransición izquierda. De hecho, si $x \in S_f$, entonces existe $y \in G$ tal que $xf = fy$. Si $g \in Gf \cap fG$, por una parte $g = tf$, para un cierto $t \in G$, y $xg \in Gf$; por la otra $g = fz$, para algún $z \in G$ y $xg = xfz = fyz \in fG$. Es decir, $xg \in Gf \cap fG$ y la acción está bien definida. Para probar la transitividad basta notar que

$$Gf \cap fG = \{xf = fy : (x,y) \in \Gamma_f\} = \{xf : x \in S_f\},$$

es decir, $Gf \cap fG$ es la órbita de f.

Sea $C_{\Gamma_f}(f)$ el estabilizador de f, entonces $C_{\Gamma_f}(f) = \{x \in S_f : xf = f\} = S_f \cap L(f) = L(f)$. Por tanto, podemos escribir:

$$|Gf \cap fG| = \frac{|S_f|}{|L(f)|} = \frac{|\Gamma_f|}{|L(f)|\,|R(f)|}.$$

Puesto que $|GfG| = |G|^2/|\Gamma_f|$, sólo resta sustituir para llegar a la fórmula final

$$|GfG| = \frac{|Gf|\,|fG|}{|Gf \cap fG|}.$$

■

Corolario 2.3.3 *Sea $f \in J^*$ y sea $\mathbf{\Psi} = GfG$ la órbita de cotransición que lo contiene. Entonces, el super-carácter $\xi_{\mathbf{\Psi}}$ es irreducible si y sólo si $Gf \cap fG = \{f\}$, esto es, si y sólo si $\mathcal{R}(f) + \mathcal{L}(f) = J$.*

Demostración: El super-carácter $\xi_{\mathbf{\Psi}}$ será irreducible si y sólo si $\langle \xi_{\mathbf{\Psi}}, \xi_{\mathbf{\Psi}} \rangle = 1$, lo que equivale, por el teorema 2.3.1 y la expresión (2.3), a que se verifique la igualdad $|GfG| = |Gf|^2$. Por el lema anterior, esta condición se verifica si y sólo si $|Gf \cap fG| = 1$. Puesto que $Gf \cap fG = f + \mathcal{R}(f)^\perp \cap \mathcal{L}(f)^\perp$, esto es equivalente a $Gf \cap fG = \{f\}$, o lo que es lo mismo: $\mathcal{R}(f)^\perp \cap \mathcal{L}(f)^\perp = (\mathcal{R}(f) + \mathcal{L}(f))^\perp = \{0\}$, de donde se sigue que $\mathcal{R}(f) + \mathcal{L}(f) = J$. ■

Teorema 2.3.4 *Sea $\mathbf{\Psi}(G)$ el conjunto de todas las órbitas de cotransición sobre J^*. Entonces, el carácter regular ρ_G es suma de super-caracteres. De hecho, se verifica que*

$$\rho_G = \sum_{\mathbf{\Psi} \in \mathbf{\Psi}(G)} \frac{|\mathbf{\Psi}|}{\xi_{\mathbf{\Psi}}(1)}\, \xi_{\mathbf{\Psi}}.$$

Demostración: En primer lugar, aplicamos el corolario 1.2.6 para obtener la descomposición de ρ_G como suma de funciones de Kirillov. De esta forma se obtiene:

$$\rho_G = \sum_{\mathcal{O}\in\mathbf{\Omega}(G)} \phi_{\mathcal{O}}(1)\phi_{\mathcal{O}} = \sum_{\mathcal{O}\in\mathbf{\Omega}(G)} \sum_{f\in\mathcal{O}} \psi_f = \sum_{f\in J^*} \psi_f,$$

para lo que se ha usado la expresión (1.2) y el hecho de que que las órbitas coadjuntas constituyen una partición de J^*.

Por otra parte, las órbitas de cotransición también son una partición de J^*, de ahí que se pueda escribir

$$\rho_G = \sum_{f\in J^*} \psi_f = \sum_{\mathbf{\Psi}\in\mathbf{\Psi}(G)} \sum_{f\in\mathbf{\Psi}} \psi_f = \sum_{\mathbf{\Psi}\in\mathbf{\Psi}(G)} \frac{|\mathbf{\Psi}|}{\xi_{\mathbf{\Psi}}(1)}\, \xi_{\mathbf{\Psi}}.$$

■

Con este resultado y con la ortogonalidad de los super-caracteres, teorema 2.3.1, ya podemos probar que cada carácter irreducible es constituyente de un único super-carácter.

Teorema 2.3.5 *Cada carácter irreducible χ de G es constituyente de un único super-carácter. Es más, si $\mathbf{\Psi} \in \mathbf{\Psi}(G)$ y $\chi \in Irr(G)$ es un constituyente de $\xi_{\mathbf{\Psi}}$, entonces*

$$\langle \chi, \xi_{\mathbf{\Psi}} \rangle = \frac{\chi(1)\,\xi_{\mathbf{\Psi}}(1)}{|\mathbf{\Psi}|}.$$

Demostración: Dado un carácter $\chi \in Irr(G)$, éste es un constituyente de ρ_G y por el resultado anterior, lo será de un super-carácter $\xi_{\mathbf{\Psi}}$ para algún $\mathbf{\Psi} \in \mathbf{\Psi}(G)$. El teorema 2.3.1 asegura la unicidad de este super-carácter. Para probar la segunda parte basta ver que, por la unicidad de $\xi_{\mathbf{\Psi}}$, se verifica

$$\chi(1) = \langle \chi, \rho_G \rangle = \frac{|\mathbf{\Psi}|}{\xi_{\mathbf{\Psi}}(1)} \langle \chi, \xi_{\mathbf{\Psi}} \rangle.$$

■

Por último, si el conjunto de constituyentes irreducibles del super-carácter $\xi_{\mathbf{\Psi}}$ se denota por $Irr_{\mathbf{\Psi}}(G)$, podemos deducir la siguiente propiedad.

Corolario 2.3.6 *Sea $\mathbf{\Psi} \in \mathbf{\Psi}(G)$ una órbita de cotransición. Entonces $|\mathbf{\Psi}| = \sum_{\chi \in Irr_{\mathbf{\Psi}}(G)} \chi(1)^2$.*

Demostración: El super-carácter $\xi_{\mathbf{\Psi}}$ se puede escribir como una combinación lineal de caracteres irreducibles. Por el resultado anterior,

$$\xi_{\mathbf{\Psi}} = \sum_{\chi \in Irr_{\mathbf{\Psi}}(G)} \langle \xi_{\mathbf{\Psi}}, \chi \rangle \chi = \frac{\xi_{\mathbf{\Psi}}(1)}{|\mathbf{\Psi}|} \sum_{\chi \in Irr_{\mathbf{\Psi}}(G)} \chi(1)\chi.$$

Si evaluamos $\xi_{\mathbf{\Psi}}$ en 1, llegamos a la expresión deseada. ■

2.4. Super-caracteres y super-clases

Los caracteres irreducibles de G son constantes en las clases de conjugación del grupo y forman una base ortogonal, con respecto al producto de Frobenius, del espacio vectorial $\mathrm{cf}(G)$ formado por todas las funciones de clase de G. En esta sección veremos que los super-caracteres son constantes en las super-clases, que son una generalización de las clases de conjugación del grupo, y que forman una base ortogonal del espacio de todas las funciones que son constantes en las super-clases de G. Además, también probaremos que verifican una relación semejante a la Segunda Relación de Ortogonalidad para los caracteres irreducibles (teorema 1.1.12). Estas propiedades, junto con las ya conocidas, es decir: ortogonalidad (teorema 2.3.1) y descomposición del carácter regular (teorema 2.3.4), hacen de los super-caracteres una generalización de los caracteres irreducibles de G.

Definición 2.4.1 *Sea ϕ una órbita de transición en J. El subconjunto $\Phi = 1 + \phi \subseteq G$ se llama super-clase de G.*

Notemos que dos elementos x e y de G pertenecen a la misma super-clase si y sólo si $x-1$ e $y-1$ están en la misma órbita de transición ϕ de J. Por otra parte, las super-clases son estables para la acción adjunta y por tanto, son unión de órbitas adjuntas.

Lema 2.4.2 *Si ξ_{Ψ} un super-carácter de G, entonces ξ_{Ψ} es constante en las super-clases de G.*

Demostración: Dados elementos $x = 1 + a$ e $y = 1 + b$ en la misma super-clase, tenemos que $x = 1 + zbt$, con $z, t \in G$. De (2.4) se sigue que $\xi_{\Psi}(x) = \xi_{\Psi}(y)$. ■

Sea $\mathrm{scf}(G)$ el espacio vectorial de funciones de super-clase de G, es decir, el conjunto de funciones $\varphi : G \to \mathbb{C}$ que son constantes en las super-clases del grupo (ver [12]). Los resultados siguientes prueban que el conjunto de super-caracteres de G es una base ortogonal con respecto al producto de Frobenius del espacio $\mathrm{scf}(G)$.

Proposición 2.4.3 *El número de super-clases de G coincide con el número de super-caracteres de G.*

Demostración: Consideramos la acción de $G \times G$ sobre J definida por la nota 2.1.1, es decir $(x, y)a = yax^{-1}$, para todo $(x, y) \in G \times G$ y todo $a \in J$. Las órbitas de esta acción son las de transición y su número será igual al de super-clases de G, denotado por $k_{G\times G}$. Sea θ el carácter permutación asociado con esta acción (ver [41]), entonces para todo $(x, y) \in G \times G$

$$\theta(x, y) = |\{a \in J : (x, y)a = a\}|,$$

y por el corolario 5.15 de [41], $k_{G\times G} = \langle \theta, 1_{G\times G} \rangle$.

Por otra parte, el grupo $G \times G$ actúa también sobre el conjunto $Irr(J) = \{\psi_f : f \in J^*\}$ de acuerdo con la nota 2.1.1. Así, dado un elemento $(x, y) \in G \times G$ y un carácter irreducible ψ_f tenemos $(x, y)\psi_f = \psi_{xfy^{-1}}$. Además, se verifica que para todo $(x, y) \in G \times G$ y todo $a \in J$

$$(x, y)\psi_f((x, y)a) = \psi_{xfy^{-1}}(yax^{-1}) = \psi[f(y^{-1}(yax^{-1})x)] = \psi_f(a),$$

En estas condiciones podemos aplicar el teorema de Brauer (teorema 6.32 de [41]) y deducir que para cada elemento $(x, y) \in G \times G$ el cardinal $|\{f \in J^* : (x, y)\psi_f = \psi_f\}|$ es igual al número de clases de conjugación de $(J, +)$ fijas por la acción de $G \times G$. Puesto que $(J, +)$ es abeliano y las clases de conjugación se reducen a un único elemento, este número ha de coincidir con el cardinal $|\{a \in J : (x, y)a = a\}|$, que por definición es $\theta(x, y)$. Por tanto,

$$\theta(x, y) = |\{f \in J^* : (x, y)\psi_f = \psi_f\}|,$$

y por ello θ es el carácter de permutación para la acción de $G \times G$ sobre $Irr(J)$. Para esta acción el número de órbitas es $|\mathbf{\Psi}(G)|$, que por el corolario 2.2.6 es igual al número de super-caracteres. Del teorema 5.15 de [41], se sigue que

$$|\mathbf{\Psi}(G)| = \langle \theta, 1_{G\times G} \rangle = k_{G\times G}.$$

Esto es, el número de super-clases es igual al número de super-caracteres. ■

Los super-caracteres son funciones de super-clase (lema 2.4.2) y además, por el teorema 2.3.1, son ortogonales entre sí. Puesto que la dimensión del espacio de las funciones de super-clase es igual al número de éstas, como consecuencia del teorema anterior deducimos el siguiente resultado.

Corolario 2.4.4 *El conjunto* $\{\xi_{\mathbf{\Psi}} : \mathbf{\Psi} \in \mathbf{\Psi}(G)\}$ *es una base ortogonal del espacio complejo de las funciones de super-clase de* G.

Una vez probado que el número de super-caracteres y el de super-clases coincide, podemos construir tablas de super-caracteres semejantes a aquéllas que se construyen para los caracteres irreducibles de G. Como vimos en el teorema 2.3.1, las filas de una de estas tablas son ortogonales entre sí. El siguiente resultado prueba que las columnas también lo son.

Teorema 2.4.5 *Sea* $\Phi(G) = \{\Phi_1, \ldots, \Phi_N\}$ *el conjunto de las super-clases de* G*, y sea* $\{1 + a_1, \ldots, 1 + a_N\}$ *un sistema completo de representantes de dichas super-clases. Si* $\{\xi_{\Psi_1} = \xi_1, \ldots, \xi_{\Psi_N} = \xi_N\}$ *son los super-caracteres, entonces se verifica que*

$$\sum_{\Psi \in \Psi(G)} \langle \xi_\Psi, \xi_\Psi \rangle^{-1} \; \xi_\Psi(1 + a_i) \; \overline{\xi_\Psi(1 + a_j)} = \frac{|G|}{|\Phi_j|} \; \delta_{i,j}$$

Demostración: A partir de la primera relación de ortogonalidad para super-caracteres (teorema 2.3.1), podemos escribir

$$\frac{\xi_i(1)^2}{|\Psi_i|} \; \delta_{i,j} = \frac{1}{|G|} \sum_{g \in G} \xi_i(g) \; \overline{\xi_j(g)} = \frac{1}{|G|} \sum_{a \in J} \xi_i(1 + a) \; \overline{\xi_j(1 + a)}.$$

Puesto que los super-caracteres son constantes en las super-clases (lema 2.4.2) y que éstas constituyen una partición de G, agrupando términos se llega a la siguiente expresión:

$$\frac{\xi_i(1)^2}{|\Psi_i|} \; \delta_{i,j} = \frac{1}{|G|} \sum_{t=1}^{N} |\Phi_t| \; \xi_i(1 + a_t) \; \overline{\xi_j(1 + a_t)}. \tag{2.5}$$

Definimos ahora las matrices $S = (s_{ij})$, $K = (k_{ij})$ y $X = (x_{ij})$ como sigue:

$$s_{ij} = \frac{\xi_i(1)^2}{|\Psi_i|} \delta_{i,j}, \quad k_{ij} = |\Phi_i| \delta_{i,j}, \quad x_{ij} = \xi_i(1 + a_j), \quad 1 \leq i, j \leq N.$$

Con la nueva notación, la ecuación (2.5) se escribe $|G| \, S = XK\overline{X}^t$, que como S es regular es equivalente a $|G| \, Id = (XK) \, (\overline{X}^t S^{-1})$. Puesto que para una

matriz cuadrada las inversas por la derecha son necesariamente inversas por la izquierda, podemos alterar el orden para llegar a la siguiente expresión:

$$|G|\, Id = (\overline{X}^t S^{-1})\,(XK).$$

Que escrita como sistema de ecuaciones da:

$$|G|\,\delta_{i,j} = \sum_{t=1}^{N} \frac{|\mathbf{\Psi}_t|}{\xi_t(1)^2}\ |\Phi_j|\ \overline{\xi_t(1+a_i)}\ \xi_t(1+a_j), \quad 1 \leq j \leq N.$$

Por el teorema 2.3.1, llegamos a la fórmula final:

$$\frac{|G|}{|\Phi_j|} = \sum_{\mathbf{\Psi}\in\mathbf{\Psi}(G)} \langle \xi_{\mathbf{\Psi}}, \xi_{\mathbf{\Psi}} \rangle^{-1}\ \xi_{\mathbf{\Psi}}(1+a_i)\ \overline{\xi_{\mathbf{\Psi}}(1+a_j)}.$$

■

2.5. Un ejemplo: El álgebra de polinomios en una indeterminada

Sea F un cuerpo y sea $X = \{x_i : i \in I\}$ una colección de indeterminadas no conmutativas. Si $k \geq 0$, la secuencia $x_{i1} \ldots x_{i_k}$ de elementos de X, se conoce como palabra en X de longitud k (cuando $k = 0$, tendremos la palabra trivial 1). Dos palabras son iguales si sus longitudes lo son y si en posiciones idénticas se encuentran letras idénticas. La *F-álgebra libre generada por el conjunto X* (ver [61]) es el espacio vectorial $F\langle X\rangle$ cuya base son todas las palabras de X junto con el producto dado por la yuxtaposición de palabras de X, es decir: $(\sum \alpha_u u)(\sum \beta_v v) = \sum \alpha_u \beta_v uv$. Notemos que esta construcción es el análogo no conmutativo de un anillo de polinomios y por ello es siempre asociativa.

Si $X = \{x\}$ y $F = \mathbb{F}_q$, el álgebra libre $F(X) = \mathbb{F}_q(\{x\})$ es el anillo de polinomios $\mathbb{F}_q[x]$. Sea $A = \mathbb{F}_q[x]/(x^n) = \mathbb{F}_q(n, \{x\})$ la $\mathbb{F}_q$-álgebra de los

polinomios de grado menor que n. Los elementos nilpotentes de A son aquellos polinomios cuyo término independiente es nulo. Así pues, su radical de Jacobson es el conjunto $J = \langle x, x^2, \ldots, x^{n-1} \rangle_{\mathbb{F}_q}$. A su vez, el espacio dual $J^* = \langle x^*, (x^2)^*, \ldots, (x^{n-1})^* \rangle_{\mathbb{F}_q}$, donde $(x^i)^*(x^j) = \delta_{i,j}$ para $1 \leq i, j \leq n-1$.

En esta sección describiremos los super-caracteres del grupo de álgebra $G = 1+J$, que claramente es conmutativo. Por ello, las acciones de transición derecha e izquierda coinciden y el estabilizador $\mathcal{R}(f) = \mathcal{L}(f) = J_f$. Notemos que sucede lo mismo con la acción de cotransición. Esta propiedad permite una descripción sencilla de órbitas y super-caracteres.

Proposición 2.5.1 *Sea* $f = \sum_{i=1}^{s} f_i (x^i)^*$, $f_s \neq 0$ *un elemento de* J^*, *entonces el estabilizador* $J_f = \langle x^s, x^{s+1}, \ldots, x^{n-1} \rangle$ *y la órbita de cotransición* $Gf = f_s (x^s)^* + \langle (x)^*, \ldots, (x^{s-1})^* \rangle$.

Demostración: Si $a \in \langle x^s, \ldots, x^{n-1} \rangle$, es fácil verificar que $f(au) = 0$ para todo $u \in J$ y por tanto, $\langle x^s, \ldots, x^{n-1} \rangle \subseteq J_f$.

Recíprocamente, sea $a = \sum_{j=1}^{n-1} a_j x^j$ un elemento cualquiera de J_f, entonces debe verificarse $f(ax^k) = 0$ para $k = 1, \ldots, n-2$. Estas condiciones permiten plantear el siguiente sistema de ecuaciones:

$$\begin{cases} f_2 a_1 + f_3 a_2 + \cdots + \cdots + f_s a_{s-1} = 0 \\ f_3 a_1 + f_4 a_2 + \cdots + f_s a_{s-2} = 0 \\ \vdots \\ f_s a_1 = 0 \end{cases}$$

que es homogéneo con determinante $f_s^{s-1} \neq 0$, pues por hipótesis $f_s \neq 0$. Así pues, sólo existe la solución trivial $a_1 = \cdots = a_{s-1} = 0$ y entonces $a \in \langle x^s, \ldots, x^{n-1} \rangle$. Por tanto, $J_f = \langle x^s, x^{s+1}, \ldots, x^{n-1} \rangle$.

Por el corolario 2.1.5, $Gf = f + (J_f)^\perp = f_s (x^s)^* + \langle (x)^*, \ldots, (x^{s-1})^* \rangle$. ■

Este resultado nos indica que las órbitas de cotransición de G en J^* diferentes de $\mathbf{\Psi}_0 = 0$ están parametrizadas por los elementos $\alpha(x^s)^*$ con $\alpha \in \mathbb{F}_q^*$ y $1 \leq s \leq n-1$. Como consecuencia obtendremos la siguiente descomposición del espacio dual.

Corolario 2.5.2 *El espacio dual J^* es la unión disjunta*

$$J^* = \bigcup_{i=1}^{n-1} \bigcup_{\alpha \in \mathbb{F}_q^*} \mathbf{\Psi}_i(\alpha) \bigcup \mathbf{\Psi}_0,$$

donde $\mathbf{\Psi}_i(\alpha)$ es la órbita de cotransición que contiene al elemento $f = \alpha(x^i)^*$.

Demostración: Sea $f \in J^*$. Supongamos que f tiene grado $s \geq 1$, en ese caso, por la proposición anterior, $f \in \mathbf{\Psi}_s(f_s)$. Por otra parte, si $f = 0$, trivialmente, $f \in \mathbf{\Psi}_0$ y el resultado se sigue. ■

Dada una órbita de cotransición $\mathbf{\Psi}_s(\alpha)$, por (2.3) el grado del super-carácter $\xi_{\mathbf{\Psi}_s(\alpha)}$ coincide con el cardinal $|\mathbf{\Psi}_s(\alpha)| = |\langle x^*, \ldots, (x^{s-1})^* \rangle| = q^{s-1}$. Por tanto, hemos probado el siguiente corolario.

Corolario 2.5.3 *Sea $\mathbf{\Psi}_s(\alpha)$ la órbita de cotransición que contiene al elemento $\alpha(x^s)^* \in J^*$, entonces $\xi_{\mathbf{\Psi}_s(\alpha)}(1) = q^{s-1}$ para todo $\alpha \in \mathbb{F}_q^*$.*

Puesto que los super-caracteres sólo dependen de las órbitas de cotransición, es fácil deducir la fórmula del super-carácter asociado a un elemento cualquiera de J^*.

Corolario 2.5.4 *Sea f un elemento cualquiera de J^* y sea $\mathbf{\Psi}_f$ la órbita de cotransición que lo contiene. Si el término de mayor grado de f es $(x^s)^*$, entonces el super-carácter asociado a $\mathbf{\Psi}_f$ se puede escribir como*

$$\xi_{\mathbf{\Psi}_f} = \begin{cases} \lambda_{f_s(x^s)^*} \displaystyle\prod_{i=1}^{s-1} \left(\sum_{\alpha \in \mathbb{F}_q} \lambda_{\alpha(x^i)^*} \right) & \text{si } f_s \neq 0, \\ 1_G & \text{en otro caso.} \end{cases} \tag{2.6}$$

Demostración: A partir de la ecuación (2.4) podemos escribir

$$\xi_{\mathbf{\Psi}_f} = \frac{\xi_{\mathbf{\Psi}_f}(1)}{|\mathbf{\Psi}_f|} \sum_{g \in \mathbf{\Psi}_f} \lambda_g = \sum_{g \in \mathbf{\Psi}_f} \lambda_g,$$

pues G es abeliano y $|\mathbf{\Psi}_f| = |Gf| = |fG| = \xi_{\mathbf{\Psi}_f}(1)$.

Supongamos que el coeficiente del término de mayor grado $f_s \neq 0$, por la proposición 2.5.1 la órbita $\mathbf{\Psi}_f = f_s(x^s)^* + \langle (x)^*, \ldots, (x^{s-1})^* \rangle$. Si sustituimos, obtenemos que el super-carácter asociado a $\mathbf{\Psi}_f$ se puede escribir como

$$\begin{aligned}\xi_{\mathbf{\Psi}_f} &= \lambda_{f_s(x^s)^*} \left(\sum_{g \in \langle x^*, \ldots, (x^{s-1})^* \rangle} \lambda_g \right) = \sum_{\alpha_1 \in \mathbb{F}_q} \cdots \sum_{\alpha_{s-1} \in \mathbb{F}_q} \lambda_{\alpha_1 x^* + \cdots \alpha_{s-1}(x^{s-1})^*} \\ &= \sum_{\alpha_1 \in \mathbb{F}_q} \cdots \sum_{\alpha_{s-1} \in \mathbb{F}_q} \lambda_{\alpha_1 x^*} \cdots \lambda_{\alpha_{s-1}(x^{s-1})^*} = \lambda_{f_s(x^s)^*} \prod_{i=1}^{s-1} \left(\sum_{\alpha \in \mathbb{F}_q} \lambda_{\alpha(x^i)^*} \right).\end{aligned}$$

Si $f = 0$, entonces $\mathbf{\Psi}_0 = \{0\}$ y de (2.4) se sigue que $\xi_{\mathbf{\Psi}_0} = 1_G$. ■

Corolario 2.5.5 *Los únicos super-caracteres irreducibles de G son aquellos asociados a las órbitas de cotransición $\mathbf{\Psi}_1(f_1) = \{f_1 x^*\}$, con $f_1 \in \mathbb{F}_q$.*

Demostración: Por el corolario 2.3.3 los únicos super-caracteres irreducibles de G son aquellos asociados a órbitas de cotransición con un único elemento. Estas órbitas que son, por la proposición 2.5.1, las que contienen a las funciones $f = f_1 x^*$, con f_1 un elemento cualquiera de $\mathbb{F}_q$ incluido el cero; pues $\xi_{\mathbf{\Psi}_0} = 1_G$. ■

El carácter regular de G se descompone de acuerdo con el teorema 2.3.4 en suma de super-caracteres. Cada uno de ellos aparece con multiplicidad 1 puesto que G es abeliano. Si a esto unimos la descomposición de J^* dada por el corolario 2.5.2, hemos demostrado el resultado recogido a continuación.

Proposición 2.5.6 *El carácter regular de G se puede descomponer como suma de super-caracteres de la forma siguiente:*

$$\rho_G = \xi_0 + \sum_{i=1}^{n-1} \sum_{\alpha \in \mathbb{F}_q^*} \xi_{\mathbf{\Psi}_i(\alpha)}.$$

Una vez que hemos terminado de describir los super-caracteres, estudiamos las super-clases de G. La situación que encontramos es dual a la de las órbitas de cotransición. De hecho, el resultado siguiente es dual de la proposición 2.5.1.

Proposición 2.5.7 *Sea $1 + a = 1 + \sum_{j=1}^{t} a_j x^j,\ a_t \neq 0$, un elemento de G. Entonces la super-clase que contiene al elemento $1 + a$ es*

$$\Phi(1 + a) = 1 + a_t x^t + \langle x^{t+1}, \ldots, x^{n-1} \rangle.$$

Demostración: Sea $1 + a = 1 + \sum_{j=1}^{t} a_j x^j,\ a_t \neq 0$. Es claro que la órbita de transición que contiene a a, Ψ_a, está contenida en el espacio afín $a_t x^t + \langle x^{t+1}, \ldots, x^{n-1} \rangle$. Por tanto, la super-clase

$$\Phi(1 + a) \subseteq 1 + a_t x^t + \langle x^{t+1}, \ldots, x^{n-1} \rangle.$$

Recíprocamente, supongamos que $z = 1 + b$ es un elemento de $1 + a_t x^t + \langle x^{t+1}, \ldots, x^{n-1} \rangle$. Este elemento pertenece a la super-clase $\Phi(1 + a)$ si y sólo si $b \in \Psi_a$, es decir, si y sólo si existe un elemento $y \in G$ tal que $b = ya$. Si $b = \sum_{j=t+1}^{n-1} b_j x^j$ e $y = 1 + \sum_{j=1}^{n-1} y_j x^j$, esta condición se traduce en el siguiente sistema de $n - t - 1$ ecuaciones e incógnitas

$$\begin{cases} a_t y_1 = b_{t+1} - a_{t+1} \\ a_{t+1} y_1 + a_t y_2 = b_{t+2} - a_{t+2} \\ \vdots \\ a_{n-2} y_1 + \cdots + a_t y_{n-t-1} = b_{n-1} - a_{n-1} \end{cases}$$

El determinante del sistema es $a_t^{n-t-1} \neq 0$, pues por hipótesis $a_t \neq 0$. Por tanto el sistema tiene solución única y

$$1 + a_t x^t + \langle x^{t+1}, \ldots, x^{n-1} \rangle \subseteq \Phi(1+a),$$

con lo que el resultado queda probado. ■

Análogamente a lo que sucede con las órbitas de cotransición, las super-clases de G vienen parametrizadas por los elementos $1 + a_t x^t$, con $a_t \in \mathbb{F}_q$ y $1 \leq t \leq n-1$, lo que permite descomponer el grupo G como se explica a continuación.

Corolario 2.5.8 *El grupo G se puede escribir como la unión disjunta de super-clases*

$$G = \bigcup_{i=1}^{n-1} \bigcup_{\alpha \in \mathbb{F}_q^*} \Phi_i(\alpha) \bigcup \Phi_0,$$

donde $\Phi_i(\alpha)$ es la super-clase que contiene al elemento $1 + \alpha x^i$.

Demostración: Sea $1 + a \neq 1$ un elemento cualquiera de G. Sea x^t es el término de menor grado de a, entonces por la proposición 2.5.7 $1+a \in \Phi_t(a_t)$ por. Por otra parte, si $a = 0$, entonces $1 + a = 1 \in \Phi_0$. ■

Por último, una vez descritas las órbitas de cotransición en J^* y las super-clases de G, estamos en condiciones de encontrar una expresión explícita para los super-caracteres de G.

Teorema 2.5.9 *Sea $\mathbf{\Psi} = \mathbf{\Psi}_s(f_s)$ la órbita de cotransición que contiene a $f = f_s(x_s)^*$, entonces el super-carácter asociado $\xi_{\mathbf{\Psi}}$ viene dado por:*

$$\xi_{\mathbf{\Psi}}(1) = q^{s-1}, \quad \xi_{\mathbf{\Psi}}(1 + a_t x^t) = \begin{cases} q^{s-1} & s < t, \\ q^{s-1}\psi(f_s a_s) & s = t, \\ 0 & s > t. \end{cases}$$

Demostración: Por el corolario 2.5.3 se sigue que $\xi_{\mathbf{\Psi}}(1) = q^{s-1}$, lo que da la primera parte del teorema. Como consecuencia del lema 2.4.2 y del corolario 2.5.8 es suficiente calcular los valores del super-carácter $\xi_{\mathbf{\Psi}}$ en los elementos $1 + a_t x^t$, con $a_t \neq 0$ y $t = 1, \ldots, n-1$, para conocerlo en todos los elementos de G. Podemos distinguir dos casos:

1. Si $s \leq t$, por el corolario 2.5.4 se tiene

$$\begin{aligned}\xi_{\mathbf{\Psi}}(1 + a_t x^t) &= \psi_{f_s(x^s)^*}(a_t x^t) \prod_{i=1}^{s-1} \left(\sum_{\alpha \in \mathbb{F}_q} \psi_{\alpha_i (x^i)^*}(a_t x^t) \right) \\ &= \psi(f_s a_t \delta_{s,t}) \prod_{i=1}^{s-1} \left(\sum_{\alpha \in \mathbb{F}_q} \psi(0) \right) = q^{s-1} \psi(f_s a_t \delta_{s,t}).\end{aligned}$$

2. Si $s > t$, tendremos

$$\begin{aligned}\xi_{\mathbf{\Psi}}(1 + a_t x^t) &= \psi_{f_s(x^s)^*}(a_t x^t) \prod_{\substack{i=1 \\ i \neq t}}^{s-1} \left(\sum_{\alpha \in \mathbb{F}_q} \psi_{\alpha (x^i)^*}(a_t x^t) \right) \left(\sum_{\beta \in \mathbb{F}_q} \psi_{\beta (x^t)^*}(a_t x^t) \right) \\ &= \psi(0) \prod_{\substack{i=1 \\ i \neq t}}^{s-1} \left(\sum_{\alpha \in \mathbb{F}_q} \psi(0) \right) \left(\sum_{\beta \in \mathbb{F}_q} (\beta a_t) \right) = q^{s-2} \left(\sum_{\beta \in \mathbb{F}_q} \psi_{a_t}(\beta) \right) \\ &= q^{s-1} \langle \psi_{a_t}, 1_{\mathbb{F}_q} \rangle_{\mathbb{F}_q} = 0,\end{aligned}$$

siempre y cuando $a_t \neq 0$, pues en ese caso ψ_{a_t} es un carácter no trivial de $\mathbb{F}_q$. ■

Capítulo 3

La aproximación combinatoria

Sea A la $\mathbb{F}_q$-álgebra finita de los polinomios en m indeterminadas no conmutativas, $x_1, \ldots, x_m$, con coeficientes en $\mathbb{F}_q$ y de grado estrictamente menor que n. Si X es el conjunto de indeterminadas, denotamos esta álgebra por $\mathbb{F}_q(n, X)$. El radical de Jacobson $J = J(A)$ está formado por todos los polinomios de A cuyo término independiente es nulo. Este capítulo continúa con el problema planteado en la sección 2.5 y trata de estudiar los super-caracteres del grupo de álgebra $G = 1 + J$. Para ello, es suficiente conocer las órbitas de la acción de cotransición de G sobre el espacio dual J^*. Sin embargo, si exceptuamos los casos más simples, estas órbitas, y por tanto los super-caracteres asociados, no tienen una descripción sencilla, sobre todo si el número m de indeterminadas es grande.

La estrategia que seguiremos será la de encontrar una descripción combinatoria de órbitas y super-caracteres, en la línea del trabajo de Carlos André (ver sección 1.3). Para ello, puesto que J es el $\mathbb{F}_q$-espacio vectorial generado por los monomios de la forma $x_{i_1}^{\alpha_1} \ldots x_{i_r}^{\alpha_r}$, con $1 \leq i_1, \ldots, i_r \leq m$ no necesariamente distintos, $\alpha_j > 0$ para todo j y $\sum_{j=1}^{r} \alpha_j < n$; dotaremos a este conjunto de un orden adecuado y probaremos que se puede asociar a cada

elemento $f \in J^*$ un conjunto básico D y un carácter básico $\xi_D(\varphi)$ de forma que el super-carácter ξ_f sea un constituyente suyo. Sin embargo, al contrario de lo que sucede en el caso del grupo $U_n(q)$ (ver sección 1.4), estos nuevos caracteres básicos no son super-caracteres, sino una combinación lineal de ellos. Aún así, constituyen un sistema de caracteres ortogonales que descompone el carácter regular de G.

3.1. Caracteres básicos. Definición y propiedades

El conjunto $\mathcal{B} = \{x_{i_1}^{\alpha_1} \dots x_{i_r}^{\alpha_r} : 1 \leq i_1, \dots, i_r \leq m,\ \alpha_j > 0,\ \sum_{j=1}^{r} \alpha_j < n\}$ es claramente una base de J. Para simplificar, nos referiremos al monomio $x_{i_1}^{\alpha_1} \dots x_{i_r}^{\alpha_r}$ de una forma más compacta como μ; el conjunto de índices asociado será $i(\mu) = \{i_1, \dots, i_r\}$ y el de exponentes $\alpha(\mu) = \{\alpha_1, \dots, \alpha_r\}$.

Definición 3.1.1 *Sean μ y ν monomios, entonces $\mu < \nu$ si existen monomios γ y δ, no necesariamente diferentes de 1, tales que $\nu = \gamma\mu\delta$.*

Es fácil ver que 3.1.1 es un orden parcial para el conjunto de monomios generadores, pero no es total. Por ejemplo, si $A = \mathbb{F}_q(4, \{x, y\})$ es el álgebra de polinomios en las indeterminadas no conmutativas x, y cuyo grado es estrictamente menor que 4, los monomios xyx e y^2 no son comparables por la relación $<$.

Puesto que $\mathcal{B}$ es una base de J, para cada $\mu \in \mathcal{B}$ podemos definir la aplicación $\mu^* : J \to \mathbb{F}_q$ tal que $\mu^*(\nu) = \delta_{\mu,\nu}$, para todo $\nu \in \mathcal{B}$. El conjunto $\mathcal{B}^* = \{\mu^* : \mu \in \mathcal{B}\}$ es la base dual de $\mathcal{B}$. El orden $<$ se puede extender a $\mathcal{B}^*$ con sólo considerar $\mu^* < \nu^*$ si y sólo si $\mu < \nu$.

Como paso previo al estudio de las órbitas de cotransición, vemos cómo actúa el grupo sobre cada uno de los elementos de la base dual.

Proposición 3.1.2 *Sea* $\mu^* = (x_{i_1}^{\alpha_1} \dots x_{i_r}^{\alpha_r})^*$ *un elemento de* $\mathcal{B}^*$, *y sea* $\nu = x_{j_1}^{\beta_1} \dots x_{j_s}^{\beta_s}$ *un monomio, entonces*

$$\nu\mu^* = \begin{cases} (x_{i_1}^{\alpha_1} \dots x_{i_{k-1}}^{\alpha_{k-1}})^* & \text{si existe k tal que } x_{i_k}^{\alpha_k} = x_{j_1}^{\beta_1}, \dots, x_{i_r}^{\alpha_r} = x_{j_s}^{\beta_s}, \\ 0 & \text{en otro caso.} \end{cases}$$

Por otra parte,

$$\mu^*\nu = \begin{cases} (x_{i_{k+1}}^{\alpha_{k+1}} \dots x_{i_r}^{\alpha_r})^* & \text{si existe k tal que } x_{i_1}^{\alpha_1} = x_{j_1}^{\beta_1}, \dots, x_{i_k}^{\alpha_k} = x_{j_s}^{\beta_s}, \\ 0 & \text{en otro caso.} \end{cases}$$

Demostración: Probaremos el resultado únicamente para la acción izquierda, puesto que para la derecha la demostración es análoga. Supongamos entonces que existe un k tal que $x_{i_k}^{\alpha_k} = x_{j_1}^{\beta_1}, \dots, x_{i_r}^{\alpha_r} = x_{j_s}^{\beta_s}$, por lo que para todo $\delta \in \mathcal{B}$

$$\nu\mu^*(\delta) = \mu^*(\delta x_{j_1}^{\beta_1} \dots x_{j_s}^{\beta_s}) = (x_{i_1}^{\alpha_1} \dots x_{i_{k-1}}^{\alpha_{k-1}} x_{i_k}^{\alpha_k} \dots x_{i_r}^{\alpha_r})^*(\delta x_{i_k}^{\alpha_k} \dots x_{i_r}^{\alpha_r}).$$

Es claro que $\nu\mu^*(\delta x_{j_1}^{\beta_1} \dots x_{j_s}^{\beta_s}) \neq 0$ si y sólo si $\delta = x_{i_1}^{\alpha_1} \dots x_{i_{k-1}}^{\alpha_{k-1}}$, de donde se sigue que

$$\nu\mu^* = (x_{i_1}^{\alpha_1} \dots x_{i_{k-1}}^{\alpha_{k-1}})^*.$$

■

Nota 3.1.3 *Como consecuencia de este resultado,* $\mu\mu^* = \mu^*\mu = 0$ *para cualquier monomio* $\mu \in \mathcal{B}$.

Dado $f \in J^*$ un elemento cualquiera, no es fácil encontrar una expresión simple para su órbita de cotransición. Nuestro objetivo consiste en intentar describir la órbita de f a partir de las órbitas de sus monomios. Para ello, necesitamos introducir la siguiente definición:

Definición 3.1.4 *Sea $\mu^* \in \mathcal{B}^*$ un elemento de la base dual. Entonces:*

1. $J_\mu = \langle \nu : \nu \not< \mu \rangle_{\mathbb{F}_q}$,

2. $V_\mu = J_\mu^\perp = \langle \nu^* : \nu^* < \mu^* \rangle_{\mathbb{F}_q}$.

Notemos que dado un elemento $\mu^* \in \mathcal{B}^*$, el conjunto $\{\nu^* : \nu^* \not< \mu^*\}$ está formado no sólo por los monomios $\nu^* > \mu^*$, sino también por aquellos que no son comparables con μ^* por la relación de orden.

Proposición 3.1.5 *Sea $\mu^* \in \mathcal{B}^*$ un elemento de la base dual. El conjunto J_μ es un ideal bilátero de J y por tanto, $1 + J_\mu$ es un subgrupo normal de G.*

Demostración: Sea β un elemento de J_μ, entonces $\beta \not< \mu$, es decir, no existen monomios γ y δ tales que $\gamma\beta\delta = \mu$. Por tanto, $\varepsilon\beta \not< \mu$ y $\beta\varepsilon \not< \mu$, para todo monomio $\varepsilon \in \mathcal{B}$. En consecuencia, $\varepsilon\beta \in J_\mu$ y $\beta\varepsilon \in J_\mu$, para todo $\varepsilon \in \mathcal{B}$. Así pues, J_μ es un ideal bilátero de J, y de acuerdo con la terminología de [42], $1 + J_\mu$ es un subgrupo ideal de G. Es fácil ver que todo subgrupo ideal es normal en G. ■

El siguiente resultado permite encontrar un espacio afín que contiene a la órbita de cada monomio, lo que constituye un primer paso para la construcción de los caracteres básicos.

Proposición 3.1.6 *Sea $f = c_\mu \mu^*$, con $c_\mu \in \mathbb{F}_q^*$. Entonces:*

1. $J_\mu \subseteq \mathcal{R}(f) \cap \mathcal{L}(f)$,

2. $\mathbf{\Psi}_f = \mathbf{\Psi}_\mu(c_\mu) \subseteq c_\mu \mu^* + V_\mu = c_\mu \mu^* + \langle \nu^* : \nu^* < \mu^* \rangle$.

Demostración: Para probar la primera afirmación consideramos β un monomio generador de J_μ y ε uno de J. Por definición, no existen monomios,

incluida la identidad, γ y δ tales que $\gamma\beta\delta = \mu$. Por tanto, $f(\beta\varepsilon) = 0$ y $f(\varepsilon\beta) = 0$ para todo $\varepsilon \in \mathcal{B}$, es decir, $\beta \in \mathcal{R}(f) \cap \mathcal{L}(f)$ y el resultado se sigue.

Para probar el segundo punto, tomamos $x = 1+a$, $y = 1+b$ dos elementos cualesquiera de G. Es claro que

$$xfy = (1+a)f(1+b) = f + af + fb + afb.$$

Por la proposición 3.1.2, concluimos que af, fb y afb son elementos del subespacio vectorial V_μ. Por lo tanto:

$$\mathbf{\Psi}_f = \mathbf{\Psi}_\mu(c_\mu) \subseteq c_\mu\mu^* + V_\mu = c_\mu\mu^* + \langle \nu^* : \nu^* < \mu^* \rangle.$$

■

Es importante notar que la órbita de cotransición $\mathbf{\Psi}_f$ puede estar contenida estrictamente en el subespacio afín $c_\mu\mu^* + \langle \nu^* : \nu^* < \mu^* \rangle$, como se puede apreciar en el siguiente ejemplo.

Ejemplo 3.1.7 *Sea $A = \mathbb{F}_q(4, \{x, y\})$. El elemento $(xyx)^* + y^* \in J^*$ pertenece al subespacio $(xyx)^* + \langle \nu^* : \nu^* < (xyx)^* \rangle$ pero no pertenece a la órbita $\mathbf{\Psi}_{(xyx)^*}$. Si así fuera, podríamos encontrar elementos a y b en J tales que $a\,(xyx)^* + (xyx)^*b + a\,(xyx)^*b = y^*$, lo que se verifica si y sólo si $a\,(xyx)^* = 0$, $(xyx)^*b = 0$, $a\,(xyx)^*b = y^*$, de donde se deduce que $a = b = x$. Sin embargo, $(1+x)\,(xyx)^*(1+x) \neq (xyx)^* + y^*$.*

En caso de que f sea un elemento cualquiera de J^*, no necesariamente un monomio, podemos definir los siguientes conjuntos:

Definición 3.1.8 *Sea $f = \sum_{\mu \in I} c_\mu \mu^*$ un elemento de J^*. Entonces:*

1. $J_f = \bigcap_{\mu \in I} J_\mu$,
2. $V_f = (J_f)^\perp = \sum_{\mu \in I} V_\mu$.

Notemos que para el álgebra conmutativa $A = \mathbb{F}_q(n, \{x\})$ esta definición se reduce a la de la proposición 2.5.1. En ese caso, el orden $<$ definido sobre el conjunto de monomios $\{x, x^2, \ldots, x^{n-1}\}$ es total y se puede expresar como $x^i < x^j$ si y sólo si $i < j$. Si tomamos un elemento $f = \sum_{i=1}^{s} f_i(x^i)^*$, con $f_s \neq 0$, por la definición anterior a cada monomio x^i le asociamos el conjunto $J_i = \langle x^k : i \leq k \rangle$, y puesto que $i < j$ implica $J_j < J_i$, el conjunto J_f será

$$J_f = \bigcap_{\substack{i=1 \\ f_i \neq 0}}^{s} J_i = J_s = \langle x^s, \ldots, x^{n-1} \rangle,$$

como se obtenía en la proposición 2.5.1.

De nuevo en el caso general, $A = \mathbb{F}_q(n, X)$, encontramos el siguiente resultado, análogo a la proposición 3.1.5.

Proposición 3.1.9 *Sea $f = \sum_{\mu \in I} c_\mu \mu^*$ un elemento de J^*, entonces J_f es un ideal de J, y por tanto $1 + J_f$ es un subgrupo normal de G.*

Demostración: La proposición 3.1.5 establece que cada J_μ es un ideal bilátero de J, por lo que su intersección J_f también lo será. Así pues, $1 + J_f$ es un subgrupo ideal, y por tanto normal, de G. ■

La siguiente definición es crucial a la hora de dar una descripción combinatoria de las órbitas de cotransición de J^*. Constituye una generalización de la noción de conjunto básico introducida en 1.3.3.

Definición 3.1.10 *Un subconjunto $D \subseteq \mathcal{B}$ se dice básico si es vacío o si sus elementos son no comparables dos a dos por la relación $<$.*

Puesto que $\mu^* < \nu^*$ si y sólo si $\mu < \nu$, un subconjunto $D^* \subseteq \mathcal{B}^*$ es básico si y sólo si el subconjunto $D = \{\mu : \mu^* \in D^*\} \subseteq \mathcal{B}$ lo es. De esta forma, podemos hablar indistintamente de subconjuntos básicos de la base $\mathcal{B}$ o de su dual $\mathcal{B}^*$.

Definición 3.1.11 *Sea $D \subseteq \mathcal{B}$ un conjunto básico no vacío. Entonces:*

1. $J_D = \bigcap_{\nu \in D} J_\nu$,
2. $V_D = J_D^\perp = \sum_{\nu \in D} V_\nu$.

Nota 3.1.12 *En caso que $D = \emptyset$ el ideal $J_D = J$ y $V_D = 0$.*

El resultado siguiente es clave, pues permite relacionar cada elemento $f \in J^*$ con un único conjunto básico.

Proposición 3.1.13 *Sea $f = \sum_{\mu \in I} c_\mu \mu^*$ un elemento de J^*. Si $f_0 = f|_{J_f} = \sum_{\nu \in D} c_\nu \nu^*$, entonces existe un conjunto básico D tal que:*

1. $J_D = J_{f_0} \subseteq \mathcal{R}(f) \cap \mathcal{L}(f)$,
2. $\mathbf{\Psi}_f \subseteq \sum_{\nu \in D} c_\nu \nu^* + V_f = f_0 + V_D$.

Demostración: Dado $f = \sum_{\mu \in I} c_\mu \mu^*$, consideramos $D \subseteq I$ el subconjunto formado por todos aquellos índices tales que el conjunto $\{\nu^* : \nu \in D\}$ está constituido por todos los elementos maximales de $\{\mu^* : \mu \in I\}$. Es fácil ver que en estas condiciones D es un conjunto básico.

Supongamos que $\mu^* < \nu^*$, entonces $V_\mu \subseteq V_\nu$ y por tanto, $J_\nu \subseteq J_\mu$. Puesto que los elementos de D son maximales se sigue que

$$J_f = \bigcap_{\mu \in I} J_\mu = \bigcap_{\nu \in D} J_\nu = J_D = J_{f_0},$$

con $f_0 = f|_{J_f} = \sum_{\nu \in D} c_\nu \nu^*$, también por maximalidad. Sea β un monomio generador de J_D. Los elementos del conjunto $\{\nu^* : \nu \in D\}$ son maximales, así pues, no existen monomios γ y δ, no necesariamente distintos de la identidad, tales que $\gamma\beta\delta = \mu$ para todo $\mu \in I$. Por tanto, $f(\beta\varepsilon) = 0$ y $f(\varepsilon\beta) = 0$ para todo $\varepsilon \in \mathcal{B}$, es decir, $\beta \in \mathcal{R}(f) \cap \mathcal{L}(f)$.

Para probar el segundo resultado partimos de dos elementos cualesquiera $y = 1 + a$, $z = 1 + b$ de G. Por la proposición 3.1.6 y por la maximalidad de los elementos del conjunto básico D tenemos que

$$yfz = y\left(\sum_{\mu\in I} c_\mu \mu^*\right) z = \sum_{\mu\in I} c_\mu (y\mu^* z) \in f + V_f = f_0 + V_D.$$

Y debido a que $V_D \leq J^*$ es estable para la acción de cotransición, la órbita $\mathbf{\Psi}_f$ está contenida en $f_0 + V_D$. ■

Definición 3.1.14 *Sea $f = \sum_{\mu\in I} c_\mu \mu^*$ un elemento de J^*. La forma reducida de f es la restricción $f_0 = f|_{J_f}$.*

Está claro que cada elemento $f \in J^*$ determina una única forma reducida f_0 por restricción y por tanto, un único conjunto básico $D \subseteq \mathcal{B}$. Recíprocamente, cada conjunto básico $D \subseteq \mathcal{B}$ determina un único subespacio $V_D = \langle \nu^* : \nu \in D \rangle$, pero no ocurre lo mismo con las formas reducidas, pues cada función $f_0 \in V_D$ es una forma reducida compatible con D. No obstante, podemos particularizar aún más si consideramos una función φ que nos dé los coeficientes. De esta forma, podemos asociar una única forma reducida a cada par (D, φ).

Definición 3.1.15 *Sea $D \subseteq \mathcal{B}$ un conjunto básico y sea $\varphi : D \to \mathbb{F}_q^*$ una función cualquiera. La forma reducida asociada al par (D, φ) es el elemento $f_0 = \sum_{\nu\in D} \varphi(\nu)\nu^*$.*

Una vez establecido el concepto de conjunto básico, será posible introducir los caracteres básicos como productos de caracteres asociados a cada elemento del conjunto.

Definición 3.1.16 *Sea $D \subseteq \mathcal{B}$ un conjunto básico y sea $\varphi : D \to \mathbb{F}_q^*$ una función cualquiera. Si $c_\nu = \varphi(\nu)$ para todo $\nu \in D$, el carácter básico $\xi_D(\varphi)$ se define como*

$$\xi_D(\varphi) = \begin{cases} \prod_{\nu\in D}(\lambda_{c_\nu\nu^*}|_{1+J_\nu})^G & \text{si } D \neq \emptyset, \\ 1_G & \text{si } D = \emptyset. \end{cases}$$

En primer lugar debemos comprobar que $\xi_D(\varphi)$ es un carácter. El caso $D = \emptyset$ es trivial, pues $\xi_D(\varphi) = 1_G$. En otro caso, por la proposición 3.1.6, $J_\nu \leq \mathcal{R}(c_\nu\nu^*)$ y por el lema 2.2.1 $\lambda_{c_\nu\nu^*}|_{1+J_\nu}$ es un carácter de $1 + J_\nu$ para cada $\nu \in D$. Su producto es claramente un carácter de G.

Los resultados siguientes van encaminados a probar que los caracteres básicos forman un conjunto de caracteres ortogonales. Comenzamos por escribir cada uno de ellos como un carácter inducido.

Lema 3.1.17 *Sea $D \subseteq \mathcal{B}$ un conjunto básico no vacío, sea $\varphi : D \to \mathbb{F}_q^*$ una aplicación cualquiera y sea $\xi_D(\varphi)$ el correspondiente carácter básico. Si $f_0 = \sum_{\nu\in D}\varphi(\nu)\nu^*$ es la forma reducida asociada a (D, φ), entonces*

$$\xi_D(\varphi)(x) = \begin{cases} \displaystyle\prod_{\nu\in D} |J : J_\nu|\ \lambda_{f_0}(x) & \text{si } x \in 1 + J_D = 1 + \bigcap_{\nu\in D} J_\nu, \\ 0 & \text{en otro caso.} \end{cases} \tag{3.1}$$

Demostración: Sea $x = 1 + a$, con $a \in J$. Por analogía con la demostración del teorema 2.2.4, para cada $\nu \in D$ podemos escribir

$$(\lambda_{c_\nu\nu^*}|_{1+J_\nu})^G(1 + a) = \frac{1}{|J_\nu|}\sum_{y\in G}\lambda^\circ[y(1 + a)y^{-1}].$$

Por la proposición 3.1.9, el subgrupo $1 + J_\nu$ es normal en G. Así pues, la función λ° viene dada por la siguiente expresión:

$$\lambda^\circ(1 + a) = \begin{cases} \lambda(1 + a) & \text{si } a \in J_\nu, \\ 0 & \text{en otro caso.} \end{cases}$$

Supongamos que $a \in J_\nu$, entonces

$$(\lambda_{c_\nu\nu^*}|_{1+J_\nu})^G(1+a) = \frac{1}{|J_\nu|}\sum_{y\in G}\psi_{c_\nu\nu^*}(yay^{-1}) = \frac{1}{|J_\nu|}\sum_{y\in G}\psi_{c_\nu y^{-1}\nu^* y}(a).$$

Como consecuencia de la proposición 3.1.6 y de la definición 3.1.4, la órbita $\mathbf{\Psi}_\mu(c_\mu) \subseteq c_\nu\nu^* + V_\nu$, con $V_\nu = J_\nu^\perp$, y para todo $y \in G$ se tiene que $\psi_{y^{-1}c_\nu\nu^* y}(a) = \psi(c_\nu\nu^*(a) + g(a)) = \psi(c_\nu\nu^*(a))$, pues $g \in J_\nu^\perp$. Por tanto, para cada $\nu \in D$ el carácter inducido

$$\lambda^G_{c_\nu\nu^*}(x) = \begin{cases} |J : J_\nu|\,\lambda_{c_\nu\nu^*}(x) & \text{si } x \in 1+J_\nu, \\ 0 & \text{en otro caso.} \end{cases}$$

Por último, si $f_0 = \sum_{\nu\in D}\varphi(\nu)\nu^*$ es la forma reducida asociada al par (D,φ), basta sustituir en la fórmula del carácter básico para obtener

$$\xi_D(\varphi)(x) = \begin{cases} \displaystyle\prod_{\nu\in D}|J : J_\nu|\ \lambda_{f_0}(x) & \text{si } x \in 1+J_D = 1+\bigcap_{\nu\in D}J_\nu, \\ 0 & \text{en otro caso.} \end{cases}$$

■

Lema 3.1.18 *Sea $D \subseteq \mathcal{B}$ un conjunto básico no vacío, sea $\varphi : D \to \mathbb{F}_q^*$ una aplicación cualquiera y sea $\xi_D(\varphi)$ el correspondiente carácter básico. Entonces $\xi_D(\varphi)$ es un múltiplo entero de $(\lambda_{f_0}|_{1+J_D})^G$, es más*

$$\xi_D(\varphi) = \frac{\prod_{\nu\in D}|J : J_\nu|}{|J : J_D|}\,(\lambda_{f_0}|_{1+J_D})^G.$$

Demostración: Sea f_0 la forma reducida asociada al par (D,φ), entonces, por la proposición 3.1.13, $J_D = J_{f_0}$ y por un argumento análogo al de la demostración anterior se obtiene la expresión

$$(\lambda_{f_0}|_{1+J_D})^G(x) = \begin{cases} |J : J_D|\ \lambda_{f_0}(x) & \text{si } x \in 1+J_D, \\ 0 & \text{en otro caso,} \end{cases} \tag{3.2}$$

que comparada con la ecuación (3.1) lleva a

$$\xi_D(\varphi) = \frac{\prod_{\nu\in D}|J:J_\nu|}{|J:J_D|}(\lambda_{f_0}|_{1+J_D})^G$$

Sólo falta probar que la constante $\dfrac{\prod_{\nu\in D}|J:J_\nu|}{|J:J_D|}$ es un entero. Para ello basta observar que para cada $\nu \in D$, el índice $|J:J_\nu| = |J_\nu^\perp| = |V_\nu| = q^{dim\, V_\nu}$, por lo que $|J:J_D| = |(\bigcap_{\nu\in D} J_\nu)^\perp| = |\sum_{\nu\in D} V_\nu| = q^{dim\,(\sum_{\nu\in D} V_\nu)}$. Así pues, con sólo sustituir se llega a la igualdad

$$\frac{\prod_{\nu\in D}|J:J_\nu|}{|J:J_D|} = \frac{q^{\sum_{\nu\in D} dim\, V_\nu}}{q^{dim\,(\sum_{\nu\in D} V_\nu)}},$$

que es siempre un entero, puesto que $\sum_{\nu\in D} dim\, V_\nu \geq dim\,(\sum_{\nu\in D} V_\nu)$, con la igualdad únicamente en el caso en que $\sum_{\nu\in D} V_\nu$ es una suma directa (ver teorema I.11 de [46]). ■

Probaremos por fin que los caracteres básicos constituyen un sistema de caracteres ortogonales.

Teorema 3.1.19 *Sean $\xi_D(\varphi)$ y $\xi_{D'}(\varphi')$ dos caracteres básicos. Entonces*

$$\langle \xi_D(\varphi), \xi_{D'}(\varphi')\rangle \neq 0 \text{ si y sólo si } D = D' \text{ y } \varphi = \varphi'.$$

Demostración: Por el lema 3.1.18, existen enteros positivos c_1 y c_2 tales que $\xi_D(\varphi) = c_1\,(\lambda_{f_0}|_{1+J_D})^G$ y $\xi_{D'}(\varphi') = c_2\,(\lambda_{f_0'}|_{1+J_{D'}})^G$, con f_0 y f_0' las formas reducidas asociadas a (D,φ) y (D',φ') respectivamente. De esta forma

$$\langle \xi_D(\varphi), \xi_{D'}(\varphi')\rangle = \mathbf{C}\,\langle (\lambda_{f_0}|_{1+J_D})^G, (\lambda_{f_0'}|_{1+J_{D'}})^G\rangle,$$

con $\mathbf{C}$ un entero positivo. Así pues, el producto escalar de los caracteres básicos será diferente de cero si y sólo si $\langle (\lambda_{f_0}|_{1+J_D})^G, (\lambda_{f_0'}|_{1+J_{D'}})^G\rangle \neq 0$. A partir de (3.2) obtenemos

$$\begin{aligned}\langle(\lambda_{f_0}|_{1+J_D})^G,(\lambda_{f_0'}|_{1+J_{D'}})^G\rangle &= \frac{|J:J_D|\,|J:J_{D'}|}{|J|}\,\langle\lambda_{f_0},\lambda_{f_0'}\rangle_{1+(J_D\cap J_{D'})}\\ &= \frac{|J|}{|J_D+J_{D'}|}\langle\psi_{f_0},\psi_{f_0'}\rangle_{J_D\cap J_{D'}}.\end{aligned}$$

Puesto que ψ_{f_0} y $\psi_{f_0'}$ son caracteres irreducibles de $(J,+)$, el producto escalar $\langle\psi_{f_0},\psi_{f_0'}\rangle_{J_D\cap J_{D'}}\neq 0$ si y sólo si $\psi_{f_0}|_{J_D\cap J_{D'}}=\psi_{f_0'}|_{J_D\cap J_{D'}}$, es decir, si y sólo si $f_0-f_0'\in(J_D\cap J_{D'})^\perp=J_D^\perp+J_{D'}^\perp$; lo que por la proposición 3.1.13 es equivalente a

$$f_0-f_0'\in\sum_{\nu\in D}V_\nu+\sum_{\mu\in D'}V_\mu. \tag{3.3}$$

Recordemos que por la definición de forma reducida $f_0\notin\sum_{\nu\in D}V_\nu$ y $f_0'\notin\sum_{\mu\in D'}V_\mu$. Supongamos $D\neq D'$, entonces podremos distinguir dos casos:

1. Para todo $\mu\in D'$ existe $\nu\in D$ tal que $\mu\leq\nu$. En ese caso, es claro que $\sum_{\mu\in D'}V_\mu\leq\sum_{\nu\in D}V_\nu$ y que $f_0'\in\sum_{\nu\in D}V_\nu$; entonces $f_0\in\sum_{\nu\in D}V_\nu$ y llegamos a una contradicción.

2. En otro caso, siempre podemos encontrar un elemento $\mu\in D'$ tal que μ^* no es comparable con ninguno de los monomios de f_0. Así, $\mu^*\notin\sum_{\nu\in D}V_\nu+\sum_{\mu\in D'}V_\mu$ y por tanto, $f_0-f_0'\notin\sum_{\nu\in D}V_\nu+\sum_{\mu\in D'}V_\mu$.

Una vez que tenemos $D=D'$, la condición 3.3 se reduce a $f_0-f_0'\in\sum_{\nu\in D}V_\nu$, que se satisface si y sólo si $f_0-f_0'=0$. La definición de forma reducida implica $\varphi=\varphi'$. ■

Al igual que ocurre con los super-caracteres, los caracteres básicos constituyen una partición de los irreducibles de G. Como primer paso, probaremos que cada super-carácter es constituyente de un único carácter básico.

Teorema 3.1.20 *Sea f un elemento de J^* y sea $\mathbf{\Psi}$ la órbita de cotransición que lo contiene. El super-carácter $\xi_{\mathbf{\Psi}}$ es constituyente de uno y sólo de un carácter básico $\xi_D(\varphi)$.*

Demostración: Sea $f = \sum_{\mu \in I} c_\mu \mu^*$ un elemento de J^*. Por la proposición 3.1.13, existe un conjunto básico D y una aplicación $\varphi : D \to \mathbb{F}_q^*$ tales que $\mathbf{\Psi} \subseteq f_0 + \sum_{\nu \in D} V_\nu$, con $c_\nu = \varphi(\nu)$ y $f_0 = \sum_{\nu \in D} c_\nu \nu^*$ la forma reducida de f. Por otra parte, sabemos que existe un entero positivo e que satisface $\xi_D(\varphi) = e\,(\lambda_{f_0}|_{1+J_D})^G$ (ver lema 3.1.18) y en consecuencia $\langle \xi_{\mathbf{\Psi}}, \xi_D(\varphi) \rangle = e\,\langle \xi_{\mathbf{\Psi}}, (\lambda_{f_0}|_{1+J_D})^G \rangle$. La reciprocidad de Frobenius (proposición 1.1.15) lleva a la siguiente expresión:

$$\langle \xi_{\mathbf{\Psi}}, \xi_D(\varphi) \rangle = e\,\langle \xi_{\mathbf{\Psi}}, \lambda_{f_0} \rangle_{1+J_D} = e\,\frac{\xi_{\mathbf{\Psi}}(1)}{|\mathbf{\Psi}|} \sum_{g \in \mathbf{\Psi}} \langle \psi_g, \psi_{f_0} \rangle_{J_D}.$$

Puesto que $\mathbf{\Psi} \subseteq f_0 + \sum_{\nu \in D} V_\nu = f_0 + (\bigcap_{\nu \in D} J_\nu)^\perp = f_0 + J_D^\perp$, claramente $g|_{J_D} = f_0$ y por ello, $\langle \psi_g, \psi_{f_0} \rangle_{J_D} = \langle \psi_{f_0}, \psi_{f_0} \rangle_{J_D} > 0$ para todo $g \in \mathbf{\Psi}$. Así pues, $\langle \xi_{\mathbf{\Psi}}, \xi_D(\varphi) \rangle \neq 0$ y $\xi_{\mathbf{\Psi}}$ es constituyente de $\xi_D(\varphi)$. Notemos que $\xi_{\mathbf{\Psi}}$ sólo puede ser constituyente de $\xi_D(\varphi)$ por la ortogonalidad de los caracteres básicos probada en el teorema anterior. ■

Por el teorema 2.3.5 cada carácter irreducible de G es constituyente de un único super-carácter, de ahí se deduce el siguiente resultado.

Corolario 3.1.21 *Sea $\chi \in Irr(G)$. Entonces existen un único conjunto básico $D \subseteq \mathcal{B}$ y una única función $\varphi : D \to \mathbb{F}_q^*$ tales que χ es constituyente de $\xi_D(\varphi)$.*

3.2. Descomposición de los caracteres básicos

En esta sección estudiaremos cómo se descomponen los caracteres básicos en términos de super-caracteres. En primer lugar, veremos que los caracte-

res básicos son constantes sobre las super-clases de G, lo que implica (ver corolario 2.4.4) que se pueden escribir como una combinación lineal compleja de super-caracteres. Probaremos que, sin embargo, esos coeficientes son números enteros. A continuación, estudiaremos un caso particular: los caracteres básicos totalmente ramificados y encontraremos una caracterización. Comenzamos por probar el dual de la proposición 3.1.13.

Lema 3.2.1 *Sea $x = 1 + \sum_{\mu \in I} a_\mu \mu$ un elemento de G y sea Φ la super-clase que lo contiene. Existe un conjunto básico $D' \subseteq \mathcal{B}$ tal que*

$$\Phi \subseteq 1 + \sum_{\nu \in D'} J_\nu.$$

Demostración: Sea $a = \sum_{\mu \in I} a_\mu \mu$. Definimos $D' \subseteq I$ como el conjunto formado por todos los elementos minimales de I. Claramente (ver definición 3.1.10), D' es un conjunto básico.

Sean x e y dos elementos cualesquiera de G, entonces, por la minimalidad de los elementos de D', se tiene que $xay^{-1} = \sum_{\nu \in D'} a_\nu \nu + h$ con $h \in \sum_{\nu \in D'} J_\nu$, de donde se sigue el resultado. ■

Proposición 3.2.2 *Todo carácter básico $\xi_D(\varphi)$ es constante sobre las super-clases de G.*

Demostración: Dado $\xi_D(\varphi)$ un carácter básico cualquiera, recordemos que es constante sobre las super-clases de G (ver definición 2.4.1) si y sólo si se verifica $\xi_D(\varphi)(1+a) = \xi_D(\varphi)(1+xay^{-1})$ para todo $x, y \in G$.

Puesto que $D \subseteq \mathcal{B}$ es un conjunto básico, el subgrupo $1 + J_D$ definido en 3.1.11 es un subgrupo ideal. Así pues, J_D es un ideal bilátero de J y por tanto, para todo par de elementos x e y de G, $xay^{-1} \in J_D$ si y sólo si $a \in J_D$. Si $a \notin J_D$ el resultado se deduce trivialmente, pues por la ecuación (3.1)

$\xi_D(\varphi)(1+xay^{-1}) = 0$ para todo $x, y \in G$. En otro caso, también por (3.1), existe una constante positiva e tal que $\xi_D(\varphi)(1+a) = e\,\lambda_{f_0}(1+a)$. Así pues, para probar el resultado basta considerar $a \in J_D$ y ver que $\lambda_{f_0}(1+a) = \lambda_{f_0}(1+xay^{-1})$ para todo $x, y \in G$.

Por el lema anterior, si $a = \sum_{\mu\in I} a_\mu\mu$ existe un conjunto básico D', formado por los elementos minimales de I, tal que para todo $x, y \in G$ se tiene que $xay^{-1} = \sum_{\nu\in D'} a_\nu\nu + h$ con $h \in \sum_{\nu\in D'} J_\nu$. Notemos que los monomios que forman h no pueden estar en D', pero tampoco pueden estar en D, pues $a \in J_D$ y para cada monomio $\nu \in D'$ no puede existir $\mu \in D$ tal que $\nu < \mu$. Puesto que $f_0 = \sum_{\mu\in D} \varphi(\mu)\mu^*$, se sigue que $f_0(h) = 0$ y entonces para todo $x, y \in G$

$$\begin{aligned} f_0(xay^{-1}) &= f_0(\sum_{\nu\in D'} a_\nu\nu + h) = f_0(\sum_{\nu\in D'} a_\nu\nu) \\ &= \sum_{\mu\in D\cap D'} \varphi(\mu)a_\mu = f_0(a). \end{aligned}$$

En consecuencia $\lambda_{f_0}(1+a) = \lambda_{f_0}(1+xay^{-1})$ y por ello,

$$\xi_D(\varphi)(1+xay^{-1}) = \xi_D(\varphi)(1+a),$$

con lo que queda probado el resultado. ■

Corolario 3.2.3 *El carácter básico $\xi_D(\varphi)$ es una $\mathbb{C}$-combinación lineal de super-caracteres.*

Demostración: Basta aplicar el corolario 2.4.4. ■

Teorema 3.2.4 *Sea $\xi_D(\varphi)$ un carácter básico. Si f_0 es la forma reducida asociada al par (D, φ), existen enteros positivos $C_{\mathbf{\Psi}}$ tales que*

$$\xi_D(\varphi) = \sum_{\mathbf{\Psi}\subseteq f_0+V_D} C_{\mathbf{\Psi}}\xi_{\mathbf{\Psi}}.$$

Demostración: Por el corolario anterior podemos escribir $\xi_D(\varphi)$ como una combinación lineal de super-caracteres. Así, si $\mathbf{\Psi}(G)$ denota el conjunto de todas las órbitas de cotransición en J^*, tenemos que

$$\xi_D(\varphi) = \sum_{\mathbf{\Psi}\in\mathbf{\Psi}(G)} C_{\mathbf{\Psi}}\xi_{\mathbf{\Psi}}.$$

Comenzamos por probar que $C_{\mathbf{\Psi}} \neq 0$ si y sólo si $\mathbf{\Psi} \subseteq f_0 + V_D$. Puesto que los super-caracteres son ortogonales (ver teorema 2.3.1) deducimos que cada constante $C_{\mathbf{\Psi}} = \langle \xi_D(\varphi), \xi_{\mathbf{\Psi}}\rangle / \langle \xi_{\mathbf{\Psi}}, \xi_{\mathbf{\Psi}}\rangle$, por lo que basta probar que $\langle \xi_D(\varphi), \xi_{\mathbf{\Psi}}\rangle \neq 0$ si y sólo si $\mathbf{\Psi} \subseteq f_0 + V_D$. Por el lema 3.1.18, el carácter básico $\xi_D(\varphi) = e\,(\lambda_{f_0}|_{1+J_D})^G$ con e un entero positivo. Por la reciprocidad de Frobenius, proposición 1.1.15, $\langle \xi_D(\varphi), \xi_{\mathbf{\Psi}}\rangle = e\,\langle (\lambda_{f_0}|_{1+J_D})^G, \xi_{\mathbf{\Psi}}\rangle_{1+J} = e\,\langle \lambda_{f_0}, \xi_{\mathbf{\Psi}}\rangle_{1+J_D}$. A partir de la fórmula (2.4) se puede escribir

$$\langle \xi_D(\varphi), \xi_{\mathbf{\Psi}}\rangle = \frac{e\,\xi_{\mathbf{\Psi}}(1)}{|\mathbf{\Psi}|}\sum_{g\in\mathbf{\Psi}}\langle \lambda_{f_0}, \lambda_g\rangle_{1+J_D} = \frac{e\,\xi_{\mathbf{\Psi}}(1)}{|\mathbf{\Psi}|}\sum_{g\in\mathbf{\Psi}}\langle \psi_{f_0}, \mathbf{\Psi}_g\rangle_{J_D}.$$

Puesto que ψ_{f_0} y $\mathbf{\Psi}_g$ son caracteres lineales de $(J,+)$ (ver proposición 1.2.2) sus restricciones a J_D también lo son, por tanto

$$\langle \psi_{f_0}, \mathbf{\Psi}_g\rangle_{J_D} = \begin{cases} 1 & \text{si } g - f_0 \in J_D^{\perp}, \\ 0 & \text{en otro caso.} \end{cases} \tag{3.4}$$

Así pues, $\langle \xi_D(\varphi), \xi_{\mathbf{\Psi}}\rangle \neq 0$ si y sólo si $\mathbf{\Psi} \cap (f_0 + V_D) \neq \emptyset$, pues por la definición 3.1.11 $J_D^{\perp} = V_D$. Ahora bien, como vimos en la proposición 3.1.13 el espacio V_D es estable para la acción de cotransición, por lo que se deduce que $\langle \xi_D(\varphi), \xi_{\mathbf{\Psi}}\rangle \neq 0$ si y sólo si $\mathbf{\Psi} \subseteq f_0 + V_D$.

Sólo resta ver que las constantes $C_{\mathbf{\Psi}}$ son números enteros. Hemos visto que para cada $\mathbf{\Psi} \in \mathbf{\Psi}(G)$ la constante $C_{\mathbf{\Psi}} = \langle \xi_D(\varphi), \xi_{\mathbf{\Psi}}\rangle / \langle \xi_{\mathbf{\Psi}}, \xi_{\mathbf{\Psi}}\rangle$. Supongamos que $\mathbf{\Psi} \subseteq f_0 + V_D$, de la fórmula (3.4) y el lema 3.1.18 concluimos que

$\langle \xi_D(\varphi), \xi_{\mathbf{\Psi}} \rangle = e\,\xi_{\mathbf{\Psi}}(1)$ con e entero y por el teorema 2.3.1, $C_{\mathbf{\Psi}} = e\,|\mathbf{\Psi}|/\xi_{\mathbf{\Psi}}(1)$. Si $f \in \mathbf{\Psi}$, entonces la fórmula (2.3), el lema 2.3.2 y la proposición 2.1.4 conducen a:

$$\frac{|\mathbf{\Psi}|}{\xi_{\mathbf{\Psi}}(1)} = \frac{|Gf|}{|Gf \cap fG|} = \frac{|\mathcal{R}(f)^{\perp}|}{|(\mathcal{R}(f) + \mathcal{L}(f))^{\perp}|} = \frac{q^{dim(\mathcal{R}(f)+\mathcal{L}(f))}}{q^{dim(\mathcal{R}(f))}},$$

que es claramente un entero. El resultado se sigue. ■

Nota 3.2.5 *Es importante notar que mientras que en el grupo $U_n(q)$ los caracteres básicos y los super-caracteres coinciden, en nuestro caso no es así. Consideremos, por ejemplo, el álgebra $\mathbb{F}_q(4, \{x, y\})$. Puesto que los super-caracteres vienen definidos por las órbitas de cotransición y los caracteres básicos por las formas reducidas, bastará encontrar dos elementos de J^* con la misma forma reducida pero cuyas órbitas de cotransición sean distintas. Las funciones $f = (xyx)^*$ y $g = (xyx)^* + y^*$ tienen la misma forma reducida: $f_0 = g_0 = (xyx)^*$. Sin embargo, en el ejemplo 3.1.7 vimos que g no pertenece a la órbita de cotransición de f.*

Una consecuencia importante del teorema 3.2.4 es el resultado que recogemos a continuación.

Corolario 3.2.6 *Sea $D \subseteq \mathcal{B}$ un conjunto básico y $\varphi : D \to \mathbb{F}_q^*$ una aplicación cualquiera. Si f_0 es la forma reducida asociada al par (D, φ) y si $\mathbf{\Psi}(D, \varphi) = \{\mathbf{\Psi} \in \mathbf{\Psi}(G) : \mathbf{\Psi} \subseteq f_0 + V_D\}$, entonces*

$$f_0 + V_D = \bigcup_{\mathbf{\Psi} \in \mathbf{\Psi}(D,\varphi)} \mathbf{\Psi}.$$

Demostración: El par (D, φ) define el carácter básico $\xi_D(\varphi)$, que por el teorema 3.2.4 se puede expresar como

$$\xi_D(\varphi) = \sum_{\mathbf{\Psi} \in \mathbf{\Psi}(D,\varphi)} C_{\mathbf{\Psi}} \xi_{\mathbf{\Psi}} = \frac{\prod_{\nu \in D} |J : J_\nu|}{|J : J_D|} \sum_{\mathbf{\Psi} \in \mathbf{\Psi}(D,\varphi)} \frac{|\mathbf{\Psi}|}{\xi_{\mathbf{\Psi}}(1)} \xi_{\mathbf{\Psi}}.$$

Por la fórmula (3.1), $\xi_D(\varphi)(1) = \prod_{\nu\in D} |J : J_\nu|$, de donde se deduce que $|J : J_D| = |V_D| = \sum_{\mathbf{\Psi}\in\mathbf{\Psi}(D,\varphi)} |\mathbf{\Psi}|$. Puesto que todos los cardinales son finitos y las órbitas de cotransición son disjuntas dos a dos, el resultado se sigue. ■

Si ahora descomponemos cada super-carácter en sus componentes irreducibles de acuerdo con el teorema 2.3.5, tendremos que el carácter básico $\xi_D(\varphi)$ se puede escribir como

$$\xi_D(\varphi) = \frac{\prod_{\nu\in D} |J : J_\nu|}{|J : J_D|} \sum_{\mathbf{\Psi}\in\mathbf{\Psi}(D,\varphi)} \sum_{\chi\in Irr_{\mathbf{\Psi}}} \chi(1)\chi. \tag{3.5}$$

A partir de esta expresión podemos caracterizar los caracteres básicos que son irreducibles, como se prueba en el siguiente resultado.

Teorema 3.2.7 *Sea $D \subseteq \mathcal{B}$ un conjunto básico y sea $\varphi : D \to \mathbb{F}_q^*$ una función cualquiera. El carácter básico $\xi_D(\varphi)$ es irreducible si y sólo si es lineal.*

Demostración: Es claro que si el carácter básico $\xi_D(\varphi)$ es lineal, entonces es irreducible. Por tanto, basta probar la otra implicación.

Supongamos que $\xi_D(\varphi)$ es irreducible. Por el teorema 3.2.4 tiene un único componente, es decir $\xi_D(\varphi) = C_{\mathbf{\Psi}}\xi_{\mathbf{\Psi}}$, y en consecuencia $\mathbf{\Psi} = f_0 + V_D$. De aquí concluimos que

$$1 = \langle \xi_D(\varphi), \xi_D(\varphi) \rangle = C_{\mathbf{\Psi}}^2 \frac{\xi_{\mathbf{\Psi}}(1)^2}{|\mathbf{\Psi}|} = \frac{\prod_{\nu\in D} |J : J_\nu|^2}{|J : J_D|^2} |\mathbf{\Psi}|.$$

Es decir, que se debe cumplir

$$|\mathbf{\Psi}| = \frac{|J : J_D|^2}{\prod_{\nu\in D} |J : J_\nu|^2} = \frac{|V_D|^2}{\prod_{\nu\in D} |V_\nu|^2}.$$

Ahora bien, recordemos que $V_D = \sum_{\nu\in D} V_\nu$ por lo que $|V_D| \leq \prod_{\nu\in D} |V_\nu|$ y el cociente $\dfrac{|V_D|}{\prod_{\nu\in D} |V_\nu|}$ será entero únicamente si se da la igualdad. Puesto

que el cardinal de la órbita $\mathbf{\Psi}$ es un número entero, la única posibilidad es $|V_D| = \prod_{\nu \in D} |V_\nu|$, y por tanto $|\mathbf{\Psi}| = 1$. De la fórmula (3.5) se sigue que $\xi_D(\varphi) = \chi = \chi(1)\chi$ y así, $\chi(1) = 1$. El carácter $\xi_D(\varphi)$ es lineal. ■

Si el carácter $\xi_D(\varphi)$ es irreducible, acabamos de probar que $\xi_D(\varphi)$ es lineal. Por la fórmula (3.1) se tiene que $|J : J_D| = 1$ y por tanto, $J_\nu = J$ para todo $\nu \in D$. Esta situación sólo puede darse si cada monomio ν^* tiene grado 1, por lo que la forma reducida asociada al par (D, φ) será un polinomio homogéneo de grado 1. Hemos probado la siguiente caracterización:

Corolario 3.2.8 *Sea $D \subseteq \mathcal{B}$ un conjunto básico y sea $\varphi : D \to \mathbb{F}_q^*$ una función cualquiera. El carácter básico $\xi_D(\varphi)$ es irreducible si y sólo si la forma reducida asociada al par (D, φ) es un polinomio homogéneo de grado 1.*

De acuerdo con [11], introducimos la siguiente definición:

Definición 3.2.9 *Sea $\xi_D(\varphi)$ un carácter básico. Entonces $\xi_D(\varphi)$ se dice completamente ramificado si y sólo si $\langle \xi_D(\varphi), \chi \rangle = \chi(1)$, para todos los componentes irreducibles de $\xi_D(\varphi)$.*

Por la ecuación (3.5), la condición dada por la definición anterior es equivalente a que se verifique

$$\frac{\prod_{\nu \in D} |J : J_\nu|}{|J : J_D|} = \frac{\prod_{\nu \in D} |V_\nu|}{|V_D|} = 1.$$

Recordemos que $V_D = \sum_{\nu \in D} V_\nu$ y así, la igualdad se da si y sólo si V_D es una suma directa (ver teorema I.11 de [46]). A continuación veremos qué implicaciones tiene esta propiedad.

Lema 3.2.10 *Sea $D \subseteq \mathcal{B}$ un conjunto básico y sea $\varphi : D \to \mathbb{F}_q^*$ una función cualquiera. Si $V_D = \bigoplus_{\nu \in D} V_\nu$ y si $g_\nu \in \varphi(\nu)\nu^* + V_\nu$ para todo $\nu \in D$, entonces la órbita de cotransición*

$$G\left(\sum_{\nu \in D} g_\nu\right) G = \sum_{\nu \in D} G\, g_\nu\, G.$$

Demostración: Para cada $\nu \in D$, denotamos por c_ν el valor $\varphi(\nu)$. Puesto que la acción de cotransición es distributiva, es claro que $G\left(\sum_{\nu \in D} g_\nu\right) G \subseteq \sum_{\nu \in D} G\, g_\nu\, G$, por lo que basta probar el otro contenido.

En primer lugar probaremos que los elementos de G actúan independientemente sobre cada función g_ν. Sea $\delta \in \mathcal{B}$ un monomio tal que $(1+\delta)\, g_\nu = g_\nu + h$ con $h \neq 0$. De la proposición 3.1.2 se sigue que $\delta < \nu$ y por tanto, $\delta^* \in V_\nu$. Dado que V_D es suma directa, se verifica que $V_\nu \cap V_\mu = 0$ para $\nu \neq \mu$, y entonces $\delta \not< \mu$ para cualquier $\mu \neq \nu$; así pues $(1+\delta) g_\mu = g_\mu$ para todo $\mu \neq \nu$. El razonamiento es idéntico para la acción por la izquierda y se extiende a cualquier elemento de G por linealidad.

Ahora bien, si $g \in \sum_{\nu \in D} G\, g_\nu\, G$, es claro que existen elementos a_ν, b_ν, para todo $\nu \in D$, tales que $g = \sum_{\nu \in D} (1 + a_\nu)\, g_\nu\, (1 + b_\nu)$. Entonces, si $x = 1 + \sum_{\nu \in D} a_\nu$ e $y = 1 + \sum_{\nu \in D} b_\nu$, el razonamiento anterior implica que $g = x\left(\sum_{\nu \in D} g_\nu\right) y$. Por tanto, $\sum_{\nu \in D} G\, g_\nu\, G \subseteq G\left(\sum_{\nu \in D} g_\nu\right) G$. ■

Supongamos que $f = \sum_{\nu \in D} f_\nu \in J^*$ satisface $\mathbf{\Psi} = G\, f\, G = \sum_{\nu \in D} G\, f_\nu\, G = \sum_{\nu \in D} \mathbf{\Psi}_\nu$. En ese caso, el super-carácter $\xi_{\mathbf{\Psi}}$ asociado a f se puede escribir como

$$\xi_{\mathbf{\Psi}} = \frac{\xi_{\mathbf{\Psi}}(1)}{|\mathbf{\Psi}|} \sum_{g \in \mathbf{\Psi}} \lambda_g = \frac{\xi_{\mathbf{\Psi}}(1)}{|\mathbf{\Psi}|} \prod_{\nu \in D} \left(\sum_{g \in \mathbf{\Psi}_\nu} \lambda_g \right) = \frac{\xi_{\mathbf{\Psi}}(1)}{|\mathbf{\Psi}|} \prod_{\nu \in D} \frac{|\mathbf{\Psi}_\nu|}{\xi_{\mathbf{\Psi}_\nu}(1)} \xi_{\mathbf{\Psi}_\nu}.$$

La condición que hemos impuesto sobre las órbitas implica que $|\mathbf{\Psi}| = \prod_{\nu \in D} |\mathbf{\Psi}_\nu|$ y también que $\xi_{\mathbf{\Psi}}(1) = |Gf| = \prod_{\nu \in D} |Gf_\nu| = \prod_{\nu \in D} \xi_{\mathbf{\Psi}_\nu}(1)$. Por tanto, el

super-carácter $\xi_{\mathbf{\Psi}} = \prod_{\nu \in D} \xi_{\mathbf{\Psi}_\nu}$. Hemos probado el resultado siguiente:

Lema 3.2.11 *Sea $f = \sum_{\nu \in D} f_\nu \in J^*$ un elemento tal que su órbita de cotransición $\mathbf{\Psi} = \sum_{\nu \in D} \mathbf{\Psi}_\nu$, con $\mathbf{\Psi}_\nu$ la órbita de cotransición que contiene a f_ν. Entonces el super-carácter asociado a $\mathbf{\Psi}$ es el producto $\xi_{\mathbf{\Psi}} = \prod_{\nu \in D} \xi_{\mathbf{\Psi}_\nu}$.*

Como consecuencia, se obtiene la siguiente descomposición para los caracteres básicos completamente ramificados en suma de productos de supercaracteres.

Teorema 3.2.12 *Sea $\xi_D(\varphi)$ un carácter básico completamente ramificado. Si $\mathbf{\Psi} = \sum_{\nu \in D} \mathbf{\Psi}_\nu$ para todo $\mathbf{\Psi} \in \mathbf{\Psi}(D, \varphi)$, entonces se verifica que*

$$\xi_D(\varphi) = \sum_{\mathbf{\Psi} \in \mathbf{\Psi}(D,\varphi)} \frac{|\mathbf{\Psi}|}{\xi_{\mathbf{\Psi}}(1)} \prod_{\nu \in D} \xi_{\mathbf{\Psi}_\nu}.$$

Demostración: Ya que $\xi_D(\varphi)$ es completamente ramificado, $|J : J_D| = \prod_{\nu \in D} |J : J_\nu|$ y entonces el carácter básico $\xi_D(\varphi)$ se puede descomponer de acuerdo con el teorema 3.2.4 como

$$\xi_D(\varphi) = \sum_{\mathbf{\Psi} \in \mathbf{\Psi}(D,\varphi)} \frac{|\mathbf{\Psi}|}{\xi_{\mathbf{\Psi}}(1)} \xi_{\mathbf{\Psi}}.$$

Dada una órbita de cotransición $\mathbf{\Psi} \in \mathbf{\Psi}(D, \varphi)$, escogemos un representante suyo: g. Es fácil ver que $g \in f_0 + V_D$ con f_0 la forma reducida asociada al par (D, φ), es decir: $f_0 = \sum_{\nu \in D} \varphi(\nu)\nu^*$. Por tanto, g se puede descomponer en la suma $g = \sum_{\nu \in D} g_\nu$ con $g_\nu \in \varphi(\nu)\nu^* + V_\nu$ para todo $\nu \in D$. Puesto que $V_D = \bigoplus_{\nu \in D} V_\nu$, por el lema 3.2.10, para cada representante g la órbita de cotransición $G\,g\,G = \sum_{\nu \in D} G\,g_\nu\,G$. Del lema anterior se sigue que el super-carácter asociado es el producto $\xi_{\mathbf{\Psi}} = \prod_{\nu \in D} \xi_{\mathbf{\Psi}_\nu}$. ■

A continuación nos centraremos en el estudio de los caracteres básicos $\xi_D(\varphi)$ completamente ramificados que están constituidos por un único supercarácter. Para ello, debe cumplirse que $|\mathbf{\Psi}(D,\varphi)| = 1$ (ver corolario 3.2.6), es decir, $f_0 + V_D = \mathbf{\Psi}$, con f_0 la forma reducida asociada al par (D,φ).

Lema 3.2.13 *Sea $D \subseteq \mathcal{B}$ un conjunto básico y sea $\varphi : D \to \mathbb{F}_q^*$ una función cualquiera. Si f_0 y $\mathbf{\Psi}$ son respectivamente la forma reducida asociada al par (D,φ) y la órbita de cotransición que la contiene, entonces $f_0 + V_D = \mathbf{\Psi}$ si y sólo si $J_{f_0} = \mathcal{L}(f_0) \cap \mathcal{R}(f_0)$.*

Demostración: Por la proposición 3.1.13, $J_{f_0} \subseteq \mathcal{L}(f_0) \cap \mathcal{R}(f_0)$, por lo que $\mathcal{L}(f_0)^\perp + \mathcal{R}(f_0)^\perp \leq J_{f_0}^\perp = V_D$. A su vez, por la proposición 2.1.4 y por el lema 2.3.2 se tiene que

$$|\mathcal{L}(f_0)^\perp + \mathcal{R}(f_0)^\perp| = \frac{|Gf_0||f_0G|}{|Gf_0 \cap f_0G|} = |\mathbf{\Psi}|.$$

Así pues, $\mathcal{L}(f_0)^\perp + \mathcal{R}(f_0)^\perp = J_{f_0}^\perp$ si y sólo si $|\mathbf{\Psi}| = |V_D|$ y el resultado se sigue. ■

En el caso concreto de los caracteres básicos completamente ramificados el resultado puede mejorarse como se muestra a continuación.

Proposición 3.2.14 *Sea $\xi_D(\varphi)$ un carácter básico completamente ramificado. Si f_0 es la forma reducida asociada al par (D,φ), la órbita $\mathbf{\Psi} = f_0 + V_D$ si y sólo si para cada $\nu \in D$ se verifica que $\mathbf{\Psi}_\nu = \varphi(\nu)\nu^* + V_\nu$.*

Demostración: Puesto que el carácter $\xi_D(\varphi)$ es completamente ramificado, $V_D = \bigoplus_{\nu\in D} V_\nu$ y $\mathbf{\Psi} = Gf_0G = \sum_{\nu\in D} G\,\varphi(\nu)\nu^* G = \sum_{\nu\in D} \mathbf{\Psi}_\nu$. Así pues, por la proposición 3.1.6 tenemos que $|\mathbf{\Psi}| = \prod_{\nu\in D} |\mathbf{\Psi}_\nu| \leq \prod_{\nu\in D} |V_\nu| = |V_D|$. La igualdad se dará si y sólo si $|\mathbf{\Psi}_\nu| = |V_\nu|$ para todo $\nu \in D$. Puesto que los

cardinales son finitos y $\varphi(\nu)\nu^* \in \mathbf{\Psi}_\nu$, esto implica $\mathbf{\Psi}_\nu = \varphi(\nu)\nu^* + V_\nu$ para todo $\nu \in D$. ■

Una vez que conocemos las condiciones que debe satisfacer el par (D, φ) para que el carácter básico $\xi_D(\varphi)$ tenga una única componente, podemos caracterizar los monomios $\mu^* \in J^*$ con esta propiedad.

Teorema 3.2.15 *Sea μ^* un monomio generador de J^*. Su órbita de cotransición $\mathbf{\Psi}_\mu$ coincide con el espacio $\mu^* + V_\mu$ si y sólo si μ^* es un monomio de la forma:*

1. $\mu^* = (x_{i_1}^{\alpha_1})^*$, *con* $\alpha_1 \geq 1$;
2. $\mu^* = (x_{i_1}^{\alpha_1} x_{i_2}^{\alpha_2})^*$, *con* $\alpha_1 = 1$ *y* $\alpha_2 \geq 1$;
3. $\mu^* = (x_{i_1}^{\alpha_1} x_{i_2}^{\alpha_2})^*$, *con* $\alpha_1 > 1$ *y* $\alpha_2 = 1$.

Demostración: Observemos en primer lugar que si μ^* tiene la forma del teorema, $V_\mu = J\mu^* + \mu^* J$, lo que de acuerdo con el lema 3.2.13 garantiza que el espacio $\mu^* + V_\mu$ está compuesto por una única órbita.

Para el caso 1, es trivial ver que $V_\mu = J(x_{i_1}^{\alpha_1})^* = (x_{i_1}^{\alpha_1})^* J$. En los restantes casos, por la proposición 3.1.6, basta probar que $V_\mu \subseteq \mu^* J + J\mu^*$. Supongamos $\alpha_1 = 1$, con lo que $\alpha_2 \geq 1$. Si $\beta^* \neq 0$ es uno de los monomios generadores de V_μ, entonces $\beta^* < \mu^*$, por lo que existen monomios γ, δ tales que $\mu = \gamma\beta\delta$. Si $\gamma = 1$ o $\delta = 1$, es claro que $\beta^* \in \mu^* J + J\mu^*$. En otro caso $\beta^* = (x_{i_2}^k)^*$, con $k < \alpha_2$, y entonces $\beta^* = x_{i_1} x_{i_2}^{\alpha_2 - k} \mu^* \in J\mu^*$. Basta intercambiar los papeles de α_1 y α_2, para probar el caso restante.

Ahora sólo falta demostrar que si $\mathbf{\Psi}_\mu = \mu^* + V_\mu$, entonces μ^* tiene la forma del teorema. Lo haremos por reducción al absurdo. Podemos suponer que $\mu^* = (x_{i_1} \delta x_{i_r})^*$, con $\delta = x_{i_1}^{\alpha_1 - 1} \dots x_{i_r}^{\alpha_r - 1} \in \mathcal{B}$. El monomio δ claramente

pertenece a la intersección $\mathcal{L}(\mu^*) \cap \mathcal{R}(\mu^*)$, pero no a J_μ. Por el lema 3.2.13 V_μ no puede estar compuesta por una única órbita, lo que constituye una contradicción. ■

Corolario 3.2.16 *Sea $D \subseteq \mathcal{B}$ un conjunto básico y sea $\varphi : D \to \mathbb{F}_q^*$ una función cualquiera. Si $\xi_D(\varphi)$ es un carácter básico completamente ramificado, entonces $\xi_D(\varphi)$ está compuesto por un único super-carácter si y sólo si la forma reducida asociada al par (D, φ) es de la forma $f_0 = \sum_{\mu \in D} \varphi(\mu)\mu^*$ con $\mu^* = (x_i^{\alpha_i} x_j^{\alpha_j})^*$ para cada $\mu \in D$, α_i, α_j en las condiciones del teorema anterior y de forma que cada variable de X aparece a lo sumo en un monomio.*

Un caso especial se tiene para un carácter básico completamente ramificado $\xi_D(\varphi)$ para el que la forma reducida asociada a (D, φ) es $f = \sum c_i (x_i^{\alpha_i})^*$. En ese caso el super-carácter asociado a cada monomio es completamente ramificado (ver [11]) por lo que si denotamos $\mathbf{\Psi}_i$ a la órbita de cotransición que contiene a $(x_i^{\alpha_i})^*$, se satisface $|\mathbf{\Psi}_i| = \xi_{\mathbf{\Psi}_i}(1)$. Puesto que el carácter básico es también completamente ramificado, se sigue que $|\mathbf{\Psi}| = \prod_i |\mathbf{\Psi}_i| = \prod_i \xi_{\mathbf{\Psi}_i}(1) = \xi_{\mathbf{\Psi}}(1)$. De donde se sigue que el carácter $\xi_D(\varphi)$ es el producto de los super-caracteres asociados a los monomios de su forma reducida, es decir:

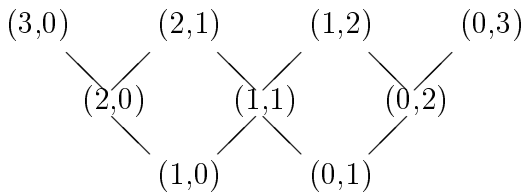
$$\xi_D(\varphi) = \prod_{\nu \in D} \xi_{\mathbf{\Psi}_\nu} = \xi_{\mathbf{\Psi}}.$$

3.3. El álgebra conmutativa libre

Para terminar analizaremos el caso del grupo $G = 1 + J(A)$, con A como en toda la sección, pero además conmutativa. Es decir, que si $X = \{x_1, \ldots, x_m\}$ es el conjunto de generadores, consideramos el cociente $A = \mathbb{F}_q(n, X)/\langle x_i x_j - x_j x_i | \, 1 \leq i < j \leq m \rangle$. Su radical de Jacobson $J = J(A)$ está formado por todos los polinomios en m indeterminadas con coeficientes en $\mathbb{F}_q$, de grado

menor o igual que n y con término independiente igual a cero. Notemos que como A es conmutativa, la base de los monomios generadores de J se puede escribir como $\mathcal{B} = \{\mu = x_1^{\alpha_1} \dots x_m^{\alpha_m} : 0 \leq \alpha_i < n, \sum_{i=1}^{m} \alpha_i < n\}$, mientras que la base dual se representa por $\mathcal{B}^* = \{\mu^* : \mu \in \mathcal{B}\}$, donde $\mu^*\nu = \delta_{\mu,\nu}$ para todo $\nu \in \mathcal{B}$. Recordemos que $\mathcal{B}$ se puede ordenar de acuerdo con la definición 3.1.1, así si $\mu = x_1^{\alpha_1} \dots x_m^{\alpha_m}$ y $\nu = x_1^{\beta_1} \dots x_m^{\beta_m}$, entonces $\mu < \nu$ si y sólo si $\alpha_i \leq \beta_i$ para $i = 1, \dots, m$. Para la base dual $\mathcal{B}^*$ consideramos $\mu^* < \nu^*$ si y sólo si $\mu < \nu$.

A modo de ejemplo, consideremos el álgebra A de los polinomios en las indeterminadas x_1, x_2 y de grado menor que 4. Si a cada monomio $x_1^{\alpha_1} x_2^{\alpha_2}$ le asociamos el par (α_1, α_2), entonces el conjunto ordenado de monomios generadores de J se puede representar de acuerdo con el siguiente diagrama:



A pesar de la conmutatividad, dado un elemento cualquiera de J^*, no es fácil encontrar su órbita de cotransición. Sin embargo, si este elemento es un monomio su órbita viene dada por el siguiente resultado.

Teorema 3.3.1 *Sea $f = c_\mu \mu^*$ con $c_\mu \in \mathbb{F}_q^*$. La órbita de cotransición que contiene a f viene dada por:*

$$\mathbf{\Psi}_f = \mathbf{\Psi}_\mu(c_\mu) = c_\mu \mu^* + \langle \nu^* : \nu^* < \mu^* \rangle_{\mathbb{F}_q}.$$

Demostración: Puesto que A es un álgebra conmutativa, la acción de cotransición coincide con la acción de cotransición izquierda (y derecha). Por

la proposición 3.1.6 sabemos que $\mathbf{\Psi}_f = \mathbf{\Psi}_\mu(c_\mu) \subseteq c_\mu\mu^* + \langle \nu^* : \nu^* < \mu^* \rangle$, por lo que sólo debemos probar el otro contenido.

Supongamos que $\mu^* = (x_1^{\alpha_1} \dots x_m^{\alpha_m})^*$ y consideremos el elemento $g = f + (x_1^{\beta_1} \dots x_m^{\beta_m})^*$ con $(x_1^{\beta_1} \dots x_m^{\beta_m})^* < (x_1^{\alpha_1} \dots x_m^{\alpha_m})^*$, en ese caso se cumple que $\alpha_i - \beta_i \geq 0$ para todo $i = 1, \dots, n$. Así pues, por la proposición 3.1.2 tendremos que $x_1^{\alpha_1-\beta_1} \dots x_m^{\alpha_m-\beta_m}(x_1^{\alpha_1} \dots x_m^{\alpha_m})^* = (x_1^{\beta_1} \dots x_m^{\beta_m})^*$. Consecuentemente $(1 + c^{-1}x_1^{\alpha_1-\beta_1} \dots x_m^{\alpha_m-\beta_m})f = g$, por lo que $g \in \mathbf{\Psi}_f$. Como la acción de cotransición es lineal, el resultado se sigue. ■

Corolario 3.3.2 *Sea $f = c_\mu\mu^*$ con $c_\mu \in \mathbb{F}_q^*$. El estabilizador $\mathcal{L}(f) = \mathcal{R}(f) = J_\mu$, es decir:*

$$\mathcal{L}(f) = \mathcal{R}(f) = \langle \nu^* \in \mathcal{B}^* : \nu^* \not< \mu^* \rangle_{\mathbb{F}_q}.$$

Demostración: Claramente los conjuntos los conjuntos $\mathcal{L}(f)$ y $\mathcal{R}(f)$ coinciden por la conmutatividad de A. Por el teorema anterior y el corolario 2.1.5, tenemos que $(\mathcal{R}(f))^\perp = \langle \nu^* \in \mathcal{B}^* : \nu^* < \mu^* \rangle_{\mathbb{F}_q}$. De la definición 3.1.8 resulta $J_\mu = \langle \nu^* \in \mathcal{B}^* : \nu^* \not< \mu^* \rangle_{\mathbb{F}_q} = \mathcal{R}(f)$. ■

Dado un conjunto básico $D \subseteq \mathcal{B}$ y una aplicación cualquiera $\varphi : D \to \mathbb{F}_q^*$ podemos definir, de acuerdo con 3.1.16, el carácter básico $\xi_D(\varphi)$ como un producto de super-caracteres.

Proposición 3.3.3 *Sea $D \subseteq \mathcal{B}$ un conjunto básico y sea $\varphi : D \to \mathbb{F}_q^*$ una aplicación cualquiera. Si $\mathbf{\Psi}_\nu$ es la órbita de cotransición del elemento $\varphi(\nu)\nu^*$, el carácter básico $\xi_D(\varphi)$ se puede escribir como*

$$\xi_D(\varphi) = \begin{cases} \prod_{\nu \in D} \xi_{\mathbf{\Psi}_\nu} & \text{si } D \neq \emptyset, \\ 1_G & \text{en otro caso.} \end{cases}$$

Demostración: Por el corolario anterior, sabemos que para cada uno de los elementos $f = c_\nu\nu^*$ con $c_\nu \neq 0$ el conjunto $\mathcal{R}(f) = J_\nu$. Por tanto, la

restricción del carácter $\lambda_{c_\nu \nu^*}$ al subgrupo $1+J_\nu$ de la definición 3.1.16 coincide con el propio carácter. De la definición 2.2.3 se sigue que el carácter inducido $\lambda^G_{c_\nu \nu^*}$ es el super-carácter $\xi_{\mathbf{\Psi}_\nu}$ asociado a f. ■

Nota 3.3.4 *Como hemos visto en el teorema 3.2.4 los caracteres básicos se pueden descomponer en suma de super-caracteres. Lo que no siempre es cierto es que un carácter básico sea producto de super-caracteres. Hemos obtenido este resultado al añadir la conmutatividad.*

En lo que resta de sección, trataremos de aplicar los resultados anteriores para obtener la descomposición del carácter básico $\xi_D(\varphi)$ en función de los super-caracteres asociados a cada uno de los monomios $\varphi(\nu)\nu^*$ con $\nu \in D$. En concreto, estamos interesados en el caso en que el carácter básico es a su vez un super-carácter.

En primer lugar, podemos descomponer el carácter básico $\xi_D(\varphi)$ como una combinación lineal de super-caracteres de acuerdo con el teorema 3.2.4. De esta forma, si f_0 es la forma reducida asociada al par (D, φ), debido a que A es conmutativa se tiene que

$$\xi_D(\varphi) = \sum_{\mathbf{\Psi} \subseteq f_0 + V_D} C_{\mathbf{\Psi}} \xi_{\mathbf{\Psi}} = \frac{\prod_{\nu \in D} |J : J_\nu|}{|J : J_D|} \sum_{\mathbf{\Psi} \subseteq f_0 + V_D} \xi_{\mathbf{\Psi}}.$$

Conviene señalar que a pesar de que la conmutatividad, la órbita $\mathbf{\Psi}$ que contiene a f_0 puede no coincidir con el espacio afín $f_0 + V_D$. Por ejemplo, si consideramos el álgebra de polinomios en las indeterminadas x_1, x_2 de grado menor que 4 y la forma reducida $f = (x^2)^* + (xy)^*$ un razonamiento similar al del ejemplo 3.1.7 nos permite ver que $g = (x^2)^* + (xy)^* + y^* \in f_0 + V_D$, pero sin embargo $g \notin \mathbf{\Psi}$. Por tanto, tendremos que $\xi_D(\varphi) = \xi_{\mathbf{\Psi}}$, si y sólo si se verifican estas dos condiciones:

1. $\prod_{\nu \in D} |J : J_\nu| = |J : J_D|$.

2. $\mathbf{\Psi} = f_0 + V_D$.

Ahora bien, la primera condición es equivalente a $V_D = \bigoplus_{\nu \in D} V_\nu$, o lo que es lo mismo, a que el carácter básico $\xi_D(\varphi)$ sea completamente ramificado. En ese caso, puesto que $\mathbf{\Psi}_\nu(\varphi(\nu)) = \varphi(\nu)\nu^* + V_\nu$ para todo $\nu \in D$ (ver teorema 3.3.1), la proposición 3.2.14 implica que $\mathbf{\Psi} = f_0 + V_D$. Acabamos de probar el siguiente resultado.

Teorema 3.3.5 *Sea $D \subseteq \mathcal{B}$ un conjunto básico y sea $\varphi : D \to \mathbb{F}_q^*$ una aplicación cualquiera. Si $\mathbf{\Psi}$ es la órbita de cotransición que contiene a la forma reducida f_0 asociada al par (D, φ), el carácter básico $\xi_D(\varphi)$ es igual al super-carácter $\xi_{\mathbf{\Psi}}$ si y sólo si $\xi_D(\varphi)$ es completamente ramificado.*

Ahora podemos caracterizar los caracteres básicos para los que se da esta propiedad. En realidad, basta caracterizar las formas reducidas para las que V_D es una suma directa.

Corolario 3.3.6 *Sea $D \subseteq \mathcal{B}$ un conjunto básico y sea $\varphi : D \to \mathbb{F}_q^*$ una aplicación cualquiera. Si f_0 es la forma reducida asociada al par (D, φ) y $\mathbf{\Psi}$ es la órbita de cotransición que la contiene, entonces el carácter básico $\xi_D(\varphi)$ es igual al super-carácter $\xi_{\mathbf{\Psi}}$ si y sólo si cada variable de X aparece a lo sumo en un monomio de la forma reducida f_0.*

Demostración: Si D es un conjunto básico, entonces todos los monomios ν^* con $\nu \in D$ son no comparables por la relación $<$. Por el teorema 3.3.1, sabemos que $\mathcal{R}(\nu^*) = V_\nu$ para todo $\nu \in D$. Así pues, si se da la condición anterior, tendremos que cada subespacio V_ν está generado por monomios diferentes y por consiguiente $V_\nu \cap V_\mu = 0$ para $\nu \neq \mu$, lo que implica que V_D es una suma directa. Recíprocamente, si V_D es una suma directa, es claro

que los monomios ν^* con $\nu \in D$ no pueden compartir variables, puesto que en ese caso encontraríamos $\nu, \mu \in D$ distintos y con $V_\nu \cap V_\mu \neq 0$. ■

Capítulo 4

Super-caracteres sobre anillos finitos

Una vez que hemos definido los super-caracteres de un $\mathbb{F}_q$-grupo de álgebra $G = 1 + J(A)$, trataremos de extender este concepto al caso en que A es una R-álgebra asociativa, nilpotente y de dimensión finita, con R un anillo finito, local, conmutativo y con identidad. En ese caso, el grupo de álgebra $G = 1 + J(A)$ se sustituye por el grupo adjunto $G(A)$, que en estas condiciones se puede identificar con el subgrupo $1 + A$ del grupo de unidades del anillo $\mathcal{S} = R \oplus A$.

La primera sección de este capítulo estudia la estructura del grupo abeliano de los $\mathbb{C}$-caracteres aditivos de una R-álgebra de dimensión finita A con R un anillo finito conmutativo. Probaremos que si R es admisible, es decir, si existe un carácter de R a partir del que se pueden obtener todos los restantes, entonces los caracteres aditivos de A se pueden parametrizar en función de los elementos del módulo dual A^* de forma similar a lo que sucedía para las $\mathbb{F}_q$-álgebras.

En la segunda sección, veremos que los anillos finitos admisibles son los

anillos de Frobenius y estudiaremos un caso particular de este tipo de anillos: los anillos de Galois. Por último, en la parte final del capítulo se extiende la noción de super-caracteres al caso en que A es un R-módulo libre de dimensión finita y, paralelamente a lo que se hizo en la sección 2.5, se estudia el caso en que A es la R-álgebra de polinomios en una indeterminada. En ambos casos R es un anillo de Galois.

4.1. Anillos admisibles y caracteres admisibles

Sea $(A,+)$ un grupo abeliano cualquiera. Como vimos en la proposición 1.1.8, todas sus $\mathbb{C}$-representaciones irreducibles son lineales. Así pues, el conjunto de caracteres de A, denotado por $\widehat{A}$, es un subconjunto de $Hom(A,\mathbb{C}^*)$, donde $\mathbb{C}^*$ representa el grupo multiplicativo de $\mathbb{C}$. El conjunto $\widehat{A}$ puede dotarse de una estructura de grupo abeliano si consideramos la suma de caracteres dada por

$$(\varphi+\psi)(a)=\varphi(a)\psi(a),$$

para todo $\varphi,\psi\in\widehat{A}$ y todo $a\in A$. Notemos que el elemento neutro de $\widehat{A}$ es el carácter trivial 1_A.

Sea $(R,+,\cdot)$ un anillo cualquiera. Denotamos por $\widehat{R}$ el grupo de caracteres irreducibles del grupo $(R,+)$. Podemos dotar este conjunto de una estructura de módulo a izquierda (respectivamente a derecha) si consideramos la acción

$$(r\psi)(x)=\psi(xr)\quad(\text{respect. }(\psi r)(x)=\psi(rx)),\tag{4.1}$$

para todo $\psi\in\widehat{R}$, y todo $x,r\in R$. Es claro que si el anillo R es conmutativo las dos acciones coinciden.

Dado un carácter $\psi\in\widehat{R}$, diremos que ψ es *admisible a izquierda* (respectivamente a derecha) si el módulo a izquierda (respectivamente a derecha) $\widehat{R}$ es cíclico y está generado por ψ. En ese caso, la aplicación

$$\begin{array}{rcl} \phi : R & \longrightarrow & \widehat{R} \\ r & \longrightarrow & r\psi \text{ (respec. } \psi r) \end{array} \tag{4.2}$$

es un isomorfismo de módulos. Si el anillo R es conmutativo, el carácter ψ se dice *admisible* y $R \cong \widehat{R}$ como bimódulo. De forma más precisa (ver definición 3.1 de [23]) podemos decir:

Definición 4.1.1 *Un anillo R se dice admisible a izquierda (respec. admisible a derecha) si el R-módulo a izquierda (respec. a derecha) $\widehat{R}$ es cíclico. El anillo R es admisible si es a la vez admisible a izquierda y derecha.*

Los cuerpos finitos constituyen un ejemplo de anillos admisibles. Si $\mathbb{F}_q$ es el cuerpo con $q = p^e$ $(e \geq 1)$ elementos y $\mathbb{F}_p$ es el cuerpo primo de característica p, la función

$$\begin{array}{rcl} Tr_{\mathbb{F}_{q|\mathbb{F}_p}} : \mathbb{F}_q & \longrightarrow & \mathbb{F}_p \\ \alpha & \longrightarrow & \alpha + \alpha^p + \cdots + \alpha^{p^{e-1}} \end{array}$$

es lineal y recibe el nombre de traza (ver definición 2.22 y teorema 2.23 de [64]). Si $Tr(\alpha)$ representa el entero $0 \leq Tr(\alpha) < p$ tal que $Tr(\alpha) + p\mathbb{Z} = Tr_{\mathbb{F}_{q|\mathbb{F}_p}}(\alpha)$, es fácil ver que

$$\begin{array}{rcl} \psi_1 : (F, +) & \longrightarrow & (\mathbb{C}, \cdot) \\ \alpha & \longrightarrow & e^{2\pi\, i\, Tr_{\mathbb{F}_q}(\alpha)/p} \end{array}$$

es un carácter de $(\mathbb{F}_q, +)$ que recibe el nombre de carácter canónico. Para cada $\alpha \in \mathbb{F}_q$, la expresión (4.1) establece que la función ψ_α definida por $\psi_\alpha(c) = \psi_1(\alpha c)$, para todo $c \in \mathbb{F}_q$, es un carácter de $(\mathbb{F}_q, +)$. Es más, todos los caracteres aditivos de $\mathbb{F}_q$ son de esta forma (ver el teorema 5.7 de [64]), por lo que el carácter canónico ψ_1 es admisible.

Notemos también que para cualquier carácter no trivial $\psi_\alpha \in \widehat{\mathbb{F}}_q$, $\alpha \neq 0$, el conjunto $\{\beta\psi_\alpha : \beta \in \mathbb{F}_q\} = \{\beta\alpha\,\psi_1 : \alpha \in \mathbb{F}_q\} = \widehat{\mathbb{F}}_q$. Es decir, cualquier carácter aditivo no trivial de $\mathbb{F}_q$ es admisible.

Sin embargo, no todos los anillos son admisibles. El anillo de polinomios $\mathbb{F}_2[x,y]/(x^2, y^2, xy - yx)$ es conmutativo y finito, pero no es admisible (ver ejemplo 3.2 de [23]).

Sea A una R-álgebra asociativa de dimensión finita, con R un anillo finito, conmutativo y admisible. En este caso es posible encontrar una descripción de los caracteres aditivos de A a partir de los elementos del módulo dual $A^* = Hom_R(A, R)$. Esta propiedad es importante, pues permitirá parametrizar los super-caracteres en función de las órbitas de cotransición como hicimos en el capítulo 2. Comenzamos por demostrar que el grupo aditivo $(A^*, +)$ y el grupo de caracteres $\widehat{A}$ son isomorfos.

Teorema 4.1.2 *Sea R un anillo finito, conmutativo y admisible. Sea A una R-álgebra asociativa de dimensión finita y sea $A^* = Hom_R(A, R)$ su R-módulo dual. Si ψ es un carácter admisible de R, la aplicación*

$$\begin{array}{rcl} \varphi : (A^*, +) & \longrightarrow & (\widehat{A}, +) \\ f & \longrightarrow & \psi_f = \psi \circ f \end{array} \tag{4.3}$$

es un isomorfismo de grupos abelianos.

Demostración: Puesto que A es un álgebra (y en particular un anillo), el conjunto de caracteres aditivos de A, denotado por $\widehat{A}$, es un grupo abeliano. Sea $\psi \in \widehat{R}$ un carácter admisible de R y sea $f \in A^*$ un elemento cualquiera. Es claro que la aplicación $\psi_f = \psi \circ f$ es un carácter aditivo de A, es decir $\psi_f \in \widehat{A}$. Así pues, la aplicación φ está bien definida. Probaremos que es un isomorfismo de grupos:

- φ es homomorfismo. Si $f, g \in A^*$, entonces $\varphi(f+g)(a) = \psi_{f+g}(a) = \psi_f(a)\psi_g(a) = (\psi_f + \psi_g)(a)$, para todo $a \in A$. Es decir, $\varphi(f+g) = \varphi(f) + \varphi(g)$.

- φ es biyectiva. Puesto que el álgebra A es finita y $|A| = |\widehat{A}| = |A^*|$, basta probar que es inyectiva. Sea $f \in A^*$ un elemento tal que $\varphi(f) = \psi_f = 1_A$, entonces $\psi_f(a) = \psi(f(a)) = 1$, para todo $a \in A$, y por tanto $Imf \subseteq \ker\psi$. Sea $r \in Imf$ cualquiera. Puesto que Imf es un ideal de R, $rR \subseteq Imf \subseteq ker\psi$ y entonces $\psi(rs) = r\psi(s) = 1$, para todo $s \in R$. Es decir, $\phi(r) = r\psi = 1_A$, con ϕ la aplicación definida en (4.2), y $r \in ker\phi = 0$; pues ϕ es un isomorfismo de módulos por ser ψ admisible. Dado que el elemento r es arbitrario, se sigue que $Imf = 0$, esto es, $f = 0$. ■

Corolario 4.1.3 *En las condiciones del teorema anterior se sigue que el conjunto de los caracteres aditivos de A es de la forma:*

$$\widehat{A} = \{\psi_f = \psi \circ f : f \in A^*\}.$$

Hemos visto que un cuerpo finito $\mathbb{F}_q$ es un anillo admisible. Es más, cualquier carácter no trivial de $\mathbb{F}_q$ es admisible. Así pues, cualquier $\mathbb{F}_q$-álgebra de dimensión finita está en las condiciones del resultado anterior y por ello se obtiene la siguiente parametrización de $\widehat{A}$, que resuelve la aparente ambigüedad de la construcción de los caracteres irreducibles de $(J, +)$ introducida en la sección 1.2.

Corolario 4.1.4 *Sea A una $\mathbb{F}_q$-álgebra de dimensión finita y sea A^* su espacio dual. El conjunto de caracteres aditivos $\widehat{A}$ tiene la forma*

$$\widehat{A} = \{\psi_f = \psi \circ f : f \in A^*\},$$

con ψ un carácter aditivo no trivial cualquiera de A.

4.2. Anillos de Frobenius y de Galois

Hemos visto que no todos los anillos son admisibles. En esta sección caracterizaremos los anillos finitos que sí lo son y que resultan ser los anillos de Frobenius. Posteriormente, estudiaremos algunas propiedades de los anillos de Galois, que constituyen un ejemplo importante de este tipo de anillos.

Sea R un anillo artiniano. Se puede definir sobre él una estructura de R-módulo a izquierda, denotado por ${}_RR$, si se considera la acción dada por la multiplicación del anillo. Puesto que R satisface la condición de cadena descendente, este módulo se puede escribir como una suma finita de módulos indescomponibles, esto es: módulos no nulos que no se pueden expresar como suma directa de dos submódulos propios. De esta forma, el módulo ${}_RR$ se puede escribir como (ver teorema 14.2 de [24]):

$${}_RR = Re_{11} \oplus \cdots \oplus Re_{1\mu_1} \oplus \cdots \oplus Re_{n1} \oplus \cdots \oplus Re_{n\mu_n}, \tag{4.4}$$

donde los e_{ij} son idempotentes primitivos ortogonales tales que $1 = \sum e_{ij}$. A esta descomposición se le llama *descomposición principal* y a cada sumando *módulo principal indescomponible.*

Los idempotentes de (4.4) se han indexado de forma que $Re_{ij} \cong Re_{kl}$ si y sólo si $i = k$, por tanto, si denotamos $e_i = e_{i1}$, para todo i, es claro que $\{Re_1, \ldots, Re_n\}$ es un conjunto completo de módulos principales indescomponibles no isomorfos. Así, si tenemos en cuenta las multiplicidades, el módulo ${}_RR$ se puede descomponer como ${}_RR \cong \bigoplus \mu_i Re_i$.

Por otra parte, R se puede dotar, con el producto, de una estructura de módulo a derecha, denotado por R_R, que también se descompone en una suma de módulos principales indescomponibles. Entonces se verifica

$$R_R = e_{11}R \oplus \cdots \oplus e_{1\mu_1}R \oplus \cdots \oplus e_{n1}R \oplus \cdots \oplus e_{n\mu_n}R,$$

con la particularidad de que los idempotentes primitivos e_{ij} son idénticos a los de la expresión (4.4). Asimismo, las multiplicidades μ_i coinciden, puesto que para cualesquiera idempotentes primitivos e y f se verifica que $Re \cong Rf$ si y sólo si $eR \cong fR$. En consecuencia, es obvio que el módulo R_R se puede descomponer como $R_R \cong \oplus \mu_i e_i R$.

Notemos que cada módulo indescomponible Re_{ij} (respec. $e_{ij}R$) posee un único submódulo maximal Je_{ij} (respec. $e_{ij}J$), donde J es el radical de Jacobson del anillo R. El cociente Re_{ij}/Je_{ij} (respec. $e_{ij}R/e_{ij}J$) se denota por $T(Re_{ij})$ (respec. $T(e_{ij}R)$). Por último, referir que para cada módulo indescomponible, la suma de todos sus submódulos irreducibles (es decir, aquéllos que no poseen submódulos propios) recibe el nombre de *socle* y se representa por $S(Re_{ij})$ (respec. $S(e_{ij}R)$).

Una vez introducidos estos conceptos, podemos definir los anillos Frobenius y quasi-Frobenius tal como se hace en los trabajos de Nakayama (ver [80], [68] y [69]).

Definición 4.2.1 *Sea R un anillo artiniano con una descomposición principal como la de (4.4). Entonces:*

1. *R se dice quasi-Frobenius si existe una permutación $\sigma \in S_n$ tal que $T(Re_i) \cong S(Re_{\sigma(i)})$ y $S(e_iR) \cong T(e_{\sigma(i)}R)$ para todo $i = 1, \ldots, n$.*

2. *R se dice Frobenius si es quasi-Frobenius y además $\mu_{\sigma(i)} = \mu_i$ para todo $i = 1, \ldots, n$.*

3. *R se dice débilmente simétrico si $T(Re_i) \cong S(Re_i)$ y $T(e_iR) \cong S(e_iR)$ para todo $i = 1, \ldots, n$.*

Es importante mencionar que estas tres propiedades coinciden cuando R es conmutativo (ver nota 1.3 de [80] para los detalles).

Si R es un anillo finito, por el teorema 3.10 de [80] se tiene que R es Frobenius si y sólo si es admisible. Es decir, si y sólo si el módulo a izquierda ${}_RR$ es isomorfo al módulo de caracteres ${}_R\widehat{R}$ y el módulo a derecha R_R es isomorfo al módulo $\widehat{R}_R$. Si además R es conmutativo, las estructuras ${}_R\widehat{R}$ y $\widehat{R}_R$ coinciden, por lo que R es Frobenius si y sólo si $R \cong \widehat{R}$ como bimódulo. Esto es, R es Frobenius si y sólo si R posee un carácter admisible. Por tanto, podemos establecer el siguiente resultado:

Teorema 4.2.2 *Sea R un anillo finito conmutativo, entonces R posee un carácter admisible si y sólo si R es Frobenius.*

Notemos en primer lugar que no todos los anillos conmutativos finitos son Frobenius. El anillo $\mathbb{F}_2[x, y]/(x^2, y^2, xy - yx)$ del ejemplo 3.2 de [23] es conmutativo y finito, pero no es admisible. Por otra parte, un ejemplo inmediato de anillos de Frobenius lo proporcionan los cuerpos finitos, pues hemos visto en la sección anterior que cualquier carácter no trivial de $\mathbb{F}_q$ es admisible. Otro ejemplo lo constituyen los anillos de residuos $R = \mathbb{Z}/m\mathbb{Z}$. Es fácil ver que si ξ es una m-raíz primitiva compleja de la unidad, la función $\chi : R \to \mathbb{C}$ definida como $\chi(x) = \xi^x$ para todo $x \in R$ es un carácter admisible de R.

Los anillos de Galois son una generalización de los anillos de residuos. También son anillos de Frobenius y por su importancia en el desarrollo de la teoría posterior les dedicaremos el final de esta sección.

Un anillo de Galois $GR(p^n, r)$, con p primo, n, r enteros, es un anillo finito, conmutativo y local (es decir, con un único ideal maximal) cuyo cardinal es

p^{nr} y cuya característica es p^n. Este anillo es una extensión de Galois del anillo $\mathbb{Z}_{p^n}$ y es, por tanto, isomorfo al cociente $\mathbb{Z}_{p^n}[x]/(f(x))$, con $f(x) \in \mathbb{Z}_{p^n}[x]$ un polinomio mónico de grado r tal que su proyección sobre $\mathbb{F}_p[X]$ es irreducible. Se puede probar que esta construcción es única salvo isomorfismo (ver [17] y [74] para los detalles). Dos ejemplos triviales los proporcionan los casos $n = 1$ y $r = 1$. El primero es la extensión de grado r del cuerpo primo $\mathbb{F}_p$, por lo que $GR(p, r) = \mathbb{F}_{p^r}$, mientras que el segundo es el anillo $GR(p^n, 1) = \mathbb{Z}_{p^n}$.

A continuación estudiaremos cómo se pueden representar de forma explícita los elementos de un anillo de Galois $GR(p^n, r)$. Básicamente encontramos dos tipos de representaciones. El primero utiliza la estructura de $GR(p^n, r)$ como extensión de $\mathbb{Z}_{p^n}$ y será de utilidad para probar que todo anillo de Galois es de Frobenius. El segundo parte de la forma del retículo de ideales de $GR(p^n, r)$; lo utilizaremos en la última sección de este capítulo.

Sea $h_1(x) \in \mathbb{F}_p[x]$ un polinomio primitivo de grado r y consideremos el cuerpo finito $\mathbb{F}_{p^r} \cong \mathbb{F}_p[x]/(h_1(x))$. A partir de $h_1(x)$ se puede construir un único polinomio de grado r, denotado por $h_n(x) \in \mathbb{Z}_{p^n}[x]$, mónico, irreducible, congruente con $h_1(x)$ módulo (p) y que divide al polinomio $x^k - 1$, con $k = p^r - 1$, en $\mathbb{Z}_{p^n}[x]$ (ver teorema 1.4.4 de [17]). Sea ξ una raíz de $h_n(x)$, puesto que $h_n(x)$ divide a $x^k - 1$ en $\mathbb{Z}_{p^n}[x]$, se cumple que $\xi^k = 1$ y por construcción, $GR(p^n, r) \cong \mathbb{Z}_{p^n}[\xi]$. Así pues, cada elemento $z \in GR(p^n, r)$ se puede representar como un elemento de $\mathbb{Z}_{p^n}[\xi]$ de la forma siguiente:

$$z = \sum_{j=0}^{r-1} v_j \xi^j, \ v_j \in \mathbb{Z}_{p^n}.$$

Si ζ es una p^n-raíz primitiva de la unidad, es posible definir para cada $z \in GR(p^n, r)$ la función $\chi : GR(p^n, r) \to \mathbb{C}$ dada por $\chi(z) = \zeta^{v_{r-1}}$, que se prueba que es un carácter admisible de $GR(p^n, r)$ (ver ejemplo 4.4 de [80]). Esto demuestra que $GR(p^n, r)$ es un anillo de Frobenius como ya habíamos

apuntado.

Es posible encontrar otra representación de los elementos de $GR(p^n, r)$ con sólo desarrollar los coeficientes v_j y agrupar las diferentes potencias de p. Así, llegamos a la expansión p-ádica:

$$z = z_0 + pz_1 + \cdots + p^{n-1}z_{n-1},$$

con cada z_i en el conjunto $\mathcal{T}_r = \{0, 1, \xi, \ldots, \xi^{p^r-2}\}$, que recibe el nombre de conjunto coordenado de Teichmüller.

Aún podemos encontrar otra expresión más para los elementos de $GR(p^n, r)$, pero para ello debemos conocer la forma del retículo de sus ideales. Puesto que los ideales de $\mathbb{Z}_{p^n}$ forman la cadena

$$p\mathbb{Z}_{p^n} \supset p^2\mathbb{Z}_{p^n} \supset \ldots \supset p^{n-1}\mathbb{Z}_{p^n} \supset (0),$$

es fácil ver que los ideales de $GR(p^n, r)$ son todos principales. De hecho, todos ellos se pueden expresar como

$$I_k = p^k\, GR(p^n, r),\ 1 \leq k \leq n-1.$$

De esta propiedad se sigue que $p\,GR(p^n, r)$ es el único ideal maximal de $GR(p^n, r)$ y que el cuerpo residual es $GR(p^n, r)/p\,GR(p^n, r) \cong \mathbb{F}_{p^r}$. Además permite escribir los elementos de $GR(p^n, r)$ de la forma siguiente (proposición 6.2.2 de [17]).

Proposición 4.2.3 *Todo elemento no nulo $z \in GR(p^n, r)$ se puede escribir de la forma $z = up^t$, con u una unidad y $0 \leq t \leq n-1$. En esta representación, el entero t está determinado unívocamente, mientras que u es único módulo (p^{n-t}).*

Demostración: Es claro que si $z \in U(GR(p^n, r))$, entonces $t = 0$. En otro caso, puesto que el anillo es local, z es nilpotente; por ello existirá un primer entero t tal que $z \in I_t = p^t GR(p^n, r)$. En consecuencia, t es único.

Una vez probada la unicidad de t, supongamos que z posee dos representaciones diferentes, es decir, que existen elementos $u, x \in \mathbf{U}(GR(p^n, r))$ tales que $z = up^t = xp^t$. Entonces se sigue que $(x - u)p^t = 0$, por lo que $x - u \in I_{n-t}$. Así, $x = u + \lambda p^{n-t}$, para algún $\lambda \in U(GR(p^n, r))$. ■

Por último, sólo resta referir la importancia de los anillos de Galois en el estudio de los anillos conmutativos finitos, lo que justifica el desarrollo de una teoría de super-caracteres de R-grupos de álgebra cuando R es un anillo de Galois. Destaquemos que cualquier anillo conmutativo finito con identidad se puede descomponer de forma única, salvo isomorfismo, como suma directa de anillos locales (ver teorema 3.1.4 de [17]); cada uno de ellos es imagen homomorfa de un cierto anillo de polinomios cuyos coeficientes están en un anillo de Galois. De hecho, se puede probar (ver teorema 6.3.1 de [17]) el resultado siguiente.

Teorema 4.2.4 *Sea R un anillo finito, conmutativo y local. Sea p^n su característica y sea $K \cong \mathbb{F}_{p^r}$ su cuerpo residual. Entonces, existe un subanillo $T \subset R$ tal que*

1. *$T \cong GR(p^n, r)$ es el único subanillo de orden p^{nr} de R;*

2. *T es la extensión de Galois de $\mathbb{Z}_{p^n}$ maximal contenida en R;*

3. *R es imagen homomorfa de un anillo de polinomios con coeficientes en T.*

El anillo de Galois T recibe el nombre de anillo de coeficientes de R.

4.3. Super-caracteres de grupos de álgebra sobre anillos de Galois

El propósito de esta sección es extender el concepto de super-carácter a grupos de álgebra asociados a una R-álgebra A, con R un cierto anillo conmutativo, finito y con identidad.

Sea $(A, +, \cdot)$ un anillo cualquiera sobre el que se define la operación $a*b = a+b+ab$, para todo $a, b \in A$. Dotado con esta operación, A es un semigrupo cuyo elemento neutro es $0 \in A$. El conjunto de elementos inversibles de $(A, *)$ recibe el nombre de *grupo adjunto* de A, y será denotado por $G(A)$. Decimos que el anillo A es *radical* si coincide con su grupo adjunto, es decir, si $A = G(A)$. En caso que sea finito, esta condición es equivalente a la nilpotencia, esto es, A es radical si y sólo si es nilpotente.

Sea R un anillo de Galois $GR(p^n, e)$ con cuerpo residual $\mathbb{F}_q$ $(q = p^e)$. Puesto que R es un anillo de Frobenius, posee un carácter admisible que denotaremos por ψ (ver teorema 4.2.2). Sea A una R-álgebra asociativa, finitamente generada y nilpotente. Este álgebra se identifica con un cierto ideal del anillo $\mathcal{S} = R \oplus A$, mientras que el grupo adjunto $G(A)$ lo hace con el subgrupo $1 + A$ del grupo $U(\mathcal{S})$ de las unidades de $\mathcal{S}$. Diremos que el grupo adjunto $G(A) = 1 + A$ es el *grupo de álgebra* asociado a la R-álgebra A (esta definición generaliza 1.2.1 para álgebras sobre anillos de Frobenius). Un ejemplo de este tipo de construcción lo proporciona el grupo $U_n(R)$, formado por las matrices unitriangulares de orden n sobre el anillo R; en este caso $U_n(R) = 1 + \mathcal{U}_n(R)$, con $\mathcal{U}_n(R)$ la R-álgebra nilpotente de las matrices triangulares superiores de orden n con coeficientes en R.

Es fácil ver que cuando A es una $\mathbb{F}_q$-álgebra de dimensión finita, el grupo de álgebra asociado $G = 1 + J$, donde J es el radical de Jacobson de A, es

un p-grupo. Este resultado también es cierto si A es una R-álgebra en las condiciones anteriores, (ver teorema 2.1 de [11] para los detalles). Además, cualquier carácter irreducible χ del R-grupo de álgebra $G(A)$ es de la forma $\chi = \tau^G$, con τ un carácter lineal de $G(B) \leq G(A)$ y B un subanillo de A (ver teorema 2.3 y corolario 2.1 de [11]). Este resultado supone una generalización del teorema 1.2 de [33] donde se establece que cualquier carácter irreducible de un $\mathbb{F}_q$-grupo de álgebra está inducido por un carácter lineal de un subgrupo suyo.

Por otra parte, recordemos que los super-caracteres de un $\mathbb{F}_q$-grupo de álgebra $G = 1 + J$ se definen para cada elemento f del espacio dual J^* (ver definición 2.2.3) como el carácter inducido por el carácter lineal λ_f dado por:

$$\begin{aligned} \lambda_f : R(f) &\longrightarrow \mathbb{C} \\ 1 + a &\longrightarrow \psi(f(a)) \end{aligned}$$

con $R(f)$ el estabilizador de f para la acción de cotransición derecha (ver sección 2.1), y donde ψ es un carácter no trivial (y por tanto admisible) de $\mathbb{F}_q$. Cada uno de ellos depende únicamente de la órbita de cotransición que contiene al elemento $f \in J^*$, por lo que se puede establecer una aplicación biyectiva entre el conjunto $\mathrm{SCh}(G)$ de super-caracteres de G y el de órbitas de cotransición de J^*, denotado por $\mathbf{\Omega}(G)$ (ver teorema 2.2.4). Nuestro objetivo será probar este resultado para el caso en que $G = G(A)$ es un R-grupo de álgebra. Para ello, basta obtener la fórmula (2.4), en la que se expresa el super-carácter en función de la órbita de cotransición, para R-grupos de álgebra.

Puesto que el anillo R es Frobenius, por el teorema 4.1.2 sabemos que el grupo de los caracteres aditivos de $(A, +)$ se puede escribir como

$$\widehat{A} = Irr(A^+) = \{\psi_f : f \in A^*\}.$$

El grupo $G = G(A)$ actúa sobre $\widehat{A}$ mediante la operación $(x\cdot\lambda)(a) = \lambda(x^{-1}a)$, para todo $x \in G$, $a \in A$ y $\lambda \in \widehat{A}$, lo que convierte a $\widehat{A}$ en un G-módulo a izquierda. Para cada $\lambda = \psi_f \in \widehat{A}$, el conjunto

$$\mathcal{L}_\lambda = \{a \in A : \lambda(au) = 1,\ \forall u \in A\},$$

es un subgrupo aditivo de A (en realidad es un ideal derecho de A) que coincide con el conjunto $\mathcal{L}(f) = \{a \in A : f(au) = 0,\ \forall u \in A\}$ definido en el lema 2.1.2; pues si $a \in \mathcal{L}_\lambda$, entonces $1 = \lambda(au) = \psi_f(au) = \psi(f(au)) = \psi_{fa}(u)$ para todo $u \in A$, con la función fa definida por $fa(u) = f(au)$. En consecuencia, $\psi_{fa} = 1_A$ y por el teorema 4.1.2 se sigue que $fa = 0$, lo que implica $a \in \mathcal{L}(f)$. El otro contenido es trivial.

El grupo adjunto asociado, $L_\lambda = G(\mathcal{L}_\lambda)$, es el estabilizador de λ para la acción de G a izquierda y coincide con el conjunto $L(f) = 1 + \mathcal{L}(f)$ del lema 2.1.2. A su vez, podemos definir el conjunto $\mathcal{L}_\lambda^\perp \leq \widehat{A}$ como

$$\mathcal{L}_\lambda^\perp = \{\tau \in \widehat{A} : \tau(a) = 1,\ \forall a \in \mathcal{L}_\lambda\},$$

que es un R-módulo cuyo cardinal viene dado por el resultado siguiente:

Lema 4.3.1 *Sea B un subgrupo aditivo de A. Si $B^\perp$ es el conjunto $B^\perp = \{\tau \in \widehat{A} : \tau(b) = 1,\ \forall b \in B\}$, entonces $|B^\perp| = |A|/|B|$.*

Demostración: Basta considerar la aplicación

$$\begin{array}{rccc} \phi : \widehat{A} & \longrightarrow & \widehat{B} \\ f & \longrightarrow & f|_B \end{array}$$

Esta función es claramente un homomorfismo de grupos suprayectivo, pues por ser A y B abelianos, cualquier carácter de B puede ser extendido a

carácter de A (ver corolario 5.5 de [41]). Además, es fácil ver que $ker\phi = B^{\perp}$. El resultado se sigue del primer teorema de isomorfía de grupos. ■

Al igual que en la sección 2.1, denotaremos por $G\lambda$ a la órbita de λ para la acción de G por la izquierda, es decir, $G\lambda = \{x \cdot \lambda : x \in G\}$. Puesto que L_λ es el estabilizador de λ para la acción de G a izquierda, se sigue que $|G\lambda| = |G|/|L_\lambda| = |A|/|\mathcal{L}_\lambda| = |\mathcal{L}_\lambda^{\perp}|$.

Alternativamente, podemos definir para $\widehat{A}$ una estructura de G-módulo a derecha si consideramos la operación definida por $(\lambda \cdot x)(a) = \lambda(ax^{-1})$, para todo $\lambda \in \widehat{A}$, $a \in A$, $x \in G$. De forma análoga, el conjunto

$$\mathcal{R}_\lambda = \{a \in A : \lambda(ua) = 1,\ \forall u \in A\},$$

es un subgrupo aditivo de A y su grupo adjunto $G(\mathcal{R}_\lambda) = R_\lambda$ es el estabilizador de λ para la acción de G por la derecha. Por el lema 4.3.1 sabemos que $|\mathcal{R}_\lambda^{\perp}| = |A|/|\mathcal{R}_\lambda|$, y si $\lambda G = \{\lambda \cdot x : x \in G\}$ es la órbita de λ para la acción de G a derecha, es claro que $|\lambda G| = |\mathcal{R}_\lambda^{\perp}|$.

Para cada $a \in A$ y $\lambda \in \widehat{A}$, la aplicación definida por $(a\lambda)(u) = \lambda(au)$ (respec. $(\lambda a)(u) = \lambda(ua)$), para todo $u \in A$, es un elemento de $\widehat{A}$. Denotamos por $A\lambda$ (respec. λA) el conjunto $\{a\lambda : a \in A\} \leq \widehat{A}$ (respec. $\{\lambda a : a \in A\} \leq \widehat{A}$). Con esta notación, podemos probar el resultado siguiente, que es la generalización de la proposición 2.1.4 para R-grupos de álgebra.

Proposición 4.3.2 *Sea $\lambda \in \widehat{A}$ un carácter aditivo de A, entonces*

1. $|G\lambda| = |A\lambda| = |\lambda A| = |\lambda G|$;
2. $A\lambda = \mathcal{R}_\lambda^{\perp}$;
3. $\lambda A = \mathcal{L}_\lambda^{\perp}$.

Demostración: Es fácil ver que $A\lambda$ y λA son subgrupos aditivos de $\widehat{A}$ y que dado $a \in A$, $a\lambda(u) = \lambda(au) = 1$, para todo $u \in \mathcal{R}_\lambda$ (respec. $\lambda a(u) = \lambda(ua) = 1$, para todo $u \in \mathcal{L}_\lambda$) , y por tanto $A\lambda \leq \mathcal{R}_\lambda^\perp$ (respec. $\lambda A \leq \mathcal{L}_\lambda^\perp$). Puesto que $|G\lambda| = |A\lambda|$ y $|\lambda G| = |\lambda A|$, se sigue que $|A\lambda| = |\mathcal{L}_\lambda^\perp| \geq |\lambda A| = |\mathcal{R}_\lambda^\perp| \geq |A\lambda|$ y se tiene el primer resultado. Los otros dos se obtienen a partir de la finitud de A. ■

La consecuencia inmediata es el resultado que aparece a continuación y que generaliza el corolario 2.1.5.

Corolario 4.3.3 *Sea $\lambda \in \widehat{A}$ un carácter aditivo de A, entonces:*

1. $G\lambda = \lambda + \mathcal{R}_\lambda^\perp$;
2. $\lambda G = \lambda + \mathcal{L}_\lambda^\perp$;
3. $|G\lambda| = |\lambda G|$.

Denotamos por $\mathfrak{F}(\mathcal{A})$ y $\mathfrak{F}(G)$ los conjuntos de funciones complejas sobre $(A, +)$ y G respectivamente. Notemos que ambos son $\mathbb{C}$-espacios unitarios con el producto de Frobenius (ver definición 1.1.10). A cada función $\varphi \in \mathfrak{F}(\mathcal{A})$ se le puede asociar una función $\widetilde{\varphi} \in \mathfrak{F}(G)$, definida por $\widetilde{\varphi}(1 + a) = \varphi(a)$ para todo $a \in A$, de forma que la aplicación $\varphi \mapsto \widetilde{\varphi}$ es un isomorfismo de espacios vectoriales que satisface $\langle \varphi, \psi \rangle_A = \langle \widetilde{\varphi}, \widetilde{\psi} \rangle_G$. Por otra parte, las acciones de G sobre $\widehat{A}$ se pueden extender al conjunto $\mathfrak{F}(\mathcal{A})$, con lo que éste adquiere una estructura de G-bimódulo. En estas condiciones, decimos que una función $\varphi \in \mathfrak{F}(\mathcal{A})$ es *invariante a izquierda* (respec. *invariante a derecha*) si $\varphi(xa) = \varphi(a)$ (respec. $\varphi(ax) = \varphi(a)$), para todo $x \in G$ y $a \in A$.

Para cada elemento $\lambda \in \widehat{A} \subseteq \mathfrak{F}(\mathcal{A})$, las funciones α_λ y β_λ definidas como

$$\alpha_\lambda = \frac{1}{|G\lambda|} \sum_{\mu \in G\lambda} \mu, \quad \beta_\lambda = \frac{1}{|\lambda G|} \sum_{\mu \in \lambda G} \mu.$$

son claramente invariantes a izquierda y derecha respectivamente. Es más, podemos probar el siguiente resultado.

Proposición 4.3.4 *El conjunto* $\{\alpha_\lambda : \lambda \in \widehat{A}\}$ *(respec.* $\{\beta_\lambda : \lambda \in \widehat{A}\}$*) es una base ortogonal, con respecto al producto de Frobenius, del espacio* $\mathfrak{L}(A)$ *(respec.* $\mathfrak{R}(A)$*) de todas las funciones de* $\mathfrak{F}(\mathcal{A})$ *invariantes a izquierda(respec. a derecha).*

Demostración: En primer lugar, es fácil ver que si $\delta \notin G\lambda$, entonces $\langle \alpha_\lambda, \alpha_\delta \rangle = 0$, mientras que $\langle \alpha_\lambda, \alpha_\lambda \rangle = 1/|G\lambda|$, por lo que el conjunto $\{\alpha_\lambda : \lambda \in \widehat{A}\}$ es un sistema de funciones ortogonales y por tanto, es libre.

Notemos que cada elemento $\varphi \in \mathfrak{L}(A)$ es constante sobre las G-órbitas a izquierda de A. Por ello, la dimensión del espacio $\mathfrak{L}(A)$ es igual al cardinal de este conjunto, que denotamos por $\Omega_G(A)$, es decir, $\dim_{\mathbb{C}}\mathfrak{L}(A) = |\Omega_G(A)|$. Puesto que $|\{\alpha_\lambda : \lambda \in \widehat{A}\}| = |\Omega_G(\widehat{A})|$, donde $\Omega_G(\widehat{A})$ es el conjunto de G-órbitas a izquierda de $\widehat{A}$, bastará probar que $|\Omega_G(A)| = |\Omega_G(\widehat{A})|$. Para ello, consideramos ϑ el carácter de la acción permutación de G sobre A. Por el corolario 5.15 de [41], se tiene que $|\Omega_G(A)| = \langle \vartheta, 1_G \rangle$. Además, por definición, $\vartheta(x) = |C_A(x)|$, con $C_A(x) = \{a \in A : xa = a\}$. Por otra parte, se cumple que $(x\lambda)(xa) = \lambda(x^{-1}(xa)) = \lambda(a)$, para todo $x \in G$, $\lambda \in \widehat{A}$ y $a \in A$ y del teorema de Brauer (teorema 6.32 de [41]) se sigue que $\vartheta(x) = |C_{\widehat{A}}|$, para todo $x \in G$, con $C_{\widehat{A}} = \{\lambda \in \widehat{A} : x \cdot \lambda = \lambda\}$. Por tanto, ϑ es también el carácter de la acción permutación de G sobre $\widehat{A}$ y entonces $\langle \vartheta, 1_G \rangle = |\Omega_G(\widehat{A})|$. La demostración es idéntica para la otra acción. ■

Proposición 4.3.5 *Sea* $\lambda \in \widehat{A}$ *cualquiera. Si* $\lambda_{\mathcal{R}_\lambda}$ *(respec.* $\lambda_{\mathcal{L}_\lambda}$*) es la restricción de* λ *al conjunto* $\mathcal{R}_\lambda$ *(respec.* $\mathcal{L}_\lambda$*), entonces* $\alpha_\lambda = |G\lambda|^{-1}(\lambda_{\mathcal{R}_\lambda})^A$ *y* $\beta_\lambda = |\lambda G|^{-1}(\lambda_{\mathcal{L}_\lambda})^A$.

Demostración: Puesto que $G\lambda = \lambda + \mathcal{R}_\lambda^\perp$, de la definición de α_λ se sigue que

$$|G\lambda|\alpha_\lambda = \sum_{\mu \in G\lambda} \mu = \lambda \sum_{\nu \in \mathcal{R}_\lambda^\perp} \nu.$$

Por otra parte, es fácil ver que por la reciprocidad de Frobenius (proposición 1.1.15), para cada $\nu \in \mathcal{R}_\lambda^\perp$ se verifica

$$\langle \nu, (1_{\mathcal{R}_\lambda})^A \rangle_A = \langle \nu, 1_{\mathcal{R}_\lambda} \rangle_{\mathcal{R}_\lambda} = \frac{1}{|\mathcal{R}_\lambda|} \sum_{x \in \mathcal{R}_\lambda} \nu(x) = 1.$$

Además,

$$\sum_{\nu \in \mathcal{R}_\lambda^\perp} \nu(1) = |\mathcal{R}_\lambda^\perp| = |A : \mathcal{R}_\lambda| = (1_{\mathcal{R}_\lambda})^A(1),$$

y por tanto, $(1_{\mathcal{R}_\lambda})^A = \sum_{\nu \in \mathcal{R}_\lambda^\perp} \nu$. Así pues,

$$|G\lambda|\alpha_\lambda = \lambda(1_{\mathcal{R}_\lambda})^A = (\lambda_{\mathcal{R}_\lambda})^A.$$

La demostración para β_λ es análoga. ■

Decimos que una función $\varphi \in \mathfrak{F}(\mathcal{A})$ es *bi-invariante* si $\varphi(xay) = \varphi(a)$ para todo $x, y \in G$ y todo $a \in A$. Denotaremos por $\mathfrak{B}(A)$ el subespacio vectorial formado por todas las funciones bi-invariantes. Notemos que $\mathfrak{B}(A) = \mathfrak{L}(A) \cap \mathfrak{R}(A)$. Asimismo, para cada $\lambda \in \widehat{A}$ se verifica que $x \cdot (\lambda \cdot y) = (x \cdot \lambda) \cdot y$, por lo que podemos definir el carácter $x\lambda y = x \cdot (\lambda \cdot y) = (x \cdot \lambda) \cdot y$. Sea $G\lambda G = \{x\lambda y : x, y \in G\}$, definimos la función $\gamma_\lambda \in \mathfrak{F}(\mathcal{A})$ como

$$\gamma_\lambda = \frac{1}{|G\lambda G|} \sum_{\mu \in G\lambda G} \mu.$$

Proposición 4.3.6 *El conjunto* $\{\gamma_\lambda : \lambda \in \widehat{A}\}$ *es una base ortogonal, con respecto al producto de Frobenius, del espacio* $\mathfrak{B}(A)$ *de todas las funciones bi-invariantes de* $\mathfrak{F}(\mathcal{A})$.

Demostración: Es claro que $\gamma_\lambda \in \mathfrak{B}(A)$ para todo $\lambda \in \widehat{A}$. A su vez, si $\delta \notin G\lambda G$, es fácil ver que $\langle \gamma_\delta, \gamma_\lambda \rangle = 0$, por lo que el conjunto $\{\gamma_\lambda : \lambda \in \widehat{A}\}$ es un sistema de funciones ortogonales y por tanto, es libre. Consideramos las acciones del grupo $G \times G$ sobre A y $\widehat{A}$ dadas respectivamente por $(x, y) \cdot a = xay^{-1}$ y $(x, y) \cdot \lambda = x\lambda y^{-1}$, para todo $a \in A$, $\lambda \in \widehat{A}$. Denotamos por $\Omega_{G\times G}(A)$ (respec. $\Omega_{G\times G}(\widehat{A})$) al conjunto de todas las órbitas para la acción de $G \times G$ sobre A (respec. sobre $\widehat{A}$). Puesto que las funciones bi-invariantes son constantes en las órbitas de $G \times G$ sobre A, se sigue que $\dim_{\mathbb{C}} \mathfrak{B}(A) = |\Omega_{G\times G}(A)|$. Por tanto, es suficiente probar que $|\{\gamma_\lambda : \lambda \in \widehat{A}\}| = |\Omega_{G\times G}(A)|$. Para ello seguimos un razonamiento análogo al de la proposición 4.3.4, pues $(x, y) \cdot \lambda((x, y) \cdot a) = \lambda(a)$ para todo $(x, y) \in G \times G$, $\lambda \in \widehat{A}$, $a \in A$, con lo que se puede aplicar el teorema de Brauer (teorema 6.3 de [41]). ■

El resultado siguiente pone de manifiesto la relación entre las funciones invariantes a derecha, a izquierda y bi-invariantes, y es clave en la generalización del teorema 2.2.4 a R-grupos de álgebra.

Teorema 4.3.7 *Sea $\lambda \in \widehat{A}$ un elemento cualquiera, entonces:*

1. *$\tilde{\lambda}_{L_\lambda}$ (respec. $\tilde{\lambda}_{R_\lambda}$) es un carácter lineal de L_λ (respec. de R_λ),*

2. *$|G\lambda|\tilde{\gamma}_\lambda = (\tilde{\lambda}_{L_\lambda})^G = (\tilde{\lambda}_{R_\lambda})^G$.*

Demostración: Basta considerar la acción a izquierda, puesto que para la otra la demostración es similar. Dados $a, b \in \mathcal{L}_\lambda$, tenemos que $\lambda(ab) = 1$, por tanto, $\tilde{\lambda}((1 + a)(1 + b)) = \lambda(a + b + ab) = \lambda(a)\lambda(b)\lambda(ab) = \lambda(a)\lambda(b) = \tilde{\lambda}(1 + a)\tilde{\lambda}(1 + b)$. Así pues, $\tilde{\lambda}_{L_\lambda}$ es un carácter lineal.

Dado $a \in A$ cualquiera, por la definición de carácter inducido (ver definición 5.1 de [41]) se tiene que

$$(\tilde{\lambda}_{L_\lambda})^G(1+a) = \frac{1}{|L_\lambda|}\sum_{x\in G}\nu_\lambda(xax^{-1}),$$

donde ν_λ se define como $\nu_\lambda(u) = \lambda(u)$ si $u \in \mathcal{L}_\lambda$ y $\nu_\lambda = 0$, en otro caso. Se sigue entonces que $\nu_\lambda = |A : \mathcal{L}_\lambda|^{-1}(\lambda_{\mathcal{L}_\lambda})^A = \alpha_\lambda$, y así

$$\begin{aligned}\alpha_\lambda(xax^{-1}) &= \frac{1}{|G\lambda|}\sum_{\mu\in G\lambda}\mu(xax^{-1}) = \frac{1}{|G\lambda|}\sum_{\mu\in G\lambda}(x^{-1}\mu x)(a)\\ &= \frac{1}{|G\lambda||L_\lambda|}\sum_{z\in G}(x^{-1}z\lambda x)(a) = \frac{1}{|G|}\sum_{y\in G}(y\lambda x)(a),\end{aligned}$$

para todo $x \in G$. Por tanto,

$$(\tilde{\lambda}_{L_\lambda})^G(1+a) = \frac{1}{|L_\lambda||G|}\sum_{x,y\in G}(y\lambda x)(a) = \frac{|G\lambda|}{|G\lambda G|}\sum_{\mu\in G\lambda G}\mu(a) = |G\lambda|\tilde{\gamma}_\lambda(1+a),$$

lo que nos lleva al resultado. ■

Como sucede con los $\mathbb{F}_q$-grupos de álgebra, podemos definir el super-carácter asociado a un elemento $\lambda \in \widehat{A}$ como sigue:

Definición 4.3.8 *Sea $\lambda \in \widehat{A}$ un carácter aditivo de A. El super-carácter de $G(A)$ asociado a λ es el carácter*

$$\xi_\lambda = (\tilde{\lambda}_{L_\lambda})^G = (\tilde{\lambda}_{R_\lambda})^G.$$

El resultado siguiente generaliza el teorema 2.2.4 y prueba que para un R-grupo de álgebra el super-carácter asociado a $\lambda \in \widehat{A}$ depende sólo de la órbita $G\lambda G$.

Corolario 4.3.9 *Sea $\lambda \in \widehat{A}$ un carácter aditivo de A. Entonces, el super-carácter asociado a λ es de la forma*

$$\xi_\lambda(1+a) = \frac{|G\lambda|}{|G\lambda G|}\sum_{\mu\in G\lambda G}\mu(a), \quad \textit{para todo } a \in A. \tag{4.5}$$

Notemos que la expresión (4.5) es idéntica a (2.2), obtenida para $\mathbb{F}_q$-grupos de álgebra. Así pues, hemos probado que cuando R es un anillo de Galois, las propiedades de los super-caracteres son independientes de que A sea un $\mathbb{F}_q$-espacio vectorial o una R-álgebra finita. Esto es debido a que los super-caracteres dependen únicamente de la acción del grupo G sobre el G-bimódulo $\widehat{A}$, que para estos dos casos resulta tener las mismas propiedades.

4.4. Un ejemplo: La R-álgebra de polinomios en una indeterminada

En esta sección, al igual que en la 2.5, estudiaremos un ejemplo sencillo. Sea R el anillo de Galois $GR(p^n, e)$ y sea $A = R_0[x]/(x^m)$ la R-álgebra de los polinomios con término independiente cero, coeficientes en R y grado estrictamente menor que m. Es claro que A es un álgebra finita, nilpotente con grado de nilpotencia m y libre. Por otra parte, notemos que debido a la nilpotencia de A, el grupo adjunto $G(A)$ coincide con el subgrupo $1+A$ de las unidades de A. Además, A tiene rango $m-1$ y el conjunto $\mathcal{B} = \{x, \ldots, x^{m-1}\}$ es una R-base suya. El R-módulo dual $A^* = Hom_R(A, R)$ también es libre de rango $m-1$ y tiene como base el conjunto $\mathcal{B}^* = \{x^*, \ldots, (x^{m-1})^*\}$, donde $(x^i)^*(x^j) = \delta_{ij}$, para todo $1 \leq i, j \leq m-1$.

De acuerdo con la sección anterior, los super-caracteres de $G(A)$ están en correspondencia biyectiva con las órbitas de la acción de G sobre A^*, que por analogía con la sección 2.1, llamaremos acción de cotransición. A pesar de que $G(A)$ es conmutativo, y por ello la acción de cotransición izquierda coincide con la acción de cotransición derecha, el hecho de que R posea divisores de cero hace que el estudio de las órbitas sea mucho más difícil que para el caso del $\mathbb{F}_q$-grupo de álgebra visto. Por este motivo, estudiaremos únicamente las

órbitas asociadas a los monomios $c_s(x^s)^*$, con $c_s \in R$ y $1 \leq s \leq m-1$.

Lema 4.4.1 *Sea $(x^s)^* \in \mathcal{B}^*$ un elemento de la base dual. Si $x^i \in \mathcal{B}$, entonces*

$$x^i(x^s)^* = \begin{cases} (x^{s-i})^* & \text{si } i < s; \\ 0 & \text{en otro caso.} \end{cases}$$

Demostración: Puesto que $x^i(x^s)^*(a) = (x^s)^*(x^i a)$, para todo $a \in A$, tenemos que $x^i(x^s)^*(x^j) = (x^s)^*(x^{i+j}) = \delta_{s,i+j}$, para todo $x^j \in \mathcal{B}$. Así pues, si $i < s$, es claro que $x^i(x^s)^*(x^j) = 1$ si y sólo si $j = s-i$, mientras que es cero en cualquier otro caso. Por tanto, $x^i(x^s)^* = (x^{s-i})^*$. De igual forma, $x^i(x^s)^* = 0$ para todo $i \geq s$. ■

Supongamos que c_s es una unidad del anillo R. En ese caso obtenemos un resultado idéntico al de la proposición 2.5.1.

Proposición 4.4.2 *Sea $(x^s)^* \in \mathcal{B}^*$ un elemento de la base dual. Entonces, si c_s es una unidad del anillo R, la órbita de cotransición del elemento $c_s(x^s)^* \in A^*$ viene dada por*

$$G(c_s(x^s)^*) = c_s(x^s)^* + \langle (x)^*, \ldots, (x^{s-1})^* \rangle_R$$

Demostración: Como consecuencia del lema anterior, para cada elemento $c_s(x^s)^*$, con $1 \leq s \leq m-1$, la órbita $G(c_s(x^s)^*)$ está contenida en el conjunto $c_s(x^s)^* + \langle (x)^*, \ldots, (x^{s-1})^* \rangle_R$. Supongamos que c_s es una unidad de R y veamos que se da la igualdad. Sea $a \in c_s(x^s)^* + \langle (x)^*, \ldots, (x^{s-1})^* \rangle_R$ un elemento cualquiera, entonces existen elementos $a_i \in R$ para $1 \leq i \leq s-1$ tales que $a = c_s(x^s)^* + \sum_{i=1}^{s-1} a_i(x^i)^*$. Pretendemos encontrar un elemento $1 + \sum_{i=1}^{m-1} f_i x^i = 1 + f(x) \in G$ tal que $(1 + f(x))c_s(x^s)^* = a$. Puesto que $x^i(c_s(x^s)^*) = 0$ para todo $i \geq s$ podemos suponer, sin pérdida de generalidad, que $f(x)$ es un polinomio de grado $s-1$, con lo que $f_i = 0$,

para todo $s \leq i \leq m-1$. Por hipótesis, $c_s \in U(R)$; por tanto, el resto de coeficientes es de la forma $f_{s-i} = c_s^{-1}a_i$, con $1 \leq i \leq s-1$. Así pues, $c_s(x^s)^* + \langle (x)^*, \ldots, (x^{s-1})^* \rangle \subseteq G(c_s(x^s)^*)$ y el resultado se sigue. ■

Proposición 4.4.3 *En las condiciones del resultado anterior, el estabilizador del elemento $c_s(x^s)^*$ para la acción de cotransición G es*

$$L_{c_s(x^s)^*} = R_{c_s(x^s)^*} = 1 + \langle x^s, \ldots, x^{m-1} \rangle_R$$

Demostración: En primer lugar, puesto que las acciones de G a derecha e izquierda coinciden, tenemos que $\mathcal{L}(c_s(x^s)^*) = \mathcal{R}(c_s(x^s)^*)$. Además, es fácil ver que

$$\langle x^s, \ldots, x^{m-1} \rangle_R \subseteq \mathcal{L}(c_s(x^s)^*). \tag{4.6}$$

Así pues, sólo resta probar el otro contenido. Sea $a \in A$ un elemento que satisface $ac_s(x^s)^* = 0$. Por la condición (4.6) es suficiente considerar $a = \sum_{i=1}^{s-1} a_i x^i$. Para cada $1 \leq i \leq s-1$, el coeficiente a_{s-i} debe verificar $a_{s-i}c_s = 0$. Puesto que $c_s \in U(R)$, $a_i = 0$ y el resultado se sigue. ■

Notemos que en este caso hemos repetido el resultado obtenido en la sección 2.5. Esto se debe a que el R-módulo $\mathcal{L}(c_s(x^s)^*)$ es un sumando directo de A, que es libre. Entonces, puesto que R es un anillo local, $\mathcal{L}(c_s(x^s)^*)$ es libre y complementado en A (ver [67]) y cualquier R-base suya se puede extender a una R-base de A, tal como sucede con los $\mathbb{F}_q$-espacios vectoriales.

Supongamos que c_s no es una unidad de R. Por la proposición 4.2.3 sabemos que $c_s = up^k$, con $u \in U(R)$ y $1 \leq k \leq n-1$. El entero k está unívocamente determinado, mientras que la unidad es única módulo p^{n-k}.

Proposición 4.4.4 *Sea $(x^s)^* \in \mathcal{B}^*$ un elemento de la base dual. Entonces, si $c_s = up^k$ con $u \in U(R)$ y $1 \leq k \leq n-1$, la órbita del elemento $c_s(x^s)^*$ tiene la forma*

$$G(c_s(x^s)^*) = c_s(x^s)^* + \langle p^k x^*, \ldots, p^k(x^{s-1})^* \rangle_R$$

Demostración: A partir del lema 4.4.1 es claro que $G(c_s(x^s)^*) \subseteq c_s(x^s)^* + \langle c_s x^*, \ldots, c_s(x^{s-1})^* \rangle_R$, puesto que $c_s = up^k$ con $u \in U(R)$, se sigue que $\langle c_s x^*, \ldots, c_s(x^s)^* \rangle_R = \langle p^k x^*, \ldots, p^k(x^{s-1})^* \rangle_R$. Por lo tanto, tenemos que

$$G(c_s(x^s)^*) \subseteq c_s(x^s)^* + \langle p^k x^*, \ldots, p^k(x^{s-1})^* \rangle_R$$

Sea $a \in c_s(x^s)^* + \langle p^k x^*, \ldots, p^k(x^{s-1})^* \rangle_R$ un elemento cualquiera, entonces podemos encontrar elementos $a_i \in R$ tales que $a = c_s(x^s)^* + \sum_{i=1}^{s-1} a_i p^k (x^i)^*$. Se dará el contenido si es posible encontrar un elemento $1 + \sum_{i=1}^{m-1} f_i x^i = 1 + f(x) \in G$, de forma que $(1 + f(x))c_s(x^s)^* = a$. Podemos suponer, sin pérdida de generalidad, que el polinomio $f(x)$ tiene grado $s-1$. Para cada $1 \leq i \leq s-1$, el coeficiente f_{s-i} debe satisfacer $f_{s-i} up^k = a_i p^k$, que se verifica siempre que $f_{s-i} u \cong a_i \, mod(p^{n-k}R)$. Puesto que $u \in U(R)$, basta tomar $f_{s-i} \cong u^{-1} a_i \, mod(p^{n-k}R)$ y el resultado se sigue. ■

La forma del estabilizador $L(c_s(x^s)^*)$, cuando $c_s \notin U(R)$, es diferente de la obtenida para $\mathbb{F}_q$-grupos de álgebra. Esta diferencia se debe a que $\mathcal{L}(c_s(x^s)^*)$ no es necesariamente un R-módulo complementado de A.

Proposición 4.4.5 *En las condiciones de la proposición anterior, el estabilizador del elemento $c_s(x^s)^*$ es el grupo*

$$R(c_s(x^s)^*) = L(c_s(x^s)^*) = 1 + \langle p^{n-k}x, \ldots, p^{n-k}x^{s-1}, x^s, \ldots, x^{m-1} \rangle_R$$

Demostración: Puesto que la acción de G es conmutativa, $\mathcal{R}(c_s(x^s)^*) = \mathcal{L}(c_s(x^s)^*)$. Además, es fácil ver que

$$\langle p^{n-k}x, \ldots, p^{n-k}x^{s-1}, x^s, \ldots, x^{m-1}\rangle_R \subseteq \mathcal{L}(c_s(x^s)^*).$$

Sólo resta probar el otro contenido. Para ello, tomamos un elemento $a \in A$ tal que $ac_s(x^s)^* = 0$. Puesto que A es un R-módulo libre con base $\mathcal{B}$, $a = \sum_{i=1}^{m-1} a_i x^i$, con $a_i \in R$ para todo i. Bastará ver que $a_i \in p^{n-k}R$ para todo $1 \leq i \leq s-1$. Dado uno cualquiera de estos coeficientes, la condición $ac_s(x^s)^* = 0$ implica que $a_{s-i}up^k = 0$. Puesto que $u \in U(R)$, se sigue que $a_i \in p^{n-k}R$. ■

Por otra parte, mientras que para los monomios $c_s(x^s)^*$ con $c_s \in U(R)$ las órbitas $G(c_s(x^s)^*)$ son todas diferentes, no ocurre lo mismo cuando $c_s = up^k$ con $u \in U(R)$. En ese caso, hemos visto en la proposición 4.2.3 que dos elementos $c_s = up^k$ y $c'_s = u'p^k$, con $u, u' \in U(R)$, son diferentes si y sólo si $u \ncong u' \, mod(p^{n-k}R)$. Así pues, podremos demostrar el siguiente resultado:

Proposición 4.4.6 *Sea $(x^s)^* \in \mathcal{B}^*$ un elemento de la base dual. Entonces, el conjunto de todas las órbitas de la forma $G(c_s(x^s)^*)$ se puede escribir como la unión disjunta de los conjuntos siguientes:*

1. $\{G(c_s(x^s)^*) : c_s \in U(R)\}$;
2. $\{G(up^k(x^s)^*) : \pi_k(u) \in I_k,\ 1 \leq k \leq n-1\}$, *donde $\pi_k : R \to R/p^{n-k}R$ es la proyección canónica e I_k es un conjunto completo de representantes de las unidades del anillo $R/p^{n-k}R$.*

Demostración: Sea $c_s = up^k$ con $u \in U(R)$ y $0 \leq k \leq n-1$ y sea $c_t = u_1p^l$ con $u_1 \in U(R)$ y $t \leq s$. Las órbitas $G(c_s(x^s)^*) = c_s(x^s)^* + p^k\langle x^*, \ldots, (x^{s-1})^*\rangle_R$ y $G(c_t(x^t)^*) = c_t(x^t)^* + p^l\langle x^*, \ldots, (x^{t-1})^*\rangle_R$ coinciden si y sólo si $c_s(x^s)^* -$

$c_t(x^t)^* \in M + N$, con $M = p^k\langle x^*, \ldots, (x^{s-1})^*\rangle_R$ y $N = p^l\langle x^*, \ldots, (x^{t-1})^*\rangle_R$. Es fácil ver que esta condición se verifica si y sólo si $s = t$ y $c_s = c_t$.

En el caso en que $c_s \in U(R)$, su representación es única; por ello todas las órbitas $G(c_s(x^s)^*)$ con $c_s \in U(R)$ son diferentes. Esto da lugar a la primera familia de órbitas.

Supongamos ahora que $c_s = up^k$ con $u \in U(R)$. Según acabamos de ver, c_s no tiene una representación única, sino que $c_s = u'p^k$ para todo $u' \cong u \, mod(p^{n-k}R)$. Si $\pi_k : R \to R/p^{n-k}R$ es la proyección canónica, se verifica que $c_s = up^k \neq c'_s = u'p^k$ si y sólo si $\pi_k(u) \neq \pi_k(u')$. Puesto que $\pi_k(U(R)) = U(\pi_k(R))$, podemos ver que sólo las órbitas de la forma $G(up^k(x^s)^*)$ con $\pi_k(u) \in U(R/p^{n-k})$ son diferentes. Esto da lugar a la segunda familia. ■

Como se puede apreciar, en todos los casos es posible escribir las órbitas $G(c_s(x^s)^*)$ como $c_s(x^s)^* + N$, con N un R-módulo. Cuando $c_s \in U(R)$, el módulo N es libre y complementado, con lo que se repite el comportamiento estudiado en la sección 2.5. Por el contrario, si $c_s = up^k$, con $k \in U(R)$, el módulo $N = p^kN'$ con N' libre y complementado. En este caso no se recupera, en general, el comportamiento de los $\mathbb{F}_q$-grupos de álgebra.

Otra particularidad es que mientras que en la sección 2.5 sólo aparecían órbitas de la forma $f_s(x^s)^* + V$ con $f_s \neq 0$ (observemos que f_s es una unidad de $\mathbb{F}_q$), en este caso tenemos una variedad mayor. Así, junto con aquellas de la forma $G(c_s(x^s)^*)$ con $c_s \notin U(R)$, aparecen también otras que no contienen ningún elemento de $\mathcal{B}$. Como ejemplo, puede servir el R-álgebra $A = R_0[x]/(x^3)$ con $R = G(3^2, 2)$. En ese caso, tendremos $|U(R)| = 72$ unidades, lo que supone que en las órbitas de la forma $G(c_s(x^s)^*)$ con $c_s \in U(R)$ se repartan $|U(R)|\sum_{s=1}^{2}(3^2)^{s-1} = 5904$ elementos. Por otra parte, las órbitas del tipo $G(up^k)$ con $u \in U(R)$ y $k = 1, 2$ suman un total de $\sum_{s=1}^{2}(3^2 - 1)(3^2)^{s-1} = 80$ elementos. La suma total es de 5984 elementos,

menor que $(3^4)^2 - 1 = 6560$ que es el número total de elementos no nulos de A.

Por último, sólo resta dar una expresión para los super-caracteres de $G = 1 + A$ asociados a este tipo de órbitas. Es el resultado siguiente:

Teorema 4.4.7 *Sea $(x^s)^* \in \mathcal{B}$ un elemento de la base dual y sea $c_s \in R$ un elemento no nulo cualquiera. Entonces, el super-carácter asociado a $c_s(x^s)^*$ es de la forma:*

1. $\xi_{c_s(x^s)^*} = \tilde{\lambda}_{c_s(x^s)^*} \prod_{i=1}^{s-1} \left(\sum_{c \in R} \tilde{\lambda}_{c(x^i)^*} \right)$ *si* $c_s \in U(R)$;
2. $\xi_{c_s(x^s)^*} = \tilde{\lambda}_{c_s(x^s)^*} \prod_{i=1}^{s-1} \left(\sum_{c \in p^k R} \tilde{\lambda}_{c(x^i)^*} \right)$ *si* $c_s = up^k$;
3. 1_G *si* $c_s = 0$.

Demostración: La demostración es igual que la del corolario 2.5.4. Partimos de la expresión (4.5) para el super-carácter $\xi_{c_s(x^s)^*}$. Puesto que la acción de G es conmutativa, tenemos que

$$\xi_{c_s(x^s)^*}(1 + a) = \sum_{\mu \in G(c_s(x^s)^*)} \mu(a),$$

para todo $a \in A$. Las proposiciones 4.4.2 y 4.4.4 permiten escribir $G(c_s(x^s)^*)$ de la forma $c_s(x^s)^* + M$, lo que tras desarrollar nos permite llegar al resultado deseado. ■

Capítulo 5

Aplicaciones: Teoría de caracteres y códigos cuánticos

En este capítulo abordaremos una de las aplicaciones de la Teoría de Representaciones: el tratamiento de los errores en los códigos cuánticos.

Los errores cuánticos pueden escribirse en términos de una base de operadores de error. En principio, existen diferentes elecciones para esta base, pero una de las más útiles se obtiene considerando una representación proyectiva de un cierto grupo H llamado. *grupo de error* Las bases de error así obtenidas reciben el nombre de *nice error bases* (ver [51]). Alternativamente, esta representación proyectiva se puede ver como una representación ordinaria de una cierta extensión central de E que recibe el nombre de *grupo abstracto de error*.

A pesar de que la naturaleza de los errores cuánticos difiere de la de los clásicos y de que existen errores cuánticos sin equivalencia clásica, el formalismo de las bases y grupos de error permite la construcción de códigos correctores cuánticos en un contexto similar al de los códigos clásicos, a la vez que aportan herramientas para el análisis del error.

Un ejemplo de estos códigos cuánticos son los códigos estabilizadores, descritos en [52], que se definen como el subespacio vectorial estabilizado por el conjunto de matrices $\{\rho(n) : n \in N\}$, donde ρ es una representación fiel y unitaria del grupo de error G y $N \trianglelefteq G$ es un subgrupo normal abeliano.

A lo largo del capítulo estudiaremos los códigos Clifford (ver [53]), una generalización de los códigos estabilizadores en los que el subgrupo N no es necesariamente abeliano, y relacionaremos sus propiedades con las de los caracteres que utilizamos para su definición. De hecho, podremos probar que las propiedades correctivas de estos de códigos vienen condicionadas por la existencia de caracteres completamente ramificados.

Por último, terminaremos el capítulo con la construcción de códigos sobre el producto directo de grupos abstractos de error, de forma similar a como se hace en el caso clásico, y estudiaremos sus propiedades correctoras.

5.1. Representaciones proyectivas y bases de error

A lo largo de este capítulo trabajaremos con sistemas cuánticos. Cada uno de ellos se puede identificar con un espacio de Hilbert que es un producto tensorial de la forma $\mathcal{H} = \mathcal{S}^{\otimes m}$, donde cada $\mathcal{S} \cong \mathbb{C}^q$ representa un sistema elemental con q estados. En el caso $q = 2$, el sistema $\mathcal{S}$ recibe el nombre de qubit. Un código cuántico Q es un subespacio vectorial del sistema $\mathcal{H}$. De forma más precisa podemos decir (definición 3 de [14]):

Definición 5.1.1 *Un código cuántico q-ario de longitud m y tamaño k es un subespacio vectorial $Q \subseteq \mathcal{H}$ de dimensión k. Para $q = 2$ el código se dice binario.*

La información cuántica es susceptible de sufrir errores, como por ejemplo cuando se produce entrelazamiento entre el sistema y el entorno, procesos de decoherencia, etc. Un error se representa en este modelo como un operador lineal que actúa sobre el espacio $\mathcal{H}$. Igual que en el caso clásico, es posible construir códigos que protejan la información frente a un conjunto de errores determinado.

En primer lugar, debemos distinguir qué errores pueden ser detectados por el código y cuáles se pueden corregir. Un operador de error E se dice detectable por el código Q (ver [56]) si para cada estado $x \in Q$ se verifica que, o bien $Ex = x$, o bien $Ex \notin Q$. Por otra parte, si $\mathcal{E} = \{E_0 = Id, E_1, \ldots, E_s\}$ es un conjunto de operadores de error, decimos que $\mathcal{E}$ es corregible por el código Q si y sólo si para todo par de estados $x, y \in Q$ con $x \neq y$ y para todo i, j se verifica que $E_i x \neq E_j y$. Notemos que el concepto de detectabilidad afecta únicamente a cada error de forma individual, mientras que el otro concepto depende del conjunto de operadores de error. Además, en caso de que todos los operadores de error sean inversibles, se puede probar que el conjunto $\mathcal{E}$ es corregible si y sólo si los errores $E_j^{-1} E_i$ son detectables para todo i, j.

También es conocido el hecho de que si Q corrige el conjunto de errores $\mathcal{E}$, también corrige todos los que se encuentran en su clausura lineal. De esta forma, es suficiente trabajar con un conjunto $\mathcal{E}$ que sea una base del espacio vectorial de todos los operadores de error que actúan sobre $\mathcal{H}^{\otimes m}$. Estos conjuntos reciben el nombre de bases de error. Un ejemplo lo proporciona, para un sistema formado por un único qubit ($\mathcal{H} = \mathcal{S} \cong \mathbb{C}^2$), el conjunto de

matrices siguiente (matrices de Pauli):

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad N = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

$$S = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad NS = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

Notemos que el conjunto $\mathcal{E} = \{I, N, S, NS\}$ es un grupo para la multiplicación de matrices y que éstas son ortogonales respecto al producto escalar $\langle A, B\rangle = tr(A^t\, B)$. Cualquier código capaz de corregir los errores de $\mathcal{E}$ será capaz de corregir cualquier error que afecte al qubit $\mathcal{H}$. Este modelo se puede extender a sistemas con m qubits con sólo definir cada operador de error como un producto tensorial de m operadores elementales.

De entre las posibles elecciones de bases de error, estudiaremos las que se conocen como *nice error bases* (ver [51]), que son una generalización del ejemplo anterior y que se definen como representaciones proyectivas de un *grupo de error*.

Definición 5.1.2 *Sea H un grupo de orden n^2. Una nice error basis sobre $\mathcal{H} \cong \mathbb{C}^n$ es un conjunto $\mathcal{E} = \{\rho(g) \in \mathcal{U}(n) : g \in H\}$ tal que:*

1. $\rho(1) = I_n$,
2. $tr(\rho(g)) = n\,\delta_{g,1}$, *para todo* $g \in H$,
3. $\rho(g)\rho(h) = \omega(g,h)\,\rho(gh)$, *para todo* $g, h \in H$.

Observemos que todas las matrices $\rho(g)$ son unitarias y por tanto, no singulares. En consecuencia, la aplicación $\omega : H \times H \to \mathbb{C}$ toma valores no nulos y está determinada unívocamente por ρ. De las condiciones 1 y 3 se

sigue que ρ es una *representación proyectiva* del grupo H con *conjunto factor* ω (ver definición 1.11 de [41]).

Por otra parte, a partir de la condición 2 se deduce que $ker\,\rho = \{g \in H : \rho(g) = cI,\, c \in \mathbb{C}\} = \{1\}$, por lo que ρ es fiel. Además, es fácil ver que las matrices $\rho(g)$ son ortogonales dos a dos con respecto al producto escalar de $\mathcal{U}(n)$ dado por $\langle A, B\rangle = tr(A^\dagger B)/n$. Por ello, el conjunto $\{\rho(g) : g \in H\}$ es una base de la $\mathbb{C}$-álgebra $\mathcal{M}_n(\mathbb{C})$ y ρ es una representación proyectiva irreducible.

Por último, podemos suponer sin pérdida de generalidad (ver [58]) que $det(\rho(g)) = 1$ para todo $g \in H$, por lo que en ese todos los elementos de ω son raíces de la unidad. Un grupo H que satisface estas propiedades recibe el nombre de *grupo índice* de la base de error $\mathcal{E}$.

Así pues, hemos probado que las nice error bases se obtienen de representaciones proyectivas de su grupo índice. El recíproco también es cierto, por lo que se tiene la siguiente caracterización (teorema 1 de [51]).

Teorema 5.1.3 *Sea $\mathcal{E} = \{\rho(g) : g \in H\}$ un conjunto de matrices unitarias parametrizadas por los elementos de un grupo finito H. El conjunto $\mathcal{E}$ es una nice error basis con grupo índice H si y sólo si ρ es una representación proyectiva, irreducible y fiel de H con grado $|H|^{1/2}$.*

Demostración: Ya hemos visto que si $\mathcal{E}$ es una nice error basis con grupo índice E, entonces ρ es una representación proyectiva, fiel e irreducible de grado $|H|^{1/2}$. Recíprocamente, si ρ es una representación proyectiva, irreducible y fiel de H, se verifican trivialmente las condiciones 1 y 3 de la definición 5.1.2. Además, si ϕ es el carácter asociado a ρ, el núcleo $ker\,\rho = \{g \in H : \rho(g) = cI,\, c \in \mathbb{C}\} = \{1\}$ se identifica con el quasi-núcleo $Z(\phi) = \{g \in H : |\phi(g)| = \phi(1)\}$ (ver definición 2.26 y lema 2.27 de [41]). Por

último, puesto que $\phi^2(1) = |H|$, se sigue que $\phi(g) = 0$ para todo $g \in H - \{1\}$ (ver corolario 2.30 de [41]), lo que da la condición 2 de 5.1.2. ■

En lugar de trabajar con grupos índice, es más práctico hacerlo con una extensión central suya que recibe el nombre de *grupo abstracto de error*. Comenzamos por introducir la siguiente definición (definición 11.8 de [41]).

Definición 5.1.4 *Una extensión central de H es un un par formado por un grupo G (posiblemente infinito) y por un epimorfismo $\pi : G \to H$ tal que $ker\,\pi \subseteq Z(G)$.*

Existe una relación entre las representaciones proyectivas de un grupo E y las representaciones ordinarias de sus extensiones centrales. Para comprenderla es necesario introducir el siguiente concepto (definición 11.11 de [41]).

Definición 5.1.5 *Sea (G, π) una extensión central de H y sea ρ una $\mathbb{C}$-representación **proyectiva** de H. Diremos que ρ se puede elevar a G si existen una representación **ordinaria** η de G y una función $\mu : G \to \mathbb{C}^*$ tal que para todo $g \in G$ se tiene*

$$\eta(g) = \rho(\pi(g))\mu(g).$$

Definición 5.1.6 *Sea H un grupo de error. Un grupo abstracto de error G es la extensión central de menor grado de H tal que cualquier representación proyectiva de H se puede elevar a G.*

Por el teorema 11.17 de [41], todo grupo finito H posee una extensión central finita G con la propiedad anterior. En consecuencia, si H es un grupo de error finito, el grupo abstracto de error también lo es. La construcción de esta extensión central, llamada grupo de representación de Schur de H, se puede ver en [51].

Definición 5.1.7 *Un grupo G es de tipo central si existe un carácter* ***ordinario*** $\phi \in Irr(G)$ *tal que* $\phi(1) = |G : Z(G)|^{1/2}$.

Los grupos abstractos de error son un caso especial de grupos tipo central. De hecho, podemos probar la siguiente caracterización (teorema 3 de [51]).

Teorema 5.1.8 *Un grupo finito G es un grupo abstracto de error si y sólo si G es un grupo de tipo central cuyo centro es cíclico.*

Demostración: Supongamos que G es un grupo abstracto de error. En ese caso, G es una extensión central del grupo de error H y existe una representación proyectiva de H, denotada por ρ, irreducible y fiel de grado $|H|^{1/2}$. Si ω es el conjunto factor asociado a ρ, el conjunto de valores de ω genera un subgrupo cíclico T del grupo multiplicativo de $\mathbb{C}$ y G es isomorfo al grupo $(T \times H, \cdot)$ (ver capítulo 11 de [41] y sección 3 de [51]), donde la operación $\cdot$ se define como

$$(a, h) \cdot (b, k) = (ab\,\omega(h, k), hk), \quad a, b \in T,\ h, k \in H$$

Por tanto, $H \cong G/T$ con T cíclico contenido en $Z(G)$. A su vez, la representación proyectiva ρ se puede elevar a una representación ordinaria e irreducible de G con el mismo grado que ρ. Sea ϕ el carácter de esta representación, entonces $\phi(1)^2 = |G : T|$ y se sigue, por el corolario 2.30 de [41], que $T = Z(G)$, por lo que G es de tipo central.

Recíprocamente, supongamos que G es un grupo de tipo central cuyo centro es cíclico. A partir del lema 4.3 de [37] se puede suponer, sin pérdida de generalidad, que el grupo G posee una representación η ordinaria, unitaria y fiel de grado $|G : Z(G)|^{1/2}$. Sea $H = G/Z(G)$, denotamos por $W = \{x_g : g \in H\}$ un sistema completo de representantes de G módulo $Z(G)$. La aplicación $\eta : H \to \mathcal{U}_n$ dada por $\eta(g) = \eta(x_g)$, para todo $g \in H$,

es una representación proyectiva de H que además es irreducible y fiel. Por el teorema 5.1.3, el conjunto $\mathcal{E} = \{\eta(g) : g \in G\}$ es una nice error basis cuyo grupo índice es H. En estas condiciones (ver capítulo 11 de [41]), G es el grupo de representación de Schur de H y por tanto, es un grupo abstracto de error. ■

Nota 5.1.9 *Tal como se puede ver en [37], todos los grupos de tipo central son resolubles.*

5.2. Códigos cuánticos: códigos estabilizadores y Clifford

El ejemplo más común de códigos cuánticos son los códigos estabilizadores binarios (ver definición 5.1.1), pues desempeñan en la teoría de codificación cuántica un papel semejante al de los lineales en la clásica. Sus algoritmos de codificación son sencillos y pueden estudiarse utilizando la teoría clásica. De hecho, los primeros ejemplos de códigos cuánticos, proporcionados por Shor [77] y Steane [79], son de este tipo. La teoría general fue introducida por Gottesman [31] y Calderbank [20], quien también estudió la relación entre éstos y los códigos clásicos autoduales [21]. Los códigos estabilizadores cuánticos no binarios (ver [14]) son una extensión en la que el sistema elemental posee $m > 2$ estados. Al igual que sucede con los binarios, se pueden relacionar con los códigos clásicos sobre $\mathbb{Z}_m$ a través de las "nice error bases" (ver [57], [58] y [71]).

De forma general, un código estabilizador cuántico, binario o no, se puede definir a partir de un grupo abstracto de error G como se muestra a continuación (ver [52]).

Definición 5.2.1 *Sea G un grupo abstracto de error y sea $\rho : G \to \mathcal{U}(n)$ una representación ordinaria, irreducible y fiel de G de grado $|G : Z(G)|^{1/2}$. Si N un subgrupo normal de G, un código estabilizador Q es el subespacio generado por todos los vectores de $\mathbb{C}^{q^m}$ que son simultáneamente vectores propios de todas las matrices $\rho(n)$, con $n \in N$. Es decir:*

$$Q = \{v \in \mathbb{C}^{q^m} : \rho(n)v = \xi(n)v,\, \xi(n) \in \mathbb{C},\, \forall n \in N\}.$$

Si el código Q es no trivial, el subgrupo $N \trianglelefteq G$ es necesariamente abeliano y la aplicación $\xi : N \to \mathbb{C}$ es un carácter lineal de N. Alternativamente, Q se puede ver como la imagen del proyector ortogonal (ver [14], [55]):

$$P = \frac{1}{|N|} \sum_{n \in N} \overline{\xi(n)} \rho(n). \tag{5.1}$$

Con esta notación es posible probar (ver [58] para los detalles) que un operador de error E es detectable por el código Q si y sólo si $PEP = c_E P$, con c_E una constante que sólo depende de E.

Los códigos estabilizadores son un caso particular de códigos Clifford. De hecho, éstos se pueden definir como la imagen de un proyector ortogonal semejante a (5.1). Para estudiarlos necesitamos algunos resultados de la teoría de Clifford que, por completitud, introducimos a continuación (ver capítulos 6 de [41] y 7 de [24]).

Sea N un subgrupo normal de G y sea $\chi \in Irr(N)$ un carácter irreducible. Dado $g \in G$, la aplicación $\chi^g : N \to \mathbb{C}$ definida como $\chi^g(n) = \chi(gng^{-1})$, para todo $n \in N$, es un carácter irreducible de N denominado *carácter conjugado* de χ. Es fácil ver que el grupo G actúa por conjugación sobre el conjunto $Irr(N)$ de los caracteres irreducibles de N. El estabilizador de $\chi \in Irr(N)$ para esta acción recibe el nombre de *subgrupo de inercia* de χ y se denota como:

$$T(\chi) = \{g \in G : \chi^g = \chi\}.$$

El teorema de Clifford (ver teorema 6.2 de [41]) establece que la restricción de un carácter $\phi \in Irr(G)$ al subgrupo N se puede escribir como una suma de caracteres conjugados, todos ellos con la misma multiplicidad. Es decir, $\phi_N = e\sum_{i=1}^{t} \chi_i$, con $\chi_1 = \chi \in Irr(N)$ y $e = \langle \phi, \chi \rangle_N \neq 0$. De la definición de subgrupo de inercia se desprende que $t = |G : T(\chi)|$.

Supongamos que V es el $\mathbb{C}G$-módulo irreducible asociado al carácter $\phi \in Irr(G)$. Es claro que V tiene también una estructura de $\mathbb{C}N$-módulo, denotada por V_N, cuando restringimos la acción al subgrupo $N \trianglelefteq G$. Si W es un $\mathbb{C}N$-submódulo irreducible cualquiera de V_N, resulta que V_N se puede escribir como una suma de $\mathbb{C}N$-módulos conjugados de la forma $W_i = g_i W$ con $g_i \in G$ (ver teorema 6.5 de [41]). Sea $\{g_1 W, \ldots, g_t W\}$ un conjunto maximal de $\mathbb{C}N$-submódulos no isomorfos. En ese caso, es posible escribir $V_N = \sum_{i=1}^{t} V_i$, donde cada V_i es la suma de todos los submódulos isomorfos a $g_i W$. Los $\mathbb{C}N$-módulos V_i, para $1 \leq i \leq t$, están unívocamente determinados, salvo isomorfismo, y reciben el nombre de *componentes homogéneas* de V_N.

Definición 5.2.2 *Sea G un grupo abstracto de error y $N \trianglelefteq G$. Sea ρ una representación unitaria y fiel de G con carácter ϕ y grado $|G : Z(G)|^{1/2}$. Si V es el $\mathbb{C}G$-módulo asociado a ϕ, un código Clifford es una cualquiera de las componentes homogéneas del $\mathbb{C}N$-módulo V_N.*

Así pues, un código Clifford Q se puede escribir como una suma de $\mathbb{C}N$-módulos isomorfos: $Q \cong W \oplus \cdots \oplus W$. El número de sumandos es el mismo para cada componente homogénea y se denota por e. Por el teorema de Clifford, $e = \langle \phi, \chi \rangle_N$, con $\chi \in Irr(N)$ el carácter asociado al módulo W. Las propiedades correctoras del código vienen determinadas por el subgrupo de

inercia $T(\chi)$, que se identifica con el subgrupo $T(W) = \{g \in G : gW \cong W\}$ y que claramente actúa sobre Q, y por el conjunto

$$Z(W) = \{g \in T(W) : \exists \lambda \in \mathbb{C},\, gv = \lambda v,\, \forall v \in Q\},$$

formado por los elementos de G que actúan sobre Q como escalares. De forma más precisa podemos probar el siguiente resultado (teorema 1 de [52]).

Teorema 5.2.3 *Sea Q un código Clifford en las condiciones anteriores. Entonces*

1. $P_\chi = \dfrac{\chi(1)}{|N|} \displaystyle\sum_{n \in N} \overline{\chi(n)} \rho(n)$ *es un proyector ortogonal sobre Q.*
2. *El código Q es capaz de corregir un conjunto de errores $\Sigma \subset G$ si y sólo si $g_1^{-1} g_2 \notin T(W) - Z(W)$ para todo $g_1, g_2 \in \Sigma$.*
3. *La dimensión de Q es $e\chi(1)$.*

Demostración: La representación ρ de G es fiel, por tanto, el grupo generado por el conjunto de matrices $\{\rho(n) : n \in N\}$ es necesariamente isomorfo a N. Puesto que $\chi \in Irr(N)$, se sigue que P_χ es un idempotente del álgebra de grupo $\mathbb{C}[\rho(N)] \cong \mathbb{C}N$. Debido a que las matrices $\rho(n)$ son unitarias, P_χ es autoadjunto, y por tanto, un proyector ortogonal sobre Q (ver teorema 8 de [76]). En cuanto a la dimensión, el módulo W tiene dimensión $\chi(1)$, así pues $dim(Q) = e\chi(1)$.

Sean $g_i, g_j \in G$ dos elementos tales que $g_i g_j^{-1} \notin T(W)$. Los caracteres $\chi_i = \chi^{g_i}$ y $\chi_j = \chi^{g_j}$, asociados a los $\mathbb{C}N$-módulos $g_i W$ y $g_j W$ respectivamente, son necesariamente ortogonales. Por tanto, los proyectores asociados P_{χ_i} y P_{χ_j} satisfacen $P_{\chi_i} P_{\chi_j} = P_{\chi_j} P_{\chi_i} = 0$. Es decir, proyectan en subespacios ortogonales.

Se puede probar (ver [57] para los detalles) que un error ω es detectable por Q si y sólo si $P_\chi \omega P_\chi$ es un múltiplo escalar de P_χ. Por otra parte, el código Q es capaz de corregir todos los errores de un conjunto Σ si y sólo si es capaz de detectar todos los errores del conjunto $\{g_1^{-1} g_2 : g_1, g_2 \in \Sigma\}$ (ver [59]). Así pues, para probar el punto 2 es suficiente ver que un error ω es detectable si y sólo si $\omega \notin T(W) - Z(W)$. Para ello distinguimos tres casos:

a) El error $\omega \in Z(W)$. Entonces ω es detectable, pues por definición existe un escalar $\lambda \in \mathbb{C}$ tal que $P_\chi \rho(\omega) P_\chi = \lambda P_\chi$.

b) El error $\omega \in G - T(W)$. Entonces también es detectable, pues por el razonamiento del párrafo anterior se tiene que $P_\chi \rho(\omega) P_\chi = 0$.

c) El error $\omega \in T(W) - Z(W)$. En este caso no puede detectarse, puesto que aunque la imagen $\rho(\omega)Q \subseteq Q$ (nótese que $\omega \in T(W)$), sin embargo $P_\chi \rho(\omega) P_\chi$ no puede ser un múltiplo de P_χ, pues en ese caso ω sería un elemento de $Z(W)$. ■

Puesto que las propiedades correctoras del código dependen de los subgrupos $T(W)$ y $Z(W)$, es práctico asociar cada uno de ellos a un carácter relacionado con Q. Como hemos dicho, el conjunto $T(W)$ coincide con el subgrupo de inercia $T = T(\chi)$ y veremos a continuación que se puede encontrar un carácter $\theta \in Irr(T)$ de forma que el subgrupo $Z(W)$ coincide con el quasi-núcleo de θ, que por la definición 2.26 de [41] es el conjunto

$$Z(\theta) = \{g \in T : |\theta(g)| = \theta(1)\}.$$

Proposición 5.2.4 *Sea G un grupo abstracto de error y sea $N \trianglelefteq G$. Sea ρ una representación unitaria y fiel de G con carácter ϕ y grado $|G : Z(G)|^{1/2}$. Si $Q \cong W \oplus \cdots \oplus W$ un código Clifford, con W un $\mathbb{C}N$-módulo irreducible cuyo*

carácter asociado es χ, existe un único carácter $\theta \in Irr(T)$, con $T = T(\chi)$, tal que $Z(W) = Z(\theta)$.

Demostración: Sean los conjuntos

$$\mathbf{A} = \{\eta \in Irr(T) : \langle \eta, \chi \rangle_N \neq 0\}, \quad \mathbf{B} = \{\psi \in Irr(G) : \langle \psi, \chi \rangle_N \neq 0\}.$$

Puesto que el carácter $\phi \in Irr(G)$ es un elemento de $\mathbf{B}$, por el teorema 6.11 de [41] existe un único carácter $\theta \in \mathbf{A}$ tal que $\phi = \theta^G$. Además, θ es la única componente irreducible de la restricción ϕ_T que satisface $\langle \theta, \chi \rangle_N \neq 0$.

Es claro que Q es un $\mathbb{C}T$-módulo, pues para todo $g \in T$ se verifica $gW \cong W$. Es más, la acción de G sobre el conjunto de todos los $\mathbb{C}N$-módulos conjugados $\{gW : g \in G\}$ es transitiva, por lo que Q no puede contener $\mathbb{C}T$-módulos propios, es decir, Q es un $\mathbb{C}T$-módulo irreducible. A su vez, si V es el $\mathbb{C}G$-módulo asociado a ϕ y V_T su restricción a T, entonces $Q \leq V_T$ como $\mathbb{C}T$-módulo, y el carácter asociado a Q debe ser un elemento de $\mathbf{A}$. Por otra parte, $W \leq Q$ como $\mathbb{C}N$-módulo, por lo que el carácter asociado al $\mathbb{C}T$-módulo Q debe estar entre las componentes irreducibles de ϕ_T. Como ya hemos referido antes, el único carácter en esas condiciones es θ y por ello, el quasi-núcleo $Z(\theta)$, formado por todos los elementos de T que actúan sobre Q como escalares, se identifica con el subgrupo $Z(W)$. ■

Así pues, un código Clifford Q viene determinado por los siguientes parámetros: un grupo abstracto de error G, una representación ρ de G, unitaria, fiel, con carácter ϕ y grado $|G : Z(G)|^{1/2}$, un subgrupo normal N y una componente irreducible $\chi \in Irr(N)$ de la restricción ϕ_N. En adelante, nos referiremos a los códigos Clifford por estos cuatro parámetros y diremos que (G, ρ, N, χ) son los datos de Q.

Otra cuestión importante es decidir cuándo un código Clifford Q con datos (G, ρ, N, χ) es o no estabilizador. Si el subgrupo $N \trianglelefteq G$ es abeliano,

el carácter χ es lineal y el proyector P_χ coincide con el de la ecuación (5.1), con lo que claramente Q es estabilizador. Sin embargo, esta condición no es necesaria, pues un código Q con N no abeliano podría definirse de forma equivalente sobre otro subgrupo $A \trianglelefteq G$ que sí lo es. Dedicaremos el resto de la sección a resolver este problema.

Dado Q un código Clifford con datos (G, ρ, N, χ), denotamos por $\mathcal{A}$ el conjunto de todos los subgrupos normales abelianos de G que están contenidos en $Z(\theta)$, es decir $\mathcal{A} = \{A \leq Z(\theta) : A \trianglelefteq G, A \text{ abeliano}\}$. Para cada $A \in \mathcal{A}$, sea $\xi : A \to \mathbb{C}$ la aplicación definida por $\rho(a) = \xi(a)Id$ para todo $a \in A$. Notemos que ξ coincide con la restricción $\phi|_A$ y por tanto, es un carácter de A. Así pues, la imagen del proyector ortogonal

$$P_A = \frac{1}{|A|} \sum_{a \in A} \overline{\xi(a)} \rho(a),$$

es un código estabilizador (ver definición 5.2.1) que contiene, por el lema 1 de [53], el código Clifford Q. Por el teorema 3 de [53], Q es estabilizador si y sólo si coincide con la imagen de alguno de estos proyectores. Puesto que el carácter ϕ satisface $\phi(g) = 0$ para todo $g \in G - Z(G)$, la condición anterior es equivalente a que $dim\, Q = Tr(P_A) = |A \cap Z(G)|\phi(1)/|A|$ para algún $A \in \mathcal{A}$.

Por otra parte, cualquier código Clifford Q con datos (G, ρ, N, χ) se puede definir de forma equivalente sobre el grupo normal $N_Z = NZ(G)$ (ver lema 4 de [53]). En la práctica, esto se traduce en que para cualquier código de datos (G, ρ, N, χ) se puede asumir que $Z(G) \leq N$. Hecha esta consideración, podemos probar el siguiente resultado (corolario 6 de [53]) que proporciona una caracterización de los códigos Clifford que son estabilizadores.

Teorema 5.2.5 *Sea Q un código Clifford con datos (G, ρ, N, χ). Supongamos, sin pérdida de generalidad, que $Z(G) \leq N$. Entonces, si $\mathcal{A} = \{A \leq Z(\theta) :$*

$A \trianglelefteq G$, A *abeliano*$\}$, *el código* Q *es estabilizador si y sólo si* $\chi^2(1) = |N|/|A|$ *para algún* $A \in \mathcal{A}$ *con* $Z(G) \leq A$.

Demostración: Por una parte, $dim\, Q = Tr(P_\chi) = \chi^2(1)\phi(1)|Z(G)|/|N|$ (ver teorema 5.2.3); por la otra $Tr(P_A) = \phi(1)|Z(G)|/|A|$, pues la imagen de P_A es un código estabilizador (por tanto, Clifford) con datos (G, ρ, A, ξ) y podemos suponer que $Z(G) \leq A$ para cada $A \in \mathcal{A}$. Entonces, $dim\, Q = Tr(P_A)$ para algún $A \in \mathcal{A}$ si y sólo si $\chi^2(1) = |N|/|A|$. ■

5.3. Grupos de tipo central y caracteres completamente ramificados

Según el teorema 5.2.5, un código Clifford Q con datos (G, ρ, N, χ) es estabilizador si y sólo si existe un subgrupo normal abeliano A que satisface $\chi^2(1) = |N|/|A|$. En esta sección probaremos que esta condición es equivalente a que el carácter χ sea completamente ramificado sobre A. Esta propiedad afecta tanto a la forma de χ como al quasi-núcleo $Z(\theta)$, lo que supone una nueva caracterización, más operativa que la del teorema 5.2.5. Comenzamos por introducir la definición de carácter completamente ramificado (definición 4.1 de [37]), que es clave en el desarrollo posterior.

Definición 5.3.1 *Sea* G *un grupo y sea* $N \trianglelefteq G$. *Un carácter* $\chi \in Irr(N)$, *se dice completamente ramificado en* G *si* $\chi^G = e\psi$, *para algún* $\psi \in Irr(G)$ *y* $e = |G : N|^{1/2}$. *Por otra parte, diremos que un carácter* $\psi \in Irr(G)$ *es completamente ramificado sobre* N *si su restricción* $\psi_N = e\chi$, *para algún* $\chi \in Irr(N)$ *y* $e = |G : N|^{1/2}$.

Un ejemplo de carácter completamente ramificado lo proporciona el carácter ϕ de grado $|G : Z(G)|^{1/2}$ de un grupo de tipo central (ver definición

5.1.7), pues si $\xi \in Irr(Z(G))$ es una componente irreducible de la restricción $\phi_{Z(G)}$, se verifica que $\phi_{Z(G)} = e\xi$ con $e = |G : Z(G)|^{1/2}$ (ver teorema 6.2 de [41]). En consecuencia, un grupo es de tipo central si y sólo si posee un carácter completamente ramificado sobre su centro.

A continuación, resumimos las principales propiedades de los caracteres completamente ramificados (proposición 4.2 de [37]).

Proposición 5.3.2 *Sea G un grupo y sea $N \trianglelefteq G$. Si $\chi \in Irr(N)$ y $\phi \in Irr(G)$ tal que $\langle \phi, \chi \rangle_N \neq 0$, entonces son equivalentes:*

1. *χ es completamente ramificado en G,*
2. *ϕ es completamente ramificado sobre N,*
3. *χ es invariante en G y χ^G es un múltiplo de ϕ,*
4. *ϕ se anula en $G - N$ y la restricción ϕ_N es un múltiplo de χ,*
5. *χ es invariante y $\phi(1) = |G : N|^{1/2}$,*
6. *ϕ se anula en $G - N$ y $\phi(1) = |G : N|^{1/2}$.*

Demostración: Basta aplicar la reciprocidad de Frobenius (proposición 1.1.15), el teorema de Clifford (teorema 6.2 de [41]) y el lema 2.29 de [41]. ■

Dado un código Clifford Q con datos (G, ρ, N, χ), notemos que la condición que ha de satisfacer el carácter χ para que Q sea estabilizador es semejante a la del punto 6 de la proposición anterior. Sin embargo, $A \leq Z(\theta)$ y θ es un carácter irreducible de $T(\chi)$, pero A puede no estar contenido en N. Por ello, tiene sentido probar los resultados siguientes.

Lema 5.3.3 (lema 4.6 de [37]) *Sea G un grupo y sea $\xi \in Irr(Z(G))$ un carácter completamente ramificado en G. Supongamos que $Z(G) \leq N \trianglelefteq G$*

y que $\chi \in Irr(N)$ *es un carácter tal que* $\langle \chi, \xi \rangle_{Z(G)} \neq 0$. *Entonces* χ *es totalmente ramificado en* $T(\chi)$.

Demostración: Puesto que $\langle \chi, \xi \rangle_N \neq 0$, de la reciprocidad de Frobenius (proposición 1.1.15) se sigue que χ es un constituyente de ξ^N y por tanto, χ^G lo es de ξ^G. El carácter ξ es completamente ramificado en G, por lo que ξ^G sólo tiene una componente irreducible, lo mismo que χ^G. La inducción define una biyección entre los conjuntos $\{\psi \in Irr(T(\chi)) : \langle \psi, \chi \rangle_N \neq 0\}$, y $\{\phi \in Irr(G) : \langle \phi, \chi \rangle_N \neq 0\}$ (ver teorema 6.11 de [41]). En consecuencia, $\chi^{T(\chi)}$ posee una única componente irreducible y por la proposición 5.3.2, (3) $\Rightarrow$ (1), es completamente ramificado en $T(\chi)$. ■

Proposición 5.3.4 *Sea* Q *un código Clifford con datos* (G, ρ, N, χ). *El carácter* χ *es completamente ramificado en* $T(\chi)$.

Demostración: Como hemos visto antes, podemos asumir sin pérdida de generalidad que $Z(G) \leq N$. El carácter $\phi \in Irr(G)$, asociado a la representación ρ, es completamente ramificado sobre $Z(G)$, pues G es de tipo central. Así pues, existe un carácter $\xi \in Irr(Z(G))$ tal que $\phi_{Z(G)} = e\,\xi$ con $e = |G : Z(G)|^{1/2}$. Es fácil ver que el subgrupo de inercia $T(\xi) = G$, por lo que el carácter ξ es invariante. Así pues, por el punto 5 de la proposición 5.3.2, ξ es completamente ramificado en G. Por otra parte, ϕ es completamente ramificado sobre $Z(G)$ y se anula en $N - Z(G)$, por tanto, podemos escribir

$$\begin{aligned}\langle \phi, \chi \rangle_N &= \frac{1}{|N|} \sum_{n \in N} \chi(n)\overline{\phi(n)} = \frac{1}{|N|} \sum_{n \in Z(G)} \chi(n)\overline{\phi(n)} \\ &= \frac{1}{|N|} \sum_{n \in Z(G)} \chi(n)\, e\, \overline{\xi(n)} = \frac{e|Z(G)|}{|N|} \langle \chi, \xi \rangle_{Z(G)}.\end{aligned}$$

Por la definición del código Q, el carácter χ es una componente irreducible de la restricción ϕ_N y en consecuencia, $\langle \chi, \xi \rangle_{Z(G)} \neq 0$. Así pues, χ verifica las hipótesis del lema 5.3.3 y el resultado se sigue. ■

Este resultado tiene consecuencias inmediatas sobre el quasi-núcleo $Z(\theta)$ y por tanto, sobre las propiedades correctoras de Q.

Corolario 5.3.5 *Sea Q un código Clifford con datos (G, ρ, N, χ), entonces $Z(\theta) = Z(\chi)$ y $ker\theta = ker\chi$.*

Demostración: Por el resultado anterior, el carácter χ es completamente ramificado en $T(\chi)$. Puesto que $N \trianglelefteq T(\chi)$ y $\langle \theta, \chi \rangle_N \neq 0$ (ver proposición 5.2.4), el carácter θ es completamente ramificado sobre N (punto 2 de 5.3.2), de donde se sigue que θ se anula en $T(\chi) - N$ y además $\theta_N = e\,\chi$ (punto 4 de 5.3.2). Por ello,

$$Z(\theta) = \{g \in N : |\theta(g)| = \theta(1)\} = \{g \in N : |e\chi(g)| = e\chi(1)\} = Z(\chi).$$

De forma análoga se prueba que $ker\theta = ker\chi$. ■

Ahora es posible afirmar que cualquier subgrupo $A \in \mathcal{A} = \{A \leq Z(\theta) : A \trianglelefteq G,\ A \text{ abeliano}\}$ está contenido en N, pues $\chi \in Irr(N)$ y por el resultado anterior, $A \leq Z(\theta) = Z(\chi) \leq N$. De esta forma, podemos reformular el teorema 5.2.5 como sigue.

Teorema 5.3.6 *Sea Q un código Clifford con datos (G, ρ, N, χ). Supongamos, sin pérdida de generalidad, que $Z(G) \leq N$. Entonces, si $\mathcal{A} = \{A \leq Z(\theta) : A \trianglelefteq G,\ A \text{ abeliano}\}$, Q es un código estabilizador si y sólo si χ es un carácter completamente ramificado sobre algún $A \in \mathcal{A}$ que contiene a $Z(G)$.*

Demostración: Supongamos que Q es un código estabilizador. Entonces, por el teorema 5.2.5 y el corolario 5.3.5, existe un subgrupo normal abeliano

$A \leq Z(\chi) \leq N$ tal que $\chi^2(1) = |N : A|$ y $Z(G) \leq A$. Del lema 2.27 de [41] se sigue que la restricción $\chi_A = \chi(1)\,\xi$, con ξ un carácter lineal de A, por tanto $\langle \chi, \chi \rangle_A = |N : A|$. Así pues, se tiene que

$$|N| = |A|\langle \chi, \chi \rangle_A = \sum_{a \in A} |\chi(a)|^2 \leq \sum_{n \in N} |\chi(n)|^2 = |N|\langle \chi, \chi \rangle_N = |N|,$$

y en consecuencia $\chi(g) = 0$ para todo $g \in N - A$. Por el punto 6 de la proposición 5.3.2 el carácter χ es completamente ramificado sobre A.

Recíprocamente, supongamos que χ es un carácter de N completamente ramificado sobre A, con $A \in \mathcal{A}$ conteniendo a $Z(G)$. En ese caso, del punto 6 de la proposición 5.3.2 se sigue que χ se anula en $N - A$ y que $\chi^2(1) = |N : A|$. Por el teorema 5.2.5, Q es un código estabilizador. ■

Aún podemos mejorar este resultado si observamos que la condición $\chi^2(1) = |N : A|$ sólo se puede satisfacer si $A = Z(\chi)$; pues si $\chi^2(1) = |N : A|$ con $A < Z(\chi)$, se tiene que $\chi(g) = 0$ para todo $g \in Z(\chi) - A \neq \emptyset$, lo que constituye una contradicción. Hemos demostrado la siguiente caracterización:

Corolario 5.3.7 *Sea Q un código Clifford con datos (G, ρ, N, χ). Entonces Q es un código estabilizador si y sólo si χ es un carácter completamente ramificado sobre $Z(\chi)$ y $Z(\chi)$ es un subgrupo normal abeliano de G.*

5.4. Códigos Clifford producto

En esta sección construiremos códigos Clifford sobre el producto directo de varios grupos abstractos de error de forma similar a como se hace con los códigos clásicos. Terminaremos con el estudio de sus propiedades correctoras, para ello nos apoyaremos en conceptos propios de la teoría clásica de códigos. Por este motivo introducimos varias definiciones clásicas que serán de utilidad (ver [30]).

Sea A un conjunto cualquiera, un código-bloque C de longitud n sobre el alfabeto A es un subconjunto no vacío de A^n. Por tanto, C está formado por secuencias (palabras) de la forma $a = a_1 \cdots a_k \cdots a_n$ de longitud n y componentes $a_k \in A$, para todo k. Dadas dos palabras a y a' de C, su *distancia de Hamming*, $d_H(a, a')$, es el número de componentes en las que difieren. Es decir, $d_H(a, a') = |\{k : a_k \neq a'_k\}|$. En el caso en que $|C| \geq 2$, definimos la *distancia mínima de Hamming* del código C, $d_H(C)$, como

$$d_H(C) = min\{d_H(a, a') : a, a' \in C,\, a \neq a'\},$$

que es un entero comprendido entre 1 y la longitud del código, n.

El alfabeto A sobre el que se construye el código-bloque puede ser cualquier conjunto, sin embargo es útil que posea alguna estructura. Éste es el caso, por ejemplo, de los códigos-grupo que definimos a continuación.

Definición 5.4.1 *Sea C un código-bloque sobre un alfabeto G que es un grupo. Decimos que C es un código-grupo si es un subgrupo del producto directo G^n. Si C es normal en G^n, el código-grupo se dice normal.*

Supongamos que C es un código-grupo de longitud n y $a = a_1 \cdots a_n \in C$ una palabra. El *peso de Hamming* de a, $\omega_H(a)$, se define como el número de componentes de a que son diferentes de uno, esto es, $\omega_H(a) = |\{k : a_k \neq 1\}|$. En cualquier código-grupo siempre está contenida la palabra $e = 1 \cdots 1$, por lo que el peso de Hamming $\omega_H(a)$ coincide con la distancia de Hamming $d_H(a, e)$. Por tanto, el *peso mínimo de Hamming* del código C, que se define como $min\{\omega_H(a) : a \in C,\, a \neq 1 \cdots 1\}$, coincide con la distancia mínima de Hamming $d_H(C)$.

La distancia de Hamming de un código-grupo es un indicador de los errores que pueden ser detectados y corregidos por él. Así pues, si la distancia

mínima de Hamming $d_H(C) = d$, el código C es capaz de detectar todos aquellos errores cuyo peso de Hamming es estrictamente menor que d, mientras que puede corregir aquellos para los que su peso de Hamming es no mayor que $(d-1)/2$.

Si $C \leq G^n$ es un código-grupo de longitud n, para cada entero $1 \leq k \leq n$ definimos el *grupo salida* G_k como el conjunto de todos los elementos $g \in G$ que aparecen como k-sima componente de alguna palabra de C. Es decir, $G_k = \pi_k(C)$, donde $\pi_k : G^n \to G$ es la k-sima proyección canónica de G^n sobre G. El producto directo $W = \prod_{i=1}^n G_i$ recibe el nombre de *espacio de salida* del código C. Sus propiedades condicionan las propiedades correctoras del código. Así, por ejemplo, se tiene el siguiente resultado (teorema 4 de [30]).

Teorema 5.4.2 *Sea C un código-grupo normal sobre un grupo G. Supongamos que su espacio de salida $W = \prod_{i=1}^n G_i$ es no abeliano, entonces la distancia mínima de Hamming de C es $d_H(C) = 1$.*

Demostración: Si C es un código-grupo normal, entonces $C \trianglelefteq G^n$, y por tanto, $C \trianglelefteq W$. Puesto que W es no abeliano, $W' = \prod_{i=1}^n G_k' \neq 1$, y existe k tal que $G_k' \neq 1$, por lo que se pueden encontrar elementos $a_k, b_k \in G_k$ con $[a_k, b_k] \neq 1$. Dado que $a_k \in G_k$, debe existir una palabra en el código C tal que su k-sima componente $c_k = a_k$. Escogemos $c' \in G^n$ dada por $c_i' = a_i^{-1}$ para $i \neq k$ y $c_k' = b_k$. Como $C \trianglelefteq G^n$ y $c \in C$, el conmutador $[c, c'] \in C$, y entonces $[c, c'] = 1 \cdots [a_k, b_k] \cdots 1$ es un elemento del código con peso de Hamming $\omega_H([c, b']) = 1$. ■

Nota 5.4.3 *Si seguimos un razonamiento similar, concluimos que todos los elementos de la forma $1 \cdots [a_k, b_k] \cdots 1$, con $a_k, b_k \in G_k$ son elementos de C. Dado que generan el subgrupo derivado W', se sigue que $W' \leq C$.*

Al igual que los códigos-grupo clásicos de longitud n se definen como subconjuntos del producto directo G^n, los códigos Clifford producto (de longitud n) se definen a partir del producto directo de n copias de un grupo abstracto de error. Sin embargo, el producto directo de éstos no es, en general, un grupo abstracto de error. No obstante, como se puede ver a continuación, siempre es posible encontrar un cociente que lo es. Como paso previo, introducimos el siguiente resultado (lema 2.27 de [41]).

Lema 5.4.4 *Sea G un grupo y sea χ un carácter suyo. Si $\mathfrak{X}$ es una representación de G cuyo carácter es χ, se cumple que:*

1. $Z(\chi) = \{g \in G : \mathfrak{X}(g) = \varepsilon I$ *para algún* $\varepsilon \in \mathbb{C}\}$;
2. $Z(\chi)$ *es un subgrupo de* G;
3. $\chi_{Z(\chi)} = \chi(1)\lambda$, *con* λ *un carácter lineal de* $Z(\chi)$;
4. $Z(\chi)/\ker\chi$ *es cíclico;*
5. $Z(\chi)/ker\chi \subseteq Z(G/ker\chi)$.
6. *Si además* $\chi \in Irr(G)$, *entonces* $Z(\chi)/ker\chi = Z(G/ker\chi)$.

Teorema 5.4.5 *Sea H un grupo abstracto de error con $\phi \in Irr(H)$ completamente ramificado sobre $Z(H)$ y fiel. Existe un cociente del producto directo H^n que es un grupo abstracto de error.*

Demostración: En estas condiciones, consideramos el carácter de H^n $\eta = \phi\times\cdots\times\phi$ definido como $\eta(h_1,\ldots,h_n) = \phi(h_1)\cdots\phi(h_n)$ para todo $(h_1,\ldots,h_n) \in H^n$, que es irreducible por el teorema 4.21 de [41]. Sea $G = H^n/ker\eta$, por

el lema anterior $Z(G) = Z(H^n/ker\eta) = Z(\eta)/ker\eta$ es un grupo cíclico. Sea $h \in Z(\eta) \leq H^n$, entonces se cumple que

$$\eta(1) = |\eta(h)| = |\prod_{i=i}^{n} \phi(h_i)| = \prod_{i=1}^{n} |\phi(h_i)| \leq \phi(1)^n = \eta(1),$$

de donde se sigue que $|\phi(h_i)| = \phi(1)$ para todo i. En consecuencia, puesto que el otro contenido es trivial, se tiene que $\mathbf{Z}(\eta) = Z(\phi)^n$. Por otra parte, por el corolario 2.30 de [41], tenemos que $\phi(1)^2 \leq |H : Z(\phi)| \leq |H : Z(H)|$ y puesto que ϕ es totalmente ramificado sobre $Z(H)$, se sigue que $Z(\phi) = Z(H)$. Por consiguiente, $Z(\eta) = Z(H)^n = Z(H^n)$ y $Z(G) = Z(H^n)/ker\eta$.

Consideramos el carácter $\hat{\eta}$ de G definido como $\hat{\eta}(h\, ker\eta) = \eta(h)$, para todo $h\, ker\eta \in G$, que es irreducible por el lema 2.22 de [41] y fiel. Además

$$|G : Z(G)| = \frac{|H^n : ker\eta|}{|Z(H^n) : ker\eta|} = |H : Z(H)|^n = (\phi^2(1))^n = \hat{\eta}^2(1),$$

por lo que $\hat{\eta}$ es completamente ramificado sobre $Z(G)$. Así pues, G es un grupo de tipo central cuyo centro es cíclico. Se sigue del teorema 5.1.8 que G es un grupo abstracto de error. ■

Dado H un grupo abstracto de error con $\phi \in Irr(H)$ totalmente ramificado sobre $Z(H)$, el grupo cociente G del teorema anterior es un grupo abstracto de error y por ello, se pueden construir códigos Clifford sobre él. Daremos a estos códigos el nombre de *códigos Clifford producto*.

Puesto que existe una correspondencia biyectiva entre los caracteres irreducibles del grupo H^n cuyo núcleo contiene a $ker\eta$ y los caracteres irreducibles de G (ver lema 2.22 de [41]), en adelante identificaremos ambos conjuntos.

Definición 5.4.6 *Sea G el grupo cociente $G = H^n/K$ del teorema 5.4.5 y $\pi : H^n \to G$ la proyección canónica. Dado $g \in G$, su peso de Hamming $\omega_H(g)$ es el menor peso de Hamming de los elementos de $\pi^{-1}(g)$. Es decir,*

$$\omega_H(g) = min\{\omega_H(h) : h \in H^n,\, \pi(h) = g\}.$$

Notemos que con esta definición el elemento $1 \in G$ tiene peso de Hamming $\omega_H(1) = 0$, pues $(1, \ldots, 1) \in \pi^{-1}(1) = K$. De igual forma, es fácil ver que si $h \in G$ y $g \in \pi^{-1}(h)$, entonces $\omega_H(h) \leq \omega_H(g)$.

Sea Q un código Clifford producto con datos (G, ρ, N, χ). A partir del teorema 5.2.3 y del corolario 5.3.5 sabemos que las propiedades correctoras de Q dependen del conjunto $T(\chi) - Z(\chi)$. Por otra parte, la preimagen $\pi^{-1}(T(\chi) - Z(\chi)) \subseteq H^n$ es un código-bloque de longitud n sobre H cuyo peso mínimo de Hamming coincide, por definición, con el de $T(\chi) - Z(\chi) \subseteq G$.

Supongamos que $\omega_H(T(\chi) - Z(\chi)) = d$, entonces cualquier elemento con menor peso de Hamming será detectable por el código Q. El resultado siguiente, cuya demostración se basa en la del teorema 5.4.2, impone restricciones a este peso mínimo.

Proposición 5.4.7 *Sea Q un código Clifford producto con datos (G, ρ, N, χ) en las condiciones del lema anterior. Sea $M = \pi^{-1}(N) \leq H^n$ y sea $W_M = \prod_{i=1}^{n} M_i \leq H^n$ el espacio de salida del código-grupo M, que suponemos no abeliano. Si $W'_M \bigcap \pi^{-1}(T(\chi) - Z(\chi)) \neq \emptyset$, con W'_M el subgrupo derivado de W_M, entonces el peso mínimo de Hamming de $T(\chi) - Z(\chi)$ es uno.*

Demostración: Supongamos que el peso mínimo de Hamming del conjunto $T(\chi) - Z(\chi) \subseteq G$ es mayor que uno, entonces el de su preimagen $\pi^{-1}(T(\chi) - Z(\chi)) \subseteq H^n$ también lo es. Puesto que $N \trianglelefteq G$, se tiene que $M \trianglelefteq H^n$ y entonces $M \trianglelefteq W_M$. Por la nota 5.4.3 sabemos que en ese caso el derivado

$W'_M \leq M$, de donde se sigue que $W'_M \leq \pi^{-1}(T(\chi))$, pues recordemos que $N \leq T(\chi)$. Puesto que W_M es no abeliano, entonces $W'_M = \prod_{i=1}^{n} M'_i \neq 1$, con lo que alguno de los $M'_i \neq 1$. Supongamos que $1 \neq h_k \in M'_k$ y consideramos la palabra c con $c_k = h_k$ y $c_i = 1$ para todo $i \neq k$. Claramente esta palabra tiene peso de Hamming $\omega_H(c) = 1$ y es un elemento de $M \leq \pi^{-1}(T(\chi))$. Sea $g = \pi(c) \in T(\chi)$, es claro que $\omega_H(g) \leq 1$. Si $\omega_H(g) = 1$, g es detectable por hipótesis, por lo que $g \notin T(\chi) - Z(\chi)$ y puesto que $g \in T(\chi)$, esto implica que $g \in Z(\chi)$. Por otra parte, si $\omega_H(g) = 0$, se sigue que $c \in \pi^{-1}(1)$ y entonces $g = 1 \in Z(\chi)$. Si repetimos este argumento para cualquier grupo no trivial M'_j, encontramos que para toda secuencia c tal que $c_j \neq 1$ y $c_i = 1$ para todo $i \neq j$, $\pi(c) \in Z(\chi)$. Como estas secuencias generan el grupo W'_M, se sigue que $W'_M \leq \pi^{-1}(Z(\chi))$, por lo que $W'_M \bigcap \pi^{-1}(T(\chi) - Z(\chi)) = \emptyset$, lo que constituye una contradicción. ■

Como consecuencia, encontramos una condición necesaria para que un código Clifford producto detecte todos los errores con peso de Hamming uno.

Corolario 5.4.8 *Sea Q un código Clifford producto con datos (G, ρ, N, χ). Si Q es capaz de detectar todos los errores con peso de Hamming uno, entonces $N' \leq Z(\chi)$.*

Demostración: Supongamos que el código Q detecta todos los errores con peso de Hamming 1, entonces $\omega_H(T(\chi) - Z(\chi)) > 1$ y por el resultado anterior $W'_M \bigcap \pi^{-1}(T(\chi) - Z(\chi)) = \emptyset$, donde $\pi : H^n \to G$ es la proyección canónica y W_M es el espacio de salida asociado a $M = \pi^{-1}(N)$. Puesto que $N \leq T(\chi)$, esta propiedad implica que $W'_M \leq \pi^{-1}(Z(\chi))$. Entonces se verifica que $\pi^{-1}(N') = KM' \leq KW'_M \leq \pi^{-1}(Z(\chi))$, y por consiguiente $N' \leq Z(\chi)$. ■

Una vez que se obtiene este resultado, cabe preguntarse si existen códigos

Clifford producto que sean capaces de detectar todos los errores con peso de Hamming uno. Como veremos a continuación, los grupos abstractos de error nilpotentes de clase dos satisfacen esta condición, por lo que aportan una familia de códigos producto con la propiedad del corolario 5.4.8.

Proposición 5.4.9 *Sea H un grupo abstracto de error nilpotente de clase dos y sea $G = H^n/K$ el grupo abstracto de error del teorema 5.4.5. Todos los códigos Clifford producto (G, ρ, N, χ) satisfacen $N' \leq Z(\chi)$.*

Demostración: Si H es un grupo nilpotente de clase 2, entonces $G = H^n/K$ también lo es. En ese caso $G' \leq Z(G)$ y así $N' \leq Z(G)$. Hemos visto que para cualquier código Clifford se puede suponer que $Z(G) \leq N$, por tanto $Z(G) \leq Z(N) = \bigcap\{Z(\xi) : \xi \in Irr(N)\}$ (ver corolario 2.28 de [41]). En consecuencia, $N' \leq Z(\chi)$. ■

Cuando G es nilpotente de clase dos, el grupo de error $G/Z(G)$ es abeliano y cualquier código Clifford con respecto a N lo es también con respecto a $Z(N)$ (ver teorema 6 en [52]). Por tanto, en estas condiciones todo código de Clifford es código estabilizador.

Dedicaremos el resto de la sección a encontrar una caracterización de aquellos códigos Clifford producto que detectan todos los errores con peso de Hamming uno y que son también estabilizadores. Comenzaremos con el resultado siguiente.

Teorema 5.4.10 *Sea Q un código Clifford producto con datos (G, ρ, N, χ). Si el código Q detecta todos los errores con peso de Hamming uno, entonces el grupo $N/ker\chi$ es nilpotente de clase dos.*

Demostración: El grupo $\hat{N} = N/ker\chi$ es nilpotente de clase dos si y sólo si $\hat{N}/Z(\hat{N})$ es abeliano. Del lema 5.4.4 se sigue que $Z(\hat{N}) = Z(\chi)/ker\chi$, por tanto $\hat{N}/Z(\hat{N}) \cong N/Z(\chi)$, que es abeliano si y sólo si $N' \leq Z(\chi)$. ■

El resultado siguiente da una condición necesaria para que un código Clifford producto que detecta todos los errores con peso de Hamming uno sea un código estabilizador.

Lema 5.4.11 *Sea Q un código Clifford producto con datos (G, ρ, N, χ) que corrige todos los errores con peso de Hamming uno. Si χ es fiel, Q es un código estabilizador.*

Demostración: Puesto que χ es un carácter irreducible y fiel de N, por el lema 5.4.4 tenemos que $Z(\chi) = Z(N)$, que es un subgrupo normal abeliano de G. Por el corolario 5.3.7 bastará probar que χ es completamente ramificado sobre $Z(\chi)$, o lo que es equivalente, que χ se anula en $N - Z(\chi)$.

Sea $g \in N - Z(\chi) = N - Z(N)$, entonces existe un elemento $n \in N$ tal que el conmutador $[g, n] = z \neq 1$. Como Q detecta todos los errores con peso de Hamming uno, $N' \leq Z(\chi)$, y en particular $z \in Z(\chi)$. Sea T una $\mathbb{C}$-representación de N cuyo carácter sea χ. Es claro que $T(gz) = T(g)T(z) = \omega T(g)$, con $\omega \in \mathbb{C}$ y $|\omega| = 1$. Por tanto, $\chi(gz) = \omega\chi(g)$ y puesto que χ es fiel, $\omega \neq 1$. Por otra parte, $\chi(g) = \chi(n^{-1}gn) = \chi(g[g, n]) = \chi(gz)$, es decir, $\chi(g) = \omega\chi(g)$, con $\omega \neq 1$, por consiguiente $\chi(g) = 0$. ■

Teorema 5.4.12 *Sea Q un código Clifford producto con datos (G, ρ, N, χ) que detecta todos los errores con peso de Hamming uno. El carácter χ es completamente ramificado sobre $Z(\chi)$.*

Demostración: Consideramos el carácter $\hat{\chi}$ del grupo cociente $\hat{N} = N/ker\chi$, que es irreducible y fiel. Por la demostración del resultado anterior, $\hat{\chi}$ es completamente ramificado sobre $Z(\hat{\chi})$. Puesto que $ker\chi \leq Z(\chi)$, es fácil ver que $Z(\hat{\chi}) = Z(\chi)/ker\chi = Z(\hat{N})$, y así se sigue que $\hat{\chi}$ se anula en $\hat{N} - Z(\hat{N})$. Sea $g \in N - Z(\chi)$ un elemento cualquiera, entonces $\hat{g} = g\,ker\chi \notin Z(\hat{\chi})$ y

así, $\chi(g) = \hat{\chi}(\hat{g}) = 0$, para todo $g \in N - Z(\chi)$. Por el corolario 2.30 de [41], tenemos que $\chi(1)^2 = |N : Z(\chi)|$, y por ello, χ es completamente ramificado sobre $Z(\chi)$. ■

Por último, a partir del corolario 5.3.7 encontramos la siguiente caracterización para los códigos Clifford producto que son estabilizadores.

Corolario 5.4.13 *Sea Q un código Clifford producto con datos (G, ρ, N, χ) que detecta todos los errores con peso de Hamming uno. Entonces Q es un código estabilizador si y sólo si $Z(\chi)$ es normal abeliano en G.*

Conclusiones

Como hemos visto, esta memoria consta de dos partes bien diferenciadas. Por una parte, a lo largo de los cuatro primeros capítulos, extendemos la teoría de super-caracteres, inicialmente desarrollada sólo para el grupo $\mathbf{U}_n(q)$, para abarcar $\mathbb{F}_q$-grupos de álgebra y grupos adjuntos asociados a módulos nilpotentes sobre anillos de Galois.

Tras el primer capítulo, donde se recopilan los resultados ya conocidos sobre super-caracteres del grupo $\mathbf{U}_n(q)$, conseguimos extender su definición a los $\mathbb{F}_q$-grupos de álgebra. Estos resultados constituyen el capítulo 2 y en ellos se apoyan los dos capítulos siguientes. En este sentido, queremos resaltar el ejemplo 2.5 que, a pesar de su sencillez, ilustra de forma clara la construcción de los super-caracteres y los problemas que aparecen cuando se trabaja con grupos de álgebra más complejos.

Merecen una mención especial los resultados del capítulo 3, pues por una parte establecen en qué forma se podrían conocer los super-caracteres para un $\mathbb{F}_q$-grupo de álgebra cualquiera sin necesidad de determinar las órbitas de cotransición y por otra, muestran las diferencias con respecto al grupo $\mathbf{U}_n(q)$. Recordemos que, por el teorema 1.4.12, los caracteres básicos (definidos como producto de caracteres elementales) y los caracteres de transición (definidos a partir de las órbitas de cotransición y que se identifican con nuestra definición de super-caracteres) coinciden para $\mathbf{U}_n(q)$. Sin embargo,

los caracteres básicos definidos en el capítulo 3 no son super-caracteres, sino una suma de ellos. Ahora bien, los teoremas 3.1.19, 3.1.20 y la proposición 3.2.2 prueban que poseen las mismas propiedades que aquellos, por lo que se podría construir una nueva "teoría de super-caracteres" basada en estos caracteres básicos. Ésta sería una de las líneas abiertas para su desarrollo futuro.

En el capítulo 4 definimos super-caracteres en grupos adjuntos asociados a módulos libres sobre anillos de Galois y comprobamos que los resultados del capítulo 2 se mantienen en la nueva situación. Al igual que allí, queremos resaltar el ejemplo de la última sección, pues si lo comparamos con el de 2.5, podemos apreciar cómo influye la naturaleza del anillo en la forma de los super-caracteres. Esperamos extender estos resultados, recogidos en [11], al estudio de grupos adjuntos asociados a módulos nilpotentes sobre dominios de valoración discreta.

La segunda parte trata de las aplicaciones de la Teoría de Representaciones al diseño de códigos cuánticos y constituye el capítulo 5. La caracterización de los códigos Clifford estabilizadores que allí se realiza fue motivada por las limitaciones técnicas encontradas a la hora de generar ejemplos de códigos Clifford producto que no fuesen estabilizadores. Para este estudio se utilizó el programa Magma (ver [18]) y no se encontraron resultados significativos pues, aun en el caso de grupos abstractos de error con los órdenes más pequeños, las dificultades de computación impidieron un estudio exhaustivo. Sin embargo, tanto los códigos obtenidos a partir de este estudio como los resultados teóricos (ver teorema 5.4.12 y corolario 5.4.13) parecen indicar que los mejores resultados se obtienen cuando el código es estabilizador. Este hecho no es nuevo, pues ya aparece contemplado en [31] para códigos cuánticos que no se obtienen a partir del producto de grupos abstractos de error. Como

trabajo futuro en este campo, esperamos construir nuevos códigos Clifford producto con el objeto de confirmar este punto y poder garantizar que un código Clifford producto corrige errores cuyo peso de Hamming es mayor que uno si y sólo si es un código estabilizador.

Bibliografía

[1] Adkins, William A. y Steven H. Weintraub: *Algebra. An Approach via Module Theory*, volumen 136 de *Graduate Texts in Mathematics*. Springer-Verlag, 1999.

[2] Alperin, J. L. y Rowen B. Bell: *Groups and Representations*, volumen 162 de *Graduate Text in Mathematics*. Springer Verlag, 1995.

[3] André, C. A. y A. P. Nicolás: *Supercaracteres de grupos-de-álgebra finitos*. En *Actas do Encontro de Algebristas Portugueses*, Braga, 2005.

[4] André, C. A. M.: *Basic Characters of the Unitriangular Group*. Journal of Algebra, 175:287–319, 1995.

[5] André, C. A. M.: *Basic Sums of Coadjoint Orbits of the Unitriangular Group*. Journal of Algebra, 176:959–1000, 1995.

[6] André, C. A. M.: *The regular character of the unitriangular group*. Journal of Algebra, 241:1–52, 1998.

[7] André, C. A. M.: *Irreducible characters of finite algebra groups*. En *Textos de Matemática. Série B*, número 19, páginas 65–80. Departamento de Matemática da Universidade de Coimbra, 1999.

[8] André, C. A. M.: *The basic character table of the unitriangular group.* Journal of Algebra, 241:437–471, 2001.

[9] André, C. A. M.: *Basic Characters of the Unitriangular Group (for arbitrary primes).* Proceeding of the American Mathematical Society, 130(7):1943–1954, 2002.

[10] André, C. A. M., A. M. Neto y A. P. Nicolás: *Basic characters of linear groups over finite rings.* En preparación.

[11] André, C. A. M. y A. P. Nicolás: *Supercharacters of the adjoint group of a finite radical ring.* J. of Group Theory.

[12] Arias-Castro, Ery, Persi Diaconis y Richard Stanley: *A super-class walk on upper-triangular matrices.* Journal of Algebra, 278:739–765, 2004.

[13] Armstrong, M. A.: *Groups ans Symmetry.* Undergraduate Texts in Mathematics. Springer Verlag, 1988.

[14] Ashikhmin, Alexei y Emanuel Knill: *Nonbinary Quantum Stabilizer Codes.* IEEE Transactions on Information Theory, 47(7):3065–3072, 2001.

[15] Ashikhmin, Alexei E., Alexander M. Barg, Emanuel Knill y Simon N. Litsyn: *Quantum Error Detection I: Statement of the Problem.* IEEE Transactions on Information Theory, 46(3):778–788, 2000.

[16] Atiyah, M. F. y I. G. Macdonald: *Introducción al Álgebra Conmutativa.* Reverté, 1973.

[17] Bini, Gilberto y Flaminio Flamini: *Finite Commutative Rings and Their Applications.* Kluwer Academic Publishers, 2002.

[18] Bosma, W., J. J. Cannon y C. Playoust: *The Magma algebra system I: The user language.* J. Symb. Comp., 24:235–266, 1997.

[19] Burgos, Juan de: *Curso de álgebra y geometría.* Alhambra, 1989.

[20] Calderbank, A. R., E. M. Rains, P. W. Shor y N. J. A. Sloane: *Quantum error correction and orthogonal geometry.* Phys. Rev. Lett., 78:405–409, 1997.

[21] Calderbank, A. R., E. M. Rains, P. W. Shor y N. J. A. Sloane: *Quantum error correction via codes over GF(4).* IEEE Transactions on Information Theory, 44:1369–1387, 1998.

[22] Catino, F. y M. M. Miccoli: *Local rings whose multiplicative group is nilpotent.* Archiv der Mathematik, 81:121–125, 2003.

[23] Claasen, H. L. y R. W. Goldbach: *A field-like property of finite rings.* Indag. Math., N. S., 3(1):11–26, 1992.

[24] Curtis, C. W. y I. Reiner: *Representation theory of finite groups and associative algebras*, volumen 1. Wiley-Interscience, New York, 1962.

[25] Curtis, C. W. y I. Reiner: *Methods of representation theory (with applications to finite groups and orders)*, volumen 1. Wiley-Interscience, New York, 1981.

[26] DeMeyer, Frank R. y Gerald J. Janusz: *Finite Groups with an Irreducible Representation of Large Degree.* Math. Z., 108:145–153, 1969.

[27] Diaconis, P. y I. M. Isaacs: *Supercharacters and superclasses for algebra groups.* preprint, 2006.

[28] Diaconis, Persi y Nathaniel Thiem: *Supercharacter formulas for pattern groups*. preprint, 2006.

[29] Eilenberg, S. y T. Nakayama: *On the dimension of modules and algebras, II*. Nagoya Math. J., 9:1–16, 1955.

[30] Forney Jr., G. David: *On Hamming distance properties of group codes*. IEEE Transactions on Information Theory, 38(6):1797–1801, 1992.

[31] Gottesman, D.: *A class of quantum error-correcting codes saturating the quantum Hamming bound*. Phys. Rev. A., 54:1862–1868, 1996.

[32] Grove, Larry C.: *Algebra*. Pure and Applied Mathematics. Academic Press, 1983.

[33] Halasi, Zoltan: *On the characters and commutators of finite algebra groups*. Journal of Algebra, 275:481–487, 2004.

[34] Hall Jr., Marshall: *The Theory of Groups*. Chelsea Publishing Company, 1976.

[35] Hirano, Y.: *On admissible rings*. Indag. Math., N. S., 8(1):55–59, 1997.

[36] Honold, Thomas: *Characterization of finite Frobenius rings*. Arch. Math., 76:406–415, 2001.

[37] Howlett, Robert B. y I. Martin Isaacs: *On groups of central type*. Math Z., 179:555–569, 1982.

[38] Hungerford, T. W.: *Algebra*, volumen 73 de *Graduate texts in mathematics*. Springer-Verlag, spanish8th edición, 1996.

[39] Huynh, Dinh van y Ngo Si Tung: *A note on Quasi-Frobenius Rings*. Proceedings of the American Mathematical Society, 124(2):371–375, 1996.

[40] Internaldo, J. Carmelo, Reginaldo Palazzo y Michele Elia: *Group block codes over non abelian groups are asymptotically bad.* IEEE Transactions on Information Theory, 48(4):1277–1280, 1996.

[41] Isaacs, I. M.: *Character Theory of Finite Groups.* Dover, 1994.

[42] Isaacs, I. M.: *Characters of Groups Associated with Finite Algebras.* Journal of Algebra, 177:708–730, 1995.

[43] Isaacs, I. M. y D. Karagueuzian: *Conjugacy in groups of upper triangular matrices.* J. Algebra, 202:704–711, 1998.

[44] Jacobson, Nathan: *Lie Algebras.* Interscience Publishers, New York, 1962.

[45] Jacobson, Nathan: *Structure of Rings*, volumen 37 de *Colloquium Publications.* American Mathematical Society, 1964.

[46] Jacobson, Nathan: *Lectures in Abstract Algebra. II. Linear Algebra*, volumen 31 de *Graduate Texts in Mathematics.* Springer Verlag, 1975.

[47] Kazhdan, D.: *Proof of Springer's hypothesis.* Israel Journal of Mathematics, 28(4):272–286, 1977.

[48] Kirillov, A. A.: *Unitary representations of nilpotent Lie groups.* Russian Math. Surveys, 17(4):57–101, 1962.

[49] Kirillov, A. A.: *Variations on the Triangular Theme.* Amer. Math. Soc. Transl., 169:43–73, 1995.

[50] Kirillov, A. A.: *Merits and demerits of the orbit method.* Bull. Amer. Math. Soc., 36:433–488, 1999.

[51] Klappenecker, Andreas y Martin Roetteler: *Beyond Stabilizer Codes I: Nice Error Basis.* IEEE Transactions on Information Theory, 48(8):2392–2395, 2002.

[52] Klappenecker, Andreas y Martin Roetteler: *Beyond Stabilizer Codes II: Clifford Codes.* IEEE Transactions on Information Theory, 48(8):2396–2399, 2002.

[53] Klappenecker, Andreas y Martin Roetteler: *On the structure of non-stabilizer Clifford codes.* Quantum Inf. Comput., 4(2):152–160, 2004.

[54] Klappenecker, Andreas y Martin Roettler: *Unitary Error Basis: Constructions, Equivalence and Applications.* Lecture Notes in Comput. Sci., 2643:139–149, 2003.

[55] Klappenecker, Andreas y Martin Roettler: *On the Monomiality of Nice Error Basis.* IEEE Transactions on Information Theory, 51(3):1084–1089, 2005.

[56] Knill, E., R. Laflamme, A. Ashikhmin, H. Barnum, L. Viola y W. H. Zurek: *Introduction to Quantum Error Correction.* arXiv:quant-ph/0207170, 2006.

[57] Knill, Emanuel: *Group representations, error bases and quantum codes.* Los Alamos National Laboratory Report LAUR-96-2807. quant-ph/96080049, 1996.

[58] Knill, Emanuel: *Non-binary Unitary Error Bases and Quantum Codes.* Los Alamos National Laboratory Report LAUR-96-2717, 1996.

[59] Knill, Emanuel y Raymond Laflamme: *Theory of Quantum Error-Correcting Codes.* Physical Review A, 55(2), 1997.

[60] Knill, Emanuel, Raymond Laflamme y Lorenzo Viola: *Theory of Quantum Error Correction for General Noise*. arXiv:quant-ph/9909066, 1999.

[61] Kostrikin, A. I. y I. R. Shafarevich (editores): *Algebra II*, volumen 18 de *Encyclopaedia of Mathematical Sciences*. Springer Verlag, 1991.

[62] Lam, T. Y.: *A first course in noncommutative rings*, volumen 131 de *Graduate texts in Mathematics*. Springer Verlag, 1991.

[63] Lehrer, G. I.: *Discrete series and the unipotent group*. Compositio Mathematica, 28(1):9–19, 1974.

[64] Lidl, Rudolf y Harald Niederreiter: *Finite Fields*. Número 20 en *Encyclopedia of Mathematics and its Applications*. Addison-Wesley Publishing Company, 1983.

[65] Manabu, Hagiwara y Hideki Imai: *Non stabilizer Clifford codes with qupit*. arXiv:quant-ph/0402060, 2004.

[66] Matsumura, Hideyuki: *Commutative ring theory*, volumen 8 de *Cambridge studies in advanced mathematics*. Cambrigde University Press, 1992.

[67] McDonald, B. R.: *Finite rings with identity*, volumen 28 de *Pure and Applied Mathematics*. Marcel Dekker, 1974.

[68] Nakayama, T.: *On Frobeniusean algebras*. Annals of Math., 40(2):611–633, 1939.

[69] Nakayama, T.: *On Frobeniusean algebras II*. Annals of Math., 42(2):1–21, 1941.

[70] Nielsen, Michael A. y Isaac L. Chuang: *Quantum Computation and Quantum Information.* Cambrigde University Press, 2000.

[71] Rains, Eric M.: *Nonbinary Quantum Codes.* IEEE Transactions on Infromation Theory, 45(6):1827–1832, 1999.

[72] Reid, Miles: *Undergraduate Commutative Algebra*, volumen 29 de *London Mathematical Society Student Texts.* Cambridge University Press, 1995.

[73] Rojo, Jesús: *Álgebra lineal.* AC, 1989.

[74] Rúa, I. F.: *Anillos no asociativos en Codificación y Criptografía.* Tesis Doctoral, Universidad de Oviedo, 2004.

[75] Rutter Jr., Edgar A.: *Two characterizations of Quasi-Frobenius rings.* Pacific Journal of Mathematics, 30(3):777–784, 1969.

[76] Serre, J. P.: *Representaciones Lineales de los Grupos Finitos.* Omega, 1970.

[77] Shor, P. W.: *Scheme for reducing decoherence in quantum memory.* Phys. Rev. A, 52:2493, 1995.

[78] Shuqin, Fan y Han Wenbao: *Character sums over Galois rings and primitive polynomials over finite fields.* Finite Fields and Their Applications, 10:36–52, 2004.

[79] Steane, A. M.: *Error correcting codes in Quantum Theory.* Phys. Rev. Lett., 77(5):793–797, 1996.

[80] Wood, J. A.: *Duality for modules over finite rings and applications to coding theory.* Amer. J. Math., 121:555–575, 1999.

[81] Xue, Weimin: *A note on finite local rings.* Indag. Math., N. S., 9(4):627.628, 1998.

[82] Yan, N.: *Representation of the finite unipotent linear group.* Tesis Doctoral, University of Pennsylvania, 2001.

Índice alfabético