ÁLGEBRAS G-GRADUADAS SOBRE GRUPOS ABELIANOS FINITOS.

por

Natalia Agudelo Muñetón.

Trabajo presentado como requisito parcial
para optar al Título de

Magíster en Matemáticas

Director: Juan Diego Vélez y Luis Alberto Wills Toro

Universidad Nacional de Colombia
Sede Medellín

Facultad de Ciencias

Escuela de Matemáticas

Diciembre 2009

Este proyecto hubiera sido imposible sin el apoyo de COLCIENCIAS que ayudó a su financiación, código QUIPU 20301006958.

Resumen

En esta tesis se estudia el problema de clasificación de las álgebras G-graduadas, salvo isomorfismo, usando una colección miscelánea de técnicas entre las que se encuentran la cohomología de grupos, la teoría de representación clásica de grupos y algunas técnicas elementales de teoría de representación de grupos de Lie. Se dará un criterio general en términos de la cohomología $H^2(G, k^*)$ para determinar cuándo dos G-álgebras son isomorfas como álgebras graduadas y se obtendrá una clasificación completa bajo isomorfismos graduados de estas álgebras, en el caso asociativo, y cuando G sea un grupo cíclico. Usando teoría de representación de grupos, se dará una clasificación completa de todas las álgebras asociativas sobre grupos finitos en el sentido general, es decir, sin tener en cuenta la graduación. En el caso no asociativo, daremos una clasificación completa bajo isomorfismos graduados de todas las álgebras complejas G-graduadas sobre un grupo cíclico G, en el caso en el que la función de asociatividad r sea simétrica en las dos primeras variables.

Contenido

Agradecimientos

Quisiera agradecer a los profesores Luis Alberto Wills Toro y Juan Diego Vélez Caicedo, quienes han sido mis tutores en la maestría, y directores de esta tésis. También quiero agradecer a mis padres por todo su apoyo durante la realización de mis estudios.

Introducción

Sea G un grupo y sea W un álgebra sobre un anillo conmutativo y unitario R. Diremos que W tiene una estructura de álgebra graduada con componentes de rango 1 *(no necesariamente conmutativa ni asociativa)* si existe una G-graduación $W = \oplus_{g\in G} W_g$ en la cual cada sumando W_g es un R-módulo libre de rango 1. Recordemos que esto quiere decir que la suma $\oplus_{g\in G} W_g$ es directa, y que para cada par de elementos $a, b \in G$ se verifica que $W_a W_b \subset W_{ab}$. Diremos que W no tiene *divisores de cero monomiales* si para todo par de elementos no nulos w_a, w_b en W_a y W_b se cumple que $w_a w_b \neq 0$. *Un álgebra W con estructura de álgebra graduada sobre G, con componentes de rango 1 y sin divisores de cero monomiales la llamaremos brevemente una R-álgebra G-graduada.*

Si fijamos $B = \{w_g : g \in G\}$, una base para $W = \oplus_{g\in G} W_g$, la estructura de W está determinada por las *constantes de estructura del álgebra*, es decir, por una función $C_B : G\times G \to A \subset R$, donde A es un subdominio del *grupo multiplicativo* de R (pedimos que A sea dominio, de tal manera que W no tenga divisores de cero monomiales) y tal que $w_a w_b = C_B(a, b) w_{ab}$. Como W es un álgebra unitaria, se sigue que si $e \in G$ es la unidad del grupo, entonces $w_e = 1$ es el elemento unitario del álgebra y por tanto $w_a w_e = C_B(a, e) w_a = w_a \cdot 1 = w_a$.

Con el fin de analizar la no conmutatividad y no asociatividad en este tipo de álgebras en el caso en el que R es un campo y $A \subset k^*$ un subgrupo del grupo multiplicativo $k^* = k - \{0\}$, definimos, con respecto a la base B, las siguientes funciones de conmutatividad y asociatividad, $q : G \times G \to A$ y $r : G \times G \times G \to A$ por:

$$\begin{aligned} q(a, b) &= C(a, b)C(b, a)^{-1} \\ r(a, b, c) &= C(b, c)C(ab, c)^{-1}C(a, bc)C(a, b)^{-1} \qquad (1) \end{aligned}$$

donde el exponente " -1"denota el inverso multiplicativo en A.

Cuando G es abeliano, vemos inmediatamente que $w_a w_b = q(a,b) w_b w_a$. Y para cualquier grupo G, en general, se verifica fácilmente que $w_a(w_b w_c) = r(a,b,c)(w_a w_b) w_c$.

Definición 0.0.1 *Un morfismo entre dos R-álgebras G-graduadas $W = \oplus_{g\in G} W_g$ y $V = \oplus_{g\in G} V_g$ es un morfismo (unitario) de R-álgebras $\phi : W \longrightarrow V$ el cual satisface que $\phi(W_g) \subset V_g$, para todo $g \in G$.*

Es fácil ver que esta definición equivale a que existan bases $B_1 = \{w_g : g \in G\}$, $B_2 = \{v_g : g \in G\}$, para W y V, respectivamente, tales que $W_g = Rw_g$ y $V_g = Rv_g$, y un morfismo de R-álgebras $\phi : W \to V$ que cumpla que $\phi(w_g) = \varphi(g) v_g$, para una cierta función $\varphi : G \to R$.

Es claro que ϕ es un isomorfismo si y sólo si $\varphi(g)$ es una unidad en R para todo $g \in G$, ya que por ser W y V R-módulos libres de igual rango, ϕ es biyectiva si y sólo si es inyectiva, y esto ocurre si y sólo si $\phi(w_g) = \varphi(g) v_g$ no es cero.

El problema de clasificación de estas álgebras admite al menos tres posibles versiones.

a. W y V pueden ser *isomorfas como R-álgebras G-graduadas*, es decir si existen $\phi : W \longrightarrow V$ y $\psi : V \longrightarrow W$ morfismos como en la definición anterior, tales que $\phi\psi$ y $\psi\phi$ sean la identidad.

b. W y V pueden ser isomorfas como R-álgebras en un sentido general, olvidando la graduación; es decir, sin que se cumpla la condición $\phi(W_g) \subset V_g$.

c. W y V admiten graduaciones (posiblemente distintas a las originales) para las cuales W y V resultan ser isomorfas como álgebras graduadas. En forma precisa, existen graduaciones $W = \oplus_{g\in G} W'_g$ y $V = \oplus_{g\in G} V'_g$, y un isomorfismo de R-álgebras $\phi : W \longrightarrow V$ el cual satisface $\phi(W'_g) \subset V'_g$, para todo $g \in G$.

En este trabajo de tesis estudiaremos álgebras sobre $R = k$, el campo de los reales o complejos, y graduadas sobre grupos finitos. El primer capítulo contiene las definiciones y teoremas básicos de la cohomología de grupos, y de la teoría de representación de grupos y caracteres que se usarán a lo largo de este trabajo.

En el segundo capítulo estudiaremos el problema de clasificación de las álgebras G- graduadas, salvo isomorfismos, usando una colección miscelánea de técnicas entre las que se encuentran la cohomología de grupos, la teoría de representación de grupos clásica y algunas técnicas elementales de teoría de representación de grupos de Lie. Se dará un criterio general en términos de la cohomología $H^2(G, k - \{0\})$ para determinar cuándo dos G-álgebras son isomorfas como álgebras graduadas (Teoremas 2.1.1 y 2.1.3). Como corolario se obtendrá una clasificación completa bajo isomorfismos graduados de estas álgebras en el caso asociativo, y cuando G sea un grupo cíclico.

Usando teoría de representación de grupos y caracteres se dará una clasificación completa de todas las álgebras asociativas sobre grupos finitos en el sentido general como en (b), es decir, sin tener en cuenta la graduación. La idea central para lograr dicha clasificación es mostrar que toda escogencia de base en el álgebra G-graduada que determine constantes de estructura $C_B : G \times G \to A \subset k^*$ da origen a un isomorfismo entre W y un cociente del anillo grupo $k[A \times_C G]/J$, donde $A \times_C G$ es una extensión apropiada de A por G (ver Ejemplo 1.1.1 del primer capítulo). La estructura de $k[A \times_C G]$ puede ser dilucidada usando teoría de caracteres.

En el caso de álgebras G-graduadas *no asociativas* daremos una clasificación completa bajo isomorfismos graduados, como en (a), de todas las álgebras graduadas sobre un grupo cíclico, en el caso en el que la función de asociatividad del álgebra r sea simétrica en las dos primeras variables, es decir, cuando satisface $r(a, b, c) = r(b, a, c)$. Es muy probable que las técnicas usadas para resolver este último problema se puedan extender a grupos abelianos finitos en general.

Capítulo 1

Preliminares

1.1 Extesiones de grupos y grupo anillo

Comenzaremos definiendo la noción de extensión de grupos.

Definición 1.1.1 (Extensión de grupos) *Sean A y G grupos. Una extensión de A por G es una secuencia exacta corta*

$$\alpha : 1 \to A \xrightarrow{i} E \xrightarrow{p} G \to 1$$

Notemos que en este caso $i(A) \lhd E$ y $\dfrac{E}{i(A)} \cong G$. El lector puede ampliar esta definición en la página 790 de [2].

Ejemplo 1.1.1

Sea W un álgebra G-graduada, y sea $C : G \times G \to A \subset k^*$ las constantes de estructura con respecto a una base B escogida. Entonces C da origen a una extensión E de A por G, que denotaremos por $A \times_C G$, de la siguiente manera. Sea $E_W = \{(\alpha, g) : \alpha \in A, g \in G\} \subset A \times G$. Definimos la operación

$$(\alpha, a) \cdot (\beta, b) = (\alpha\beta C(a, b), ab)$$

Entonces si las constantes $C(a, b)$ hacen de W un álgebra asociativa, E_W es un grupo. En efecto todos los axiomas de grupos se verifican fácilmente, excepto posiblemente la asociatividad. La unidad en E_W es el elemento $(1, e)$. Verifiquemos la asociatividad:

$$\begin{aligned} [(\alpha, a)(\beta, b)](\gamma, c) &= (\alpha\beta C(a, b), ab)(\gamma, c) \\ &= (\alpha\beta\gamma C(a, b)C(ab, c), abc) \end{aligned}$$

De otro lado

$$
\begin{aligned}
(\alpha, a)[(\beta, b)(\gamma, c)] &= (\alpha, a)(\beta\gamma C(b, c), bc) \\
&= (\alpha\beta\gamma C(b, c)C(a, bc), abc)
\end{aligned}
$$

Luego, como W es un álgebra asociativa, $r(a, b, c) = 1$ y por tanto $C(b, c)C(a, bc) = C(a, b)C(ab, c)$ de donde se sigue la asociatividad del grupo $A\times_C G$. No es difícil ver que la construcción anterior produce una extensión $1 \to A \xrightarrow{i} E_W \xrightarrow{p} G \to 1$, donde $i(\alpha) = (\alpha, e)$ y $p(\alpha, g) = g$.

En general, si W no es asociativa, $A \times_C G$ resulta ser un *loop, es decir,* un conjunto dotado de una oparación binaria, con elemento unidad a izquierda y derecha, y con inversos a derecha e izquierda (no necesariamente iguales).

Definición 1.1.2 (Grupo anillo) *Sea G un grupo y R un anillo conmutativo. Entonces el grupo anillo de R sobre G se define como el conjunto se sumas formales finitas indizadas por G*

$$
R[G] = \left\{ \sum_{g\in G} r_g g : r_g \in R \right\},
$$

con las operaciones usuales

$$
\begin{aligned}
\sum_{g\in G} r_g g \sum_{h\in G} r_h h &= \sum_{g,h\in G} r_g r_h gh \\
\sum_{g\in G} r_g g + \sum_{g\in G} r_g^{'} g &= \sum_{g\in G} (r_g + r_g^{'})g
\end{aligned}
$$

1.2 Cohomología de grupos

Definición 1.2.1 *Sea G un grupo finito y D un G-módulo. Definimos $C^0(G, D) = D$, y para $n \geq 1$ definimos $C^n(G, D)$ como la colección de todos los mapeos $G^n = G \times \cdots \times G$ (n copias) sobre D. Los elementos de $C^n(G, D)$ son llamados n-cocadenas (de G con valores en D).*

Cada $C^n(G, D)$ es un grupo abeliano multiplicativo: $C^0(G, D) = D$ son las funciones constantes con valores en D (donde la operación binaria de D se denotará en forma multiplicativa y no aditiva, como es costumbre). Para $n \geq 1$, el producto en $C^n(G, D)$ está dado por el producto usual de funciones

$$(f_1f_2)(g_1, g_2, \ldots, g_n) = f_1(g_1, g_2, \ldots, g_n)f_2(g_1, g_2, \ldots, g_n).$$

Definición 1.2.2 *Para $n \geq 0$, definimos la n-cofrontera como el homomorfismo de $C^n(G, D)$ en $C^{n+1}(G, D)$ dado por*

$$\begin{aligned} & d_D^n(\varphi)(g_1, \ldots, g_{n+1}) \\ = \;& g_1\varphi(g_2, \ldots, g_{n+1})(\prod_{i=2}^{n} \varphi(g_1, \ldots, g_{i-1}, g_ig_{i+1}, g_{i+2}, \ldots, g_{n+1})^{(-1)^i})\varphi(g_1, \ldots, g_n)^{(-1)^{n+1}} \end{aligned}$$

1. Sea $Z^n(G, D) = Ker(d_D^n)$, para $n \geq 0$. Los elementos de $Z^n(G, D)$ son llamados *n-cociclos.*

2. Sea $B^n(G, D) = \mathrm{Im}(d_D^{n-1})$, para $n \geq 1$, y sea $B^0(G, D) = 1$. Los elementos de $B^n(G, D)$ son llamados *n-cofronteras.*

Dado que $d_D^n \circ d_D^{n-1} = 0$, se sigue que $\mathrm{Im}(d_D^{n-1}) \subset Ker(d_D^n)$. Por tanto $B^n(G, D)$ es un subgrupo de $Z^n(G, D)$.

Definición 1.2.3 *Sea D un G-módulo. El grupo cociente $Z^n(G, D)/B^n(G, D)$ es llamado la n-ésima cohomología de G con coeficientes en D y es denotado por $H^n(G, D)$, $n \geq 0$. Ver página 764 de [2].*

Si $W = \oplus_{g \in G} W_g$ es un álgebra G-graduada, y B una base para W, entonces las constantes de estructura con respecto a esta base $C : G \times G \to A \subset R$ son elementos de $C^2(G, A)$. Un cómputo elemental muestra que $d^2C(a, b, c) = r(a, b, c)$, donde r es la función definida en (1).

Ejemplo 1.2.1

a) Supongamos que f es la función constante $a \in C^0(G, A) = A$,donde G actúa trivialmente. Entonces, $d^0(f)(g) = ga(a)^{-1}$ y $\ker(d^0) = \{a \in A : ga = a, \forall g \in G\}$. Esto es, $Z^0(G, A) = A^G$, y por tanto $H^0(G, A) = A^G$.

b) Sea G un grupo cíclico de orden m con generador σ y sea $N = 1 + \sigma + \cdots + \sigma^{m-1} \in \mathbb{Z}[G]$. Entonces $N(\sigma - 1) = (\sigma - 1)N = \sigma^m - 1 = 0$. Tomando una resolución libre para $\mathbb{Z}$,

$$\cdots \stackrel{\sigma-1}{\to} \mathbb{Z}[G] \stackrel{N}{\to} \mathbb{Z}[G] \stackrel{\sigma-1}{\to} \cdots \stackrel{N}{\to} \mathbb{Z}[G] \stackrel{\sigma-1}{\to} \mathbb{Z}[G] \stackrel{aug}{\to} \mathbb{Z} \to 0$$

donde aug es la función *aumentación*

$$\begin{aligned} aug : \mathbb{Z}[G] &\to \mathbb{Z} \\ (\sum_{i=0}^{m-1} a_i \sigma^i) &\to \sum_{i=0}^{m-1} a_i \end{aligned}$$

Ahora, aplicando los homomorfismo de $\mathbb{Z}[G]$-módulos para los términos de la resolución y usando la identificación $Hom_{\mathbb{Z}[G]}(\mathbb{Z}[G], A) = A$ obtenemos la cadena de complejos $1 \to A \stackrel{\sigma-1}{\to} A \stackrel{N}{\to} A \stackrel{\sigma-1}{\to} \cdots$.Calculemos los grupos de homología. Para esto basta calcular $H^0(G, A), H^1(G, A)$ y $H^2(G, A)$ ya que los mapeos en la secuencia anterior aparecen alternadamente.

$$\begin{aligned} H^0(G, A) &= \ker(\sigma - 1) = \{a \in A : a(\sigma - 1) = 0\} \\ &= \{a \in A : \sigma a = a\} = A^G \end{aligned}$$

$$H^1(G, A) = \frac{\ker(N)}{im(\sigma - 1)} = \frac{{}_N A}{(\sigma - 1)A}$$

donde ${}_N A = \ker(N) = \{a \in A : Na = 0\}$.

$$H^2(G, A) = \frac{\ker(\sigma - 1)}{im(N)} = \frac{A^G}{NA}$$

En conclusión tenemos

$$H^n(G, A) = \begin{cases} \dfrac{A^G}{NA} \text{ si } n \text{ es par y } n \geq 2 \\ \dfrac{{}_N A}{(\sigma - 1)A} \text{ si } n \text{ es impar y } n \geq 1 \end{cases}$$

En particular, si G actua trivialmente sobre A entonces $Na = a^m$ y obtenemos $H^0(G, A) = A$

$$H^n(G, A) = \begin{cases} \dfrac{A}{A^m} \text{ si } n \text{ es par y } n \geq 2 \\ {}_mA \text{ si } n \text{ es impar y } n \geq 1 \end{cases}$$

Como aplicación, consideremos $A = \mathbb{Z}, \mathbb{Q}, \mathbb{Q}/\mathbb{Z}, \mathbb{R}^*, \mathbb{C}^*$ y G un grupo ciclico finito de orden m actuando trivialmente sobre A.

a)

$$H^n(G, \mathbb{Z}\ ) = \begin{cases} \mathbb{Z} \text{ si } n = 0 \\ \dfrac{\mathbb{Z}}{\mathbb{Z}^m} \text{ si } n \text{ es par y } n \geq 2 \\ 1 \text{ si } n \text{ es impar y } n \geq 1 \end{cases}$$

b)

$$H^n(G, \mathbb{Q}) = \begin{cases} \mathbb{Q} \text{ si } n = 0 \\ 1 \text{ si } n \geq 1 \end{cases}$$

c)

$$H^n(G, \mathbb{Q}/\mathbb{Z}\ ) = \begin{cases} \mathbb{Q}/\mathbb{Z} \text{ si } n = 0 \\ 1 \text{ si } n \text{ es par y } n \geq 2 \\ \dfrac{\mathbb{Z}}{\mathbb{Z}^m} \text{si } n \text{ es impar y } n \geq 1 \end{cases}$$

d)

$$H^n(G, \mathbb{R}^*) = \begin{cases} \mathbb{R}^* \text{ si } n = 0 \\ \dfrac{\mathbb{R}^*}{(\mathbb{R}^*)^m} \text{si } n \text{ es par y } n \geq 2 \\ 1 \text{ si } n \text{ es impar y } n \geq 1 \end{cases}$$

además

$$\frac{\mathbb{R}^*}{(\mathbb{R}^*)^m} = \begin{cases} \{1, -1\} \text{ si } m \text{ es par} \\ \{1\} \text{ si } m \text{ es impar} \end{cases}$$

$$H^n(G, \mathbb{C}^*) = \begin{cases} \mathbb{C}^* \text{ si } n = 0 \\ \dfrac{\mathbb{C}^*}{(\mathbb{C}^*)^m} \text{si } n \text{ es par y } n \geq 2 \\ 1 \text{ si } n \text{ es impar y } n \geq 1 \end{cases}$$

Recordemos que en toda teoría de Cohomología hay secuencias largas asociadas a cada secuencia corta de objetos. En términos precisos tenemos el siguiente resultado..

Teorema 1.2.1 *Sea $1 \to A \to B \to C \to 1$ una secuencia exacta corta de G-módulos. Entonces existe una secuencia exacta larga*

$$1 \to H^0(G,A) \to H^0(G,B) \to H^0(G,C) \xrightarrow{\delta^0} H^1(G,A) \to \cdots \to H^n(G,C) \xrightarrow{\delta^n} H^{n+1}(G,A) \to \cdots$$

de grupos de cohomología.

Este teorema se puede encontrar en la página 768 de [2]

Nuestro objetivo es computar explícitamente el homomorfismo conexión δ. Para tal fin consideremos $A \subset k^*$ y la secuencia exacta corta $1 \to A \xrightarrow{i} k^* \xrightarrow{\pi} k^*/A \to 1$. Aplicando $C^\bullet(G,-)$, donde la acción de G sobre k^* es la trivial, es decir, $ga = a$, $\forall a \in k^*, \forall g \in G$, obtenemos la secuencia exacta corta

$$1 \to C^\bullet(G,A) \xrightarrow{i.} C^\bullet(G,k^*) \xrightarrow{\pi.} C^\bullet(G,k^*/A) \to 1. \qquad (\#)$$

Notemos que existe una identificación natural entre $C^n(G,k^*)/C^n(G,A)$ y $C^n(G,k^*/A)$ dada por

$$\begin{aligned} p : C^n(G,k^*) &\to C^n(G,k^*/A) \\ f &\to \overline{f} \end{aligned}$$

con $\overline{f} = \pi \circ f$ y $\pi : k^* \to k^*/A$. Claramente p es sobreyectiva y

$$\begin{aligned} Ker(p) &= \{f : \overline{f} = \overline{1}\} \\ &= \{f : G \times \cdots \times G \to k^* : f(g_1,\ldots,g_n) \in A, \forall g_1,\ldots,g_n \in G\} \\ &= C^n(G,A). \end{aligned}$$

Luego p induce un isomorfismo entre $C^n(G,k^*)/C^n(G,A)$ y $C^n(G,k^*/A)$, y de aquí se sigue la exactitud de la secuencia (#). Veamos cómo computar el primer *homomorfismo conexión* δ^1.

Lema 1.2.2 (Zig-Zag) *Dada una secuencia exacta corta*

$$1 \to C^{\bullet}(G,A) \xrightarrow{i.} C^{\bullet}(G,k^*) \xrightarrow{p.} C^{\bullet}(G,k^*/A) \to 1$$

entre los complejos $\{C^{\bullet}(G,A), d_A^{\bullet}\}, \{C^{\bullet}(G,K), d_K^{\bullet}\}, \{C^{\bullet}(G,k^*/A), d_{k^*/A}^{\bullet}\}$, *entonces existen transformaciones* δ^k *llamadas homomorfismos conexión y una secuencia exacta de grupos*

$$\cdots \xrightarrow{\delta^{k-1}} H^k(G,A) \xrightarrow{i_k} H^k(G,k^*) \xrightarrow{\pi_k} H^k(G,k^*/A) \xrightarrow{\delta^k} H^{k+1}(G,A) \to \cdots$$

Prueba. Es sólo de interés la construcción de $\delta^1 : H^1(G,k^*/A) \to H^2(G,A)$. Tomemos $[\varphi] \in H^1(G,k^*/A)$ y un representante cualquiera de esta clase, $\varphi \in Ker(d^1_{k^*/A})$, y consideremos el siguiente diagrama

$$\begin{array}{ccccccccc}
 & & \vdots & & \vdots & & \vdots & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \to & C^1(G,A) & \stackrel{i_1}{\to} & C^1(G,k^*) & \stackrel{p_1}{\to} & C^1(G,k^*/A) & \to & 1 \\
 & & \downarrow d^1_A & & \downarrow d^{1*}_K & & \downarrow d^1_{k^*/A} & & \\
1 & \to & C^2(G,A) & \stackrel{i_2}{\to} & C^2(G,k^*) & \stackrel{p_2}{\to} & C^2(G,k^*/A) & \to & 1 \\
 & & \downarrow d^2_A & & \downarrow d^{2*}_K & & \downarrow d^2_{k^*/A} & & \\
1 & \to & C^3(G,A) & \stackrel{i_3}{\to} & C^3(G,k^*) & \stackrel{p_3}{\to} & C^3(G,k^*/A) & \to & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \vdots & & \vdots & & \vdots & &
\end{array}$$

donde cada fila es una secuencia exacta corta. Como p_1 es sobreyectivo podemos escoger $\phi \in C^1(G,k^*)$ tal que $p_1(\phi) = \varphi$, entonces

$$p_2(d^1_{k^*}(\phi)) = d^1_{k^*/A}(p_1(\phi)) = d^1_{k^*/A}(\varphi) = 1,$$

y la exactitud de las filas implica que existe un único $\delta^1\varphi \in C^2(G,A)$ tal que $i_2(\delta^1\varphi) = \psi$ con $\psi = d^1_{k^*}(\phi)$.

Veamos que $\delta^1\varphi \in Ker(d^2_A)$. En primer lugar tenemos que $i_3(d^2_A(\delta^1\varphi)) = d^2_{k^*}(\psi) = 1$. Como i_3 es inyectiva se sigue que $d^2_A(\delta^1\varphi) = 1$ y por consiguiente $\delta^1\varphi \in Ker(d^2_A)$. Definamos

$\delta^1([\varphi]) = [\delta^1\varphi] \in H^2(G, A)$. Vemos que la clase $[\delta^1\varphi]$ no depende de ninguna de las escogencias anteriores. En primer lugar, si se escoge otro elemento σ con $p_1(\sigma) = \varphi$ entonces $p_1(\phi\sigma^{-1}) = 0$, y por la exactitud en el medio de cada fila, existe un elemento $f \in C^1(G, A)$ tal que $i_1(f) = \phi\sigma^{-1}$ y por tanto $d^1_A(f) = \delta^1\varphi(\delta^1\sigma)^{-1}$, donde $\delta^1\sigma$ es el único elemento tal que $i_2(\delta^1\sigma) = \eta = d^1_{k^*}(\sigma)$. Esto muestra que $\delta^1\varphi$ y $\delta^1\sigma$ difieren por una cofrontera y por consiguiente definen la misma clase de equivalencia en $H^2(G, A)$. En segundo lugar, veamos que si φ es una cofrontera, entonces el elemento que le corresponde de acuerdo con esta construcción es cero, y por tanto $\delta^1([\varphi])$ tampoco depende del representante escogido para la clase $[\varphi]$.

Supongamos que $\varphi = d^0_{k^*/A}(g)$ con $g \in C^0(G, k^*/A)$. Si tomamos $\psi \in C^0(G, k^*)$ tal que $p_0(\psi) = g$ entonces $d^0_{k^*}(\psi) = \gamma$ satisface $p_1(\gamma) = \varphi$. Como cualquier preimagen de φ puede usarse para computar el homomorfismo conexión, entonces si usamos γ, vemos que $\delta^1(\varphi) = 1$, ya que $d^1_{k^*}(\gamma) = 1$ (γ es una cofrontera). ■

Ahora computemos el homomorfismo conexión explícitamente. Sean $\varphi : G \to k^*/A$ y $\phi : G \to k^*$ tales que $\pi \circ \phi = \varphi$, como en la construcción anterior. Entonces tenemos que

$$\begin{aligned} d^1_{k^*}\phi(g_1, g_2) &= g_1\phi(g_2)\phi(g_1g_2)^{-1}\phi(g_1) \\ &= \phi(g_2)\phi(g_1g_2)^{-1}\phi(g_1). \end{aligned}$$

Así δ^1 está dado por $\delta^1\varphi(g_1, g_2) = \phi(g_2)\phi(g_1g_2)^{-1}\phi(g_1) \in A$ pues $i_2(\delta^1\varphi) = 1$.

En forma similar, si $\phi \in C^2(G, k^*)$ y $\varphi \in C^2(G, k^*/A)$ es tal que $\pi \circ \phi = \varphi$, se tiene que $\delta^2\varphi \in C^3(G, A)$ con

$$\delta^2\varphi(g_1, g_2, g_3) = \phi(g_2, g_3)\phi(g_1g_2, g_3)^{-1}\phi(g_1, g_2g_3)\phi(g_1, g_2)^{-1}.$$

El siguiente corolario (1.2.6) proporciona un criterio muy útil para determinar cuándo se desvanece la cohomología.

Proposición 1.2.3 *Sea A un G-módulo tal que $A^m = 1$ para algún entero $m \geq 1$. Entonces*

$$(Z^n(G, A))^m = (B^n(G, A))^m = (H^n(G, A))^m = 1, \text{ para todo } n \geq 0.$$

Prueba. Sea $f \in C^n(G,A)$ una n-cocadena. Entonces $f \in A$ si $n = 0$, y en tal caso $f^m = 1$, o f es una función de G^n en A, si $n \geq 1$ y en este caso también se tiene que $f^m = 1$. Como $((Z^n(G,A))^m = (B^n(G,A))^m = 1$, ya que son subgrupos de $C^n(G,A)$, entonces $(H^n(G,A))^m = 1$. ■

Proposición 1.2.4 *Sea H un subgrupo de G de orden m y sea $Cor : H^n(H,A) \to H^n(G,A)$ y $Res : H^n(G,A) \to H^n(H,A)$ los homorfismos correstricción y restricción. Entonces $Cor \circ Res = m$; es decir, si c es una clase de cohomología en $H^n(G,A)$ para algún G-módulo A, entonces*

$$Cor(\operatorname{Re} s(c) = c^m \in H^n(G,A), \text{ para todo } n \geq 0.$$

Prueba. Denotemos por $P^\bullet$ una resolución proyectiva para $\mathbb{Z}$. Si f es también un G-homomorfismo, entonces $g_i f(g_i^{-1}p) = g_i g_i^{-1} f(p) = f(p)$, para $1 \leq i \leq m$. Como la restricción es el mapeo inducido sobre la inclusión natural de $Hom_{\mathbb{Z}[G]}(P^\bullet, A)$ en $Hom_{\mathbb{Z}[H]}(P^\bullet, A)$, para este f, obtenemos

$$\begin{array}{ccccc} Hom_{\mathbb{Z}[G]}(P^\bullet, A) & \overset{Res}{\to} & Hom_{\mathbb{Z}[H]}(P^\bullet, A) & \overset{Cor}{\to} & Hom_{\mathbb{Z}[G]}(P^\bullet, A) \\ f & \longmapsto & f & \longmapsto & f^m \end{array}$$

De aquí se sigue que $Res \circ Cor$ es elevar a la potencia m, y también lo es sobre la cohomología de grupos. ■

Corolario 1.2.5 *Sea G un grupo finito de orden m. Entonces $(H^n(G,A))^m = 1$ para todo $n \geq 1$ y cualquier G-módulo A.*

Prueba. Sea $H = 1$. Entonces $[G : H] = m$ en la proposición anterior. Luego, para cualquier clase $c \in H^n(G,A)$ tenemos que $c^m = Cor(Res(c))$. Dado que $Res(c) \in H^n(H,A) = H^n(1,A)$, se sigue que $Res(c) = 1$, para todo $n \geq 1$. Así $c^m = 1$ para todo $n \geq 1$. ■

Corolario 1.2.6 *Sea G un grupo finito con orden relativamente primo al exponente del G-módulo A. Entonces $H^n(G,A) = 1$, para todo $n \geq 1$. En particular, si A es un grupo finito tal que $(|G|, |A|) = 1$, entonces $H^n(G,A) = 1$, para todo $n \geq 1$.*

Prueba. Esto se sigue debido a que $(H^n(G,A))^{|G|} = 1$ por el colorario anterior y $H^n(G,A)$ elevado al exponente de A es trivial por la proposición (1.2.3). ■

1.3 Representación de Grupos Finitos

Definición 1.3.1 *Sean G un grupo finito, F un campo y V un espacio vectorial sobre F. Una representación de G, es un homomorfismo de G en $GL(V)$, $\rho : G \to GL(V)$. A la dimensión de V se le denomina el grado de la representación.*

De la definición se sigue que si V es un espacio vectorial de dimensión n, entonces fijando una base para V, obtenemos un isomorfismo de $GL(V) \cong GL_n(F)$. De este modo cualquier representación de G induce una representación matricial y viceversa.

El mapeo ρ dota a V de estructura de $F[G]$-módulo: en efecto, definamos la acción de un elemento del anillo grupo sobre un elemento de V como sigue

$$(\sum_{i=1}^{n} \alpha_i g_i).v = \sum_{i=1}^{n} \alpha_i \rho(g_i) v \ .$$

Entonces, sean $g_i, g_j \in G$ y $v \in V$. Vemos que

$$\begin{aligned} (g_i g_j).v &= \rho(g_i g_j) v \\ &= (\rho(g_i) \circ \rho(g_j)).v \\ &= \rho(g_i)(\rho(g_j) v) \\ &= g_i(g_j v) \end{aligned}$$

Recíprocamente, dado un $F[G]$-módulo V obtenemos un espacio vectorial sobre F y una representanción de G como sigue. Dado que V es un $F[G]$-módulo, este es en particular un F-módulo. Para cada $g \in G$ tenemos un mapeo de V en V denotado por $\varphi(g)$, y definido por $\varphi(g)v = g \cdot v$, $\forall v \in V$, donde $g \cdot v$ es la acción dada por el elemento del anillo sobre el elemento v de V. Entonces, por los axiomas de módulo tenemos que $\forall v, w \in V$ y $\forall \alpha, \beta \in F$

$$\begin{aligned} \varphi(g)(\alpha v + \beta w) &= g(\alpha v + \beta w) \\ &= g(\alpha v) + g(\beta w) \\ &= \alpha \varphi(g) v + \beta \varphi(g) w \end{aligned}$$

Luego para cada $g \in G$, $\varphi(g)$ es una transformación lineal. El lector puede encontrar una demostración del siguiente teorema en la página 806 de [2].

Teorema 1.3.1 *Existe una biyección entre $F[G]$-módulos y los pares (V, ρ) dada por*

$$\{V \text{ un } F[G]\text{-módulo}\} \Longleftrightarrow \left\{ \begin{array}{c} V \text{ un espacio vectorial sobre } F,\ \rho : G \to GL(V) \\ \text{una representación.} \end{array} \right\}$$

Definición 1.3.2 *Sea V un $F[G]$-módulo. Un subespacio U de V es llamado G-invariante si $gu \in U$, $\forall g \in G, \forall u \in U$. Una representación V es llamada irreducible si no existen subespacios propios invariantes no triviales W de V.*

1.3.1 Ejemplos de representaciones

1.(Representación trivial) Sea V un espacio vectorial 1-dimensional sobre F. A V se le puede dotar de estructura de $F[G]$-módulo de acuerdo a la regla

$$gv = v \quad \forall g \in G, \forall v \in V.$$

Este módulo proporciona la representación

$$\begin{array}{rcl} \rho : G & \to & GL(V) \\ g & \to & I \end{array}$$

donde I es la transformación identidad.

2.(Representación regular) Sea $V = F[G]$ y consideremos este anillo como un módulo sobre sí mismo. Entonces V proporciona una representación de G de grado igual a $|G|$, si tomamos los elementos de G como una base de V, entonces para cada $g \in G$ tenemos

$$g.g_i = gg_i$$

3.(Representación signo) Sea $G = S_n$ el grupo simétrico en n símbolos y sea $V = F$, el espacio vectorial de dimensión 1. Definimos la función signo, $sgn : S_n \rightarrow GL(F)$ como:

$$\sigma \rightarrow \begin{cases} 1_F \text{ si } \sigma \text{ es par} \\ -1_F \text{ si } \sigma \text{ es impar} \end{cases}$$

Claramente sgn es un homomorfismo, por lo que F recibe estructura de G-módulo con la acción

$$\sigma x = \begin{cases} x \text{ si } \sigma \text{ es par} \\ -x \text{ si } \sigma \text{ es impar} \end{cases}$$

para $\sigma \in G, x \in F$.

4. **(Representación permutación)** Sea $n \in \mathbb{Z}^+$, $G = S_n$ y V un espacio vectorial n-dimensional sobre un campo F con base $e_1, e_2, \ldots, e_n$. La acción de G sobre V está dada para cada $\sigma \in G$ por

$$\sigma.e_i = e_{\sigma(i)} \ , \ \ 1 \leq i \leq n,$$

es decir, σ actúa permutando los elementos de la base. Esto permite obtener un homomorfismo inyectivo de S_n en $GL(V)$.

5. **(Representación estándar)** Sea $V = F^n = \{\{x_1, x_2, \ldots, x_n\} : x_i \in F\}$ y la acción de G en V, está dada por

$$\sigma(x_1, x_2, \ldots, x_n) = (x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}),$$

lo cual define un homomorfismo de grupos $S_n \rightarrow GL(F^n)$, que convierte a $V = F^n$ en un $F[S_n]$-módulo. Un submódulo importante de dimensión $n-1$ de F^n es

$$E = \left\{ (x_1, x_2, \ldots, x_n) \in F : \sum_{i=1}^{n} x_i = 0 \right\}$$

La representación asociada a este módulo se llama *representación estándar.*(ver [2]).

Si V y W son representaciones, la suma directa $V \oplus W$, y el producto tensorial $V \otimes W$, también son representaciones, dadas por $g(v \oplus w) = gv \oplus gw$ y $g(v \otimes w) = gv \otimes gw$, respectivamente.

El dual $V^* = Hom(V, F)$ de V es también una representación, definida por $\varphi^*(g) = \varphi(g^{-1}) : V^* \to V^*$ para todo $g \in G$.

Además, $Hom(V, W)$ también proporciona una representación, vía la identificación

$$Hom(V, W) = V^* \otimes W$$

Tomando cada elemento de $Hom(V, W)$ como un mapeo lineal ϕ de V en W, tenemos $(g\phi)(v) = g\phi(g^{-1}v)$ para todo $v \in V$. (ver [2]).

Notemos que la representación dual es un caso especial del anterior. Esta se obtiene si tomamos $W = \mathbb{C}$ con la representación trivial. Es decir, $gw = w$ para todo $w \in \mathbb{C}$, y por tanto V^* es un G-módulo, dado por $(g\phi)v = \phi(g^{-1}v)$.

En general el espacio vectorial de mapeos G-lineales entre dos representaciones V y W de G es justamente el subespacio $Hom(V, W)^G$ de elementos de $Hom(V, W)$ fijados bajo la acción de G. (Ver [2]).

Definición 1.3.3 *Dos representaciones de G son equivalentes si los correspondientes $F[G]$-módulos son isomorfos.*

Supongamos que $\varphi : G \to GL(V)$ y $\psi : G \to GL(W)$ son dos representaciones equivalentes. Sea $T : V \to W$ un isomorfismo de $F[G]$-módulos, en particular un isomorfismo de F-módulo (Como T es un isomorfismo de espacios vectoriales, entonces V y W tienen la misma dimensión). Entonces, para todo $g \in G, v \in V$ se tiene que $T(g.v) = gT(v)$. Por definición de la acción de los elementos del anillo, esto significa que $T(\varphi(g).v) = \psi(g)T(v)$. Es decir, $T \circ \varphi(g) = \psi(g) \circ T$, $\forall g \in G$. En particular, si se identifican V y W como espacios vectoriales, entonces dos representaciones φ y ψ de G sobre un espacio vectorial V son equivalentes sí y solo si existe $T \in GL(V)$ tal que $T \circ \varphi(g) \circ T^{-1} = \psi(g)$, $\forall g \in G$.

Definición 1.3.4 *Una subrrepresentación de una representación V es un subespacio vectorial W de V el cual es invariante bajo G.*

Definición 1.3.5 *Una representación se llama reducible si contiene al menos una subrrepresentación propia no trivial como subespacio. En caso contrario se llama irreducible.*

Lema 1.3.2 *Supongamos que V es un G-módulo que tiene un G-submódulo W y un homomorfismo de G-módulos $\phi : V \to V$ tal que $\phi(v) \in W$, $\forall v \in V$ y $\phi(w) = w$, $\forall w \in W$. Entonces $V = W \oplus Ker(\phi)$ y diremos que ϕ es la proyección sobre el submódulo W.*

Prueba. Sea $v \in V$. Entonces $v = (v) + (v - \phi(v))$, donde $\phi(v) \in W$ y $v - \phi(v) \in Ker\phi$; esto último ya que

$$\phi(v - \phi(v)) = \phi(v) - \phi(\phi(v)) = v - v = 0.$$

Por tanto $V = W + Ker\phi$. Ahora, si $v \in W \cap Ker\phi$ entonces $v \in W$ y $v \in Ker\phi$ y por tanto $v = \phi(v) = 0$. Luego $W \cap Ker\phi = (0)$, y $V = W \oplus Ker\phi$. ■

Teorema 1.3.3 *Sea W una subrrepresentación de una representación V de un grupo finito G. Entonces existe un subespacio G-invariante complementario W' de V tal que $V = W \oplus W'$.*

Prueba. Sea W' un subespacio vectorial de V tal que $V = W \oplus W'$ como espacios vectoriales, y sea $\pi_0 : V \to W$ la proyección en W. Claramente $\pi_0(v) = v$, $\forall v \in W$.

Sea

$$\begin{aligned} \pi : V &\to V \\ v &\to \frac{1}{|G|} \sum_{g \in G} g(\pi_0(g^{-1}v)). \end{aligned}$$

Veamos que π es G-lineal. Sea $h \in H$ y $v \in V$,

$$\begin{aligned} \pi(hv) &= \frac{1}{|G|} \sum_{g \in G} g(\pi_0(g^{-1}hv)) = \frac{1}{|G|} \sum_{g \in G} h(h^{-1}g)(\pi_0(g^{-1}hv)) \\ &= \frac{1}{|G|} \sum_{k \in G} hk(\pi_0(k^{-1}v)) = h\pi(v) \end{aligned}$$

Además, si $w \in W$, entonces

$$\begin{aligned} \pi(w) &= \frac{1}{|G|} \sum_{g \in G} g(\pi_0(g^{-1}w)) = \frac{1}{|G|} \sum_{g \in G} g(g^{-1}w) \\ &= \frac{1}{|G|} \sum_{g \in G} w = \frac{1}{|G|} |G| w = w. \end{aligned}$$

En conclusión $\pi : V \to V$ es un homorfismo de G-módulos tal que $\pi(v) \in W$, $\forall v \in V$ y $\pi(w) = w$, $\forall w \in W$. Por el lema anterior tenemos que $V = W \oplus Ker(\pi)$. ■

Corolario 1.3.4 *Cualquier representación es una suma directa de representaciones irreducibles.*

Lema 1.3.5 (Schur) *Sean V y W dos representaciones irreducibles de G y $\varphi : V \to W$ un homomorfismo de G-módulos. Entonces*

i) φ es un isomorfismo o φ es el homomorfismo trivial.

ii) Si $V \cong W$ entonces $\varphi = \lambda I$ para algún $\lambda \in \mathbb{C}$, donde I denota la identidad.

Prueba. Supongamos que φ es no trivial. Sabemos que $Ker\varphi$ es un submódulo de V. Como φ es no trivial, $Ker\varphi \neq V$, y dado que V es irreducible, se sigue que $Ker\varphi = 0$, y por tanto φ es inyectiva. Similarmente, $im(\varphi)$ es un submódulo de W diferente de cero; por tanto $im(\varphi) = W$ y φ es sobreyectiva.

Para demostrar (ii) tenemos que como $\mathbb{C}$ es algebraicamente cerrado, entonces φ tiene un valor propio λ, es decir, para algún $\lambda \in \mathbb{C}\,, \varphi - \lambda I$ tiene un kernel no cero, pero por (i) tenemos que $\varphi - \lambda I = 0$ y entonces $\varphi = \lambda I$. ■

Proposición 1.3.6 *Para cualquier representación V de un grupo finito G existe una descomposición*

$$V = V_1^{\oplus a_1} \oplus V_2^{\oplus a_2} \oplus \cdots \oplus V_k^{\oplus a_k}$$

donde V_i son no isomorfas representaciones irreducibles. La descomposición de V como la suma directa de k factores es única y los V_i aparecen con multiplicidad a_i.

Prueba. Por el lema de Schur, si W es otra representación de G con descomposición

$$W = W_1^{\oplus a_1} \oplus \cdots \oplus W_r^{\oplus a_r}$$

y $\varphi : V \to W$ un mapeo de representaciones, entonces el mapeo φ mapea cada factor $V_i^{\oplus a_i}$ en $W_j^{\oplus b_j}$, y por tanto $W_j \cong V_i$. Aplicando el mapeo identidad de V en V se sigue la unicidad. ■

El objetivo es describir todas las representaciones irreducibles de G, y encontrar una técnica para dar una descomposición en suma directa

$$V = V_1^{a_1} \oplus \cdots \oplus V_k^{a_k}$$

y determinar las multiplicidades a_i, para una representación arbitraria V.

Para esto introducimos la teoría de caracteres.

1.3.2 Caracteres

A lo largo de está sección trabajaremos en el campo complejo.

Definición 1.3.6 *Sea V un $\mathbb{C}[G]$-módulo. Definimos el caracter de V como la función*

$$\begin{aligned} \chi_V : G &\rightarrow \mathbb{C} \\ g &\rightarrow tr(g_V : V \rightarrow V) \end{aligned}$$

donde tr denota la traza del operador.

Por tanto, una función $\chi : G \rightarrow \mathbb{C}$ es un caracter si existe un G-módulo V tal que $\chi = \chi_V$. Notemos que $\chi_V(ghg^{-1}) = \chi_V(h)$, y por tanto χ_V es constante bajo conjugación de clases de G.

Recordemos que para calcular la traza de una transformación lineal $V \rightarrow V$ es suficiente fijar una base de V, obtener la matriz de la transformación con respecto a la base escogida, y sumar los elementos de la diagonal.

Proposición 1.3.7 (Propiedades básicas de los caracteres) *Sea V un G-módulo, y sean $g, h \in G$. Entonces:*

i) $\chi_V((1)) = \dim V$

ii) $\chi_V(g^{-1}) = \overline{\chi_V(g)}$

iii) $|\chi_V(g)| \leq \chi_V((1))$

iv) Si $V \cong W$ entonces $\chi_V = \chi_W$.

Prueba. i) $\chi_V((1))$ es la traza de la matriz identidad $V \rightarrow V$, la cual es igual a $\dim V$.

ii) Recordemos que si V es un G-módulo entonces g_V es diagonalizable. Además todos los valores propios de g_V tienes norma 1, ya que si t es el orden de $g \in G$, entonces $g^t = 1$, lo cual implica que el polinomio minimal $p(x)$ de la transformación lineal g_V divide a $x^t - 1$. En particular $p(x)$ no tiene raíces multiples, y por tanto g_V es diagonalizable. Como los valores propios satisfacen la ecuación $x^t - 1 = 0$, todos tienen norma 1.

Si $n = \dim V$, entonces la transformación lineal g_V tiene n valores propios, digamos $\lambda_1, \lambda_2, \dots, \lambda_n \in \mathbb{C}$. Luego $\chi_V(g) = tr(g_V) = \sum_{k=1}^{n} \lambda_k$. Además, λ_i^{-1}, $i = 1, \dots, n$ son los valores propios de g_V^{-1}. Como $z^{-1} = \overline{z}/|z|^2$ para todo $z \in \mathbb{C}$, tenemos que, $\lambda_k^{-1} = \overline{\lambda}_k$. De donde

$$\chi_V(g^{-1}) = \sum_{k=1}^{n} \lambda_k^{-1} = \sum_{k=1}^{n} \overline{\lambda}_k = \overline{\chi_V(g)}.$$

Además, de $\chi_V(g) = \sum_{k=1}^{n} \lambda_k$ se deduce que

$$|\chi_V(g)| \leq \sum_{k=1}^{n} |\lambda_k| = n = \dim V = \chi_V((1)),$$

lo cual prueba (iii).

iv) Sea $\varphi : V \to W$ un isomorfismo. Entonces, para todo $g \in G$, $\varphi \circ g_V = g_W \circ \varphi$, y por tanto $g_V = \varphi^{-1} \circ g_W \circ \varphi$. Así

$$\chi_V(g) = tr(g_V) = tr(\varphi^{-1} \circ g_W \circ \varphi) = tr(g_W) = \chi_W(g).$$

■

Proposición 1.3.8 *Sean V y W dos G-módulos y $g \in G$. Entonces:*

i) $\chi_{V \oplus W} = \chi_V + \chi_W$

ii) $\chi_{V \otimes W} = \chi_V \chi_W$

iii) $\chi_{V^*} = \overline{\chi_V}$

Prueba. Sea $g \in G$ y sean $\beta_1 = \{v_1, \dots, v_m\}$ y $\beta_2 = \{w_1, \dots, w_n\}$ bases de vectores propios de g_V y g_W respectivamente, con valores propios $\lambda_1, \dots, \lambda_m$ y $\mu_1, \dots, \mu_n$. Entonces

$$\begin{aligned} \chi_V(g) &= \lambda_1 + \cdots + \lambda_m \\ \chi_W(g) &= \mu_1 + \cdots + \mu_n. \end{aligned}$$

Como $\beta_1 \cup \beta_2$ es una base para $V \oplus W$, y la matriz de $g_{V\oplus W}$ con respecto a estas bases es una matriz por bloques

$$\begin{pmatrix} [g_V]_{\beta_1} & 0 \\ 0 & [g_W]_{\beta_2} \end{pmatrix}$$

obtenemos que la traza de esta matriz es la suma de las trazas de g_V y de g_W; es decir, $\chi_{V\oplus W} = \chi_V + \chi_W$.

Para la segunda afirmación, notemos que

$$g(v_j \otimes w_k) = gv_j \otimes gw_k = \lambda_j v_j \otimes \mu_k w_k = \lambda_j \mu_k (v_j \otimes w_k),$$

y por tanto $v_j \otimes w_k$ es un vector propio de $g_{V\otimes W}$ con valor propio $\lambda_j \mu_k$. Entonces

$$\chi_{V\otimes W}(g) = \sum_{j=1}^{m} \sum_{k=1}^{n} \lambda_j \mu_k = \sum_{j=1}^{m} \lambda_j \sum_{k=1}^{n} \mu_k = \chi_V(g)\chi_W(g).$$

Para la tercera afirmación, sea $\beta_1^* = \{v_1^*, \ldots, v_m^*\}$ la base de V^* dual a β_1. Notemos que

$$g_{v_j^*}(v_k) = v_j^*(g^{-1}v_k) = v_j^*(\lambda_k^{-1}v_k) = \lambda_k^{-1}v_j^*(v_k)$$

de donde $gv_j^* = \lambda_k^{-1}v_j^*$, es decir, β_1^* es una base de vectores propios de V^*. Por tanto

$$\chi_{V^*}(g) = \sum_{j=1}^{m} \lambda_j^{-1} = \sum_{j=1}^{m} \overline{\lambda_j} = \overline{\chi_V(g)}.$$

■

Notemos que si n es un entero positivo y V es un G-módulo, el caracter de $V^n = V \oplus \cdots \oplus V$ es igual a

$$\chi_V + \chi_V + \cdots + \chi_V = n\chi_V.$$

Por tanto el caracter del G-módulo $S_1^{n_1} \oplus \cdots \oplus S_r^{n_r}$ es $n_1\chi_{S_1} + \cdots + n_r\chi_{S_r}$.

Definición 1.3.7 *Sean χ y ψ dos caracteres. Definimos su producto interno como*

$$\langle \chi, \psi \rangle = \frac{1}{|G|} \sum_{g\in G} \chi(g^{-1})\psi(g) = \frac{1}{|G|} \sum_{g\in G} \overline{\chi(g)}\psi(g)$$

Además, si cambiamos a g por g^{-1} tenemos que

$$\langle \chi, \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \chi(g) \overline{\psi(g).}$$

Es decir, $\langle \chi, \psi \rangle = \langle \psi, \chi \rangle$.

Lema 1.3.9 *Sea V un G-módulo. Entonces $\varphi : V \to V$, dado por $\varphi(v) = \frac{1}{|G|} \sum_{g \in G} gv$ es un morfismo de G-módulos que es la proyección en el submódulo $V^G = \{v \in V : gv = v \ \forall g \in G\}$.*

Prueba. Claramente φ es lineal. Veamos que es un morfismo de G-módulos. Sea $h \in G$ y $v \in V$, entonces

$$\begin{aligned} \varphi(hv) &= \frac{1}{|G|} \sum_{g \in G} g(hv) = \frac{1}{|G|} \sum_{gh \in G} (gh)v = \varphi(v) \\ &= \frac{1}{|G|} \sum_{hg \in G} (hg)v = \frac{1}{|G|} \sum_{g \in G} h(gv) = h\varphi(v). \end{aligned}$$

Con esto, φ es un morfismo de G-módulos y $\varphi(v) \in V^G$, para todo $v \in V$. Por otro lado, si $v \in V^G$, entonces

$$\begin{aligned} \varphi(v) &= \frac{1}{|G|} \sum_{g \in G} gv = \frac{1}{|G|} \sum_{g \in G} v \\ &= \frac{1}{|G|} |G| \, v = v. \end{aligned}$$

Así, por el lema 1.3.2 se tiene que φ es la proyección en el submódulo V^G. ■

Recordemos que si $\phi : V \to V$ es la proyección en el submódulo W, entonces la igualdad $tr\phi = \dim W$ se sigue inmediatamente de tomar una base para W, extenderla a una base de V y considerar la matriz de ϕ con respecto a tal base.

Teorema 1.3.10 *Sean V y W G-módulos. Entonces $\langle \chi_V, \chi_W \rangle$ es un entero no negativo. Si V es un G-módulo irreducible, se verifca que $\langle \chi_V, \chi_V \rangle = 1$. Y si V y W son G-módulos irreducibles no isomorfos entonces $\langle \chi_V, \chi_W \rangle = 0$.*

Prueba.

$$\begin{aligned}
\langle \chi_V, \chi_W \rangle &= \frac{1}{|G|}\sum_{g\in G}\chi_V(g)\overline{\chi_W(g)} \\
&= \frac{1}{|G|}\sum_{g\in G}\chi_{V^*\otimes W}(g) \\
&= tr(\frac{1}{|G|}\sum_{g\in G} g_{V^*\otimes W}) \\
&= \dim((V^*\otimes W)^G) \\
&= \dim(\hom(V,W)^G).
\end{aligned}$$

Ahora, si V y W son irreducibles, por el lema de Schur, tenemos que

$$\dim(\hom(V,W)^G) = \begin{cases} 1 \text{ si } V \cong W \\ 0 \text{ si } V \ncong W \end{cases}$$

■

En términos de este producto interno, los caráteres de las representaciones irreducibles de G son ortonormales. De aquí deducimos el siguiente resultado.

Corolario 1.3.11 *El número de representaciones irreducibles de G es menor o igual que el número de clases de conjugancia.*

El siguiente objetivo es probar que no existe una función de clase, no nula y ortogonal a todos los carácteres, de modo que la igualdad se da en el corolario anterior.

Corolario 1.3.12 *Sea V un G-módulo y supongamos que $V = S_1^{n_1} \oplus \cdots \oplus S_r^{n_r}$, donde los S_j son G-módulos irreducibles no isomorfos entre sí. Entonces $n_j = \left\langle \chi_V, \chi_{S_j} \right\rangle$.*

Ejemplo 1.3.1 *Tomemos la representación regular R de G. Vemos que*

$$\chi_R(g) = \begin{cases} 0 \;\; si\ g \neq e \\ |G| \;\; si\ g = e \end{cases}$$

Si $R = \oplus V_i^{\oplus a_i}$ *, donde los* V_i *son* G*-módulos irreducibles, se sigue que*

$$a_i = \langle \chi_{Vi}, \chi_R \rangle = \frac{1}{|G|} \chi_{Vi}(e)\,|G| = \dim V_i.$$

En particular, esto prueba que *hay finitas representaciones irreducibles.* Como consecuencia se obtiene la siguiente formula

$$|G| = \dim(R) = \sum_i a_i \dim(V_i) = \sum_i \dim(V_i)^2.$$

Corolario 1.3.13 *Sea* V *un* G*-módulo y* $\langle \chi_V, \chi_V \rangle = 1$*. Entonces* V *es irreducible.*

Prueba. Supongamos que $V = S_1^{n_1} \oplus \cdots \oplus S_r^{n_r}$, donde los S_j son G-módulos irreducibles, $\forall j = 1, \ldots, n$ no isomorfos entre sí. Entonces $\langle \chi_V, \chi_V \rangle = \sum_{i=1}^{n} n_i^2 = 1$. Se tiene entonces que algún n_j es 1 y los demás son cero, y $V \cong S_j$ y por tanto V es irreducible. ■

Teorema 1.3.14 V *es un* G*-módulo irreducible si y sólo si* $\langle \chi_V, \chi_V \rangle = 1$*.*

Denotemos el centralizador de $g \in G$ por $C_G(g) = \{x \in G : gx = xg\}$ el cual es el estabilizador de g cuando G actúa en G por conjugación. Por tanto $C_G(g)$ es un subgrupo de G y el tamaño de la clase de conjugación de g es igual a $|G| \, / \, |C_G(g)|$.

Corolario 1.3.15 *Sea* $g_1, g_2, \ldots, g_r$ *una colección de representantes de las clases de conjugación de* G*. Sea* X *la tabla de caracteres de* G *vista como una matriz* $r \times r$*, y sea* C *la matriz diagonal*

$$C = \begin{pmatrix} |C_G(g_1)| & 0 & \cdots & 0 \\ 0 & |C_G(g_2)| & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & |C_G(g_r)| \end{pmatrix}$$

Entonces $\overline{X}^T X = C$*, donde* $\overline{X}^T$ *denota la conjugada transpuesta de la matriz* X*.*

Prueba. Del teorema 1.3.10 tenemos que las filas de X son ortogonales. Entonces $XC^{-1}\overline{X}^T = I$, donde C^{-1} es una matriz diagonal con entradas de la forma

$$\frac{\text{tamaño de la clase de } g}{|G|}$$

Entonces $(XC^{-1})^{-1} = \overline{X}^T = CX^{-1}$, lo cual implica que $\overline{X}^T X = C$. ∎

Corolario 1.3.16 (Ortogonalidad de las columnas) *Si G tiene r clases de conjugación y $\chi_1, \ldots, \chi_r$ es una lista completa de caracteres irreducibles entonces*

$$\sum_{i=1}^{r} \overline{\chi_i(g)}\chi_i(h) = \begin{cases} |C_G(g)| & si\ g \sim h \\ 0 & si\ g \nsim h \end{cases}$$

Definición 1.3.8 *Sea G un grupo finito. Una función de clases es una función $\theta : G \to \mathbb{C}$ que es constante en clases de conjugación de G.*

Por ejemplo, para cualquier G-módulo V, su caracter χ_V es una función de clase.

Claramente el conjunto de las funciones de clase forman una subálgebra del algebra de funciones $G \to \mathbb{C}$. En particular, la suma y el producto de funciones de clase es una función de clase.

Proposición 1.3.17 *Sean $\alpha : G \to \mathbb{C}$ y V una representación de G. Sea*

$$\varphi_{\alpha,V} = \sum \alpha(g).g : V \to V$$

Entonces $\varphi_{\alpha,V}$ es un homomorfismo de G-módulos para todo V si y sólo si α es una función de clase.

Prueba. Veamos que $\varphi_{\alpha,V}$ es G-lineal. Si $h \in G$ y $v \in V$

$$\varphi_{\alpha,V}(hv) = \sum \alpha(g).g(hv) = \sum \alpha(hgh^{-1}).hgh^{-1}(hv).$$

Sustituyendo hgh^{-1} por g se ve que la suma anterior es igual a

$$\begin{aligned} & h \sum \alpha(hgh^{-1}).g(v) \\ = \quad & h \sum \alpha(g)g(v). \end{aligned}$$

Como α es una función de clase, esta suma es igual a $h(\varphi_{\alpha,V}(v))$.

El recíproco es claro. ∎

Proposición 1.3.18 *El número de representaciones irreducibles de G es igual al número de clases de conjugancia de G.*

Prueba. Sea $\alpha : G \to \mathbb{C}$ una función de clase tal que $\langle \alpha, \chi_V \rangle = 0$, para toda representación irreducible V. Veamos que $\alpha = 0$. Consideremos

$$\varphi_{\alpha,V} = \sum \alpha(g) \cdot g : V \to V.$$

Por el lema de Schur, $\varphi_{\alpha,V} = \lambda I$. Si $n = \dim V$, entonces

$$\begin{aligned}
\lambda &= \frac{1}{n} traza(\varphi_{\alpha,V}) \\
&= \frac{1}{n} \sum \alpha(g) \chi_V(g) \\
&= \frac{|G|}{n} \overline{\langle \alpha, \chi_{V^*} \rangle} \\
&= 0.
\end{aligned}$$

Luego $\varphi_{\alpha,V} = 0$ ó $\sum \alpha(g) \cdot g = 0$ para cualquier representación V de G. En particular, si tomamos $V = R$ la representación regular, pero tenemos que en R los elementos $g \in G$, pensados como elementos de $End(R)$, son linealmente independientes. Por ejemplo, los elementos $\{g(e)\}$ son todos independientes. Así $\alpha(g) = 0$ para todo g, como se quería probar. ■

1.3.3 Grupos Cíclicos

Proposición 1.3.19 *Sea G un grupo cíclico de orden n, $G = \langle a \rangle$, y sea $\zeta \in \mathbb{C}$ una raíz n-ésima primitiva de la unidad. Para cada $j = 0, 1, \ldots, n-1$, sea V_j el espacio vectorial de dimensión 1 generado por v_j y sea una acción en V_j definida por*

$$av_j = \zeta^j v_j \qquad \#$$

Entonces $V_0, \ldots, V_{n-1}$ es una lista completa de G-módulos irreducibles.

Prueba. Los G-módulos irreducibles de dimensión 1 se pueden identificar con los homomorfismos de $G \to \mathbb{C}^*$. En el casocuando G es cíclico de orden n, existen exactamente n diferentes homomorfismo dados por

$$\begin{aligned} G &\to \mathbb{C}^* \\ a &\to \zeta^i, \end{aligned}$$

para $i = 0, 1, \ldots, n-1$. Identificando estos homomorfismos como módulos obtenemos los definidos en (1.3.18), los cuales son irreducibles por tener dimensión 1, y son no isomorfos, ya que se tiene uno por cada homomorfismo, y dado que el orden de G es n, entonces hay exactamente n homomorfismos distintos. Además, $n = |G| = \sum_{i=0}^{n-1} (\dim V_i)^2$. Tenemos por tanto una lista completa de G-módulos. ■

Ejemplo 1.3.2 *Sea $n = 5$ y $G = \mathbb{Z}_5$ el grupo cíclico de orden 5, digamos que $G = \left\langle a : a^5 = 1 \right\rangle$. Como G es abeliano, cada clase de conjugación de G tiene exactamente un elemento. Sea $\zeta \in \mathbb{C}$ una raíz primitiva quinta de la unidad. Usando la proposición anterior obtenemos la siguiente tabla de caracteres*

C_5	1 1	1 a	1 a^2	1 a^3	1 a^4
χ_{V_0}	1	1	1	1	1
χ_{V1}	1	ζ	ζ^2	ζ^3	ζ^4
χ_{V2}	1	ζ^2	ζ^4	ζ	ζ^3
χ_{V3}	1	ζ^3	ζ	ζ^4	ζ^2
χ_{V4}	1	ζ^4	ζ^3	ζ^2	ζ

Capítulo 2

Clasificación de las álgebras G-graduadas

2.1 Introducción

Recordemos que si G es un grupo y W un álgebra sobre un anillo conmutativo y unitario R, entonces W es una G-álgebra graduada si existe una G-graduación $W = \oplus_{g \in G} W_g$ en la cual cada sumando W_g es un R-módulo libre de rango 1. Recordemos que W no tiene *divisores de cero monomiales* si para todo par de elementos no nulos w_a, w_b en W_a y W_b se cumple que $w_a w_b \neq 0$.

Escojamos para cada R-módulo W_g un generador v_g cualquiera. Entonces el conjunto $B = \{v_g : g \in G\}$ es una base libre para W y la estructura multiplicativa del álgebra W quedará determinada en esta base por una función

$$\begin{aligned} C_B : G \times G &\rightarrow A \subset R \\ v_a v_b &\rightarrow C_B(a,b) v_{ab}, \end{aligned}$$

donde $A \subset R$ denota un subdominio de R.

Nota 2.1.1 *A lo largo de este trabajo R será igual a los reales o complejos, que denotaremos por k cuando se quiera hacer referencia a uno cualquiera de estos campos, y G será un grupo finito.*

Con el fin de analizar la no conmutatividad y no asociatividad en este tipo de álgebras definimos, con respecto a la base B, las siguientes funciones de conmutatividad y asociatividad, q y r:

$$\begin{aligned} q(a,b) &= C(a,b)C(b,a)^{-1} \\ r(a,b,c) &= C(b,c)C(ab,c)^{-1}C(a,bc)C(a,b)^{-1}, \end{aligned}$$

donde el exponente " -1" denota el inverso multiplicativo en el campo k. Y para cualquier grupo G, en general, se verifica fácilmente que $v_a(v_bv_c) = r(a,b,c)(v_av_b)v_c$. Si G es abeliano, vemos inmediatamente que $v_av_b = q(a,b)v_bv_a$.

Recordemos la noción de morfismo en esta categoría.

Definición 2.1.1 *Un morfismo entre álgebras G-graduadas $W = \oplus_{g\in G}W_g$ y $V = \oplus_{g\in G}V_g$ es un morfismo (unitario) de k-álgebras $\phi : W \longrightarrow V$ el cual satisface $\phi(W_g) \subset V_g$, para todo $g \in G$.*

Es fácil ver que esta definición equivale a que existan bases $\{w_g : g \in G\}$, $\{v_g : g \in G\}$, para W y V, respectivamente, tales que $W_g = kw_g$ y $V_g = kv_g$, y un morfismo de k-álgebras $\phi : W \to V$ que cumpla que $\phi(v_g) = \varphi(g)w_g$, para una cierta función $\varphi : G \to k$. Es claro también que ϕ es un isomorfismo sí y sólo si $\varphi(g) \neq 0$ para todo $g \in G$, ya que por ser W y V espacios vectoriales de la misma dimensión, ϕ es biyectiva si y solo si es inyectiva, y esto ocurre si y solo si $\phi(v_g) = \varphi(g)w_g$ no es el vector cero.

El problema de clasificación de estas álgebras admite al menos tres posibles versiones.

1. W y V pueden ser *isomorfas como k-álgebras graduadas*, es decir, si existen $\phi : W \longrightarrow V$ y $\psi : V \longrightarrow W$ morfismos como en la definición anterior, tales que $\phi\psi$ y $\psi\phi$ sean la identidad.

2. W y V pueden ser isomorfas como k-álgebras en un sentido general, olvidando la graduación; es decir, sin que se cumpla la condición $\phi(W_g) \subset V_g$.

3. W y V admiten graduaciones (posiblemente distintas a las originales) para las cuales W y V resulten ser isomorfas como álgebras graduadas. En forma precisa, existen graduaciones $W = \oplus_{g\in G}W'_g$ y $V = \oplus_{g\in G}V'_g$, y un isomorfismo de k-álgebras $\phi : W \longrightarrow V$ el cual satisface $\phi(W'_g) \subset V'_g$, para todo $g \in G$.

Nuestro primer teorema de clasificación es el siguiente.

Teorema 2.1.1 *Sean $V = \oplus_{g\in G}V_g$ y $W = \oplus_{g\in G}W_g$ dos k-álgebras G-graduadas. Fijemos bases $B_1 = \{v_g : g \in G\}$ y $B_2 = \{w_g : g \in G\}$ para V y W, respectivamente, de tal forma que referidas* *a estas bases, las constantes de estructura para V y W sean C_1 y C_2. Entonces V es isomorfa a W como k-álgebras graduadas, sí y sólo si la función $C_1C_2^{-1}$ con $(a,b) \longmapsto C_1(a,b)(C_2(a,b))^{-1}$ está en el kernel de $d^2 : C^2(G,k^*) \to C^3(G,k^*)$; es decir, $d^2(C_1C_2^{-1}) = 1$, y además se verifica que $[C_1C_2^{-1}] = 1$ en $H^2(G,k^*)$.*

Nota 2.1.2 *Si V y W son asociativas, con constantes de estructura $C_1, C_2 : G \times G \to k^*$, entonces $d^2C_1 = d^2C_2 = 1$, ya que como notamos en (1.2)*

$$d^2C_i(a,b,c) = r_i(a,b,c) = 1, \;\; i = 1,2.$$

En este caso cada C_i define un elemento en $H^2(G,k^*)$, y la condición $[C_1C_2^{-1}] = 1$ de la proposición anterior es equivalente a que $[C_1] = [C_2]$ en $H^2(G,k^*)$.

Prueba. Escribamos cada componente homogénea como $V_g = kv_g$ y $W_g = kw_g$. Supongamos que V y W son isomorfas como k-álgebras graduadas. Por definición, existe un isomorfismo de k-álgebras $\phi : V \to W$ que envía a cada vector v_g en $\varphi(g)w_g$, donde, φ es una función $\varphi : G \to k^*$, es decir, tal que $\varphi(g) \neq 0$ para todo $g \in G$. Por la inyectividad de ϕ. Por ser ϕ un homomorfismo de k-álgebras, se cumple que

$$\begin{aligned} \phi(v_a v_b) &= \phi(v_a)\phi(v_b) \\ \phi(C_1(a,b)v_{a+b}) &= \varphi(a)w_a\varphi(b)w_b \\ C_1(a,b)\varphi(ab)w_{a+b} &= \varphi(a)\varphi(b)C_2(a,b)w_{a+b}. \end{aligned}$$

Se sigue que

$$C_1(a,b)C_2^{-1}(a,b) = \varphi(a)\varphi(ab)^{-1}\varphi(b). \tag{2.1}$$

Notemos que $d^1\varphi(a,b) = \varphi(b)\varphi^{-1}(ab)\varphi(a)$ y por tanto $C_1C_2^{-1}$ pertenece a la imagen de $d^1 : C^1(G,k^*) \to C^2(G,k^*)$. Luego $d^2(C_1C_2^{-1}) = 1$ y $[C_1C_2^{-1}] = 1$ en $H^2(G,k^*)$.

Recíprocamente, si $d^2(C_1C_2^{-1}) = 1$ y $[C_1C_2^{-1}] = 1$ en $H^2(G,k^*)$, entonces existe $\varphi : G \to k^*$ tal que $d^1\varphi = C_1C_2^{-1}$ y por consiguiente se cumple la ecuación (2.1). La función $\phi : V \to W$ definida en las bases B_1 y B_2 por $\phi(v_g) = \varphi(g)w_g$ es entonces un homomorfismo de k-álgebras, que es isomorfismo, ya que ϕ es inyectiva y V y W son espacios vectoriales de la misma dimensión

$|G|$. ∎

Corolario 2.1.2 *Sea $W = \oplus_{g\in G} W_g$ una k-álgebra G-graduada, B y B' bases para W, C, y C' las constantes de estructura de W con respecto a estas bases, y sean r y r' las correspondientes funciones de asociatividad. Entonces $r = r'$, es decir, las funciones de asociatividad de W no dependen de las bases escogidas.*

Prueba. Sean $B_1 = \{w_g : g \in G\}$ y $B_2 = \{w'_g : g \in G\}$. La función identidad $I : W \longrightarrow W$ es trivialmente un isomorfismo graduado de álgebras. Si en el teorema anterior hacemos $W = V$, vemos que $[C'C^{-1}] = 1$ y por tanto $C'C^{-1} \in im(d^1)$. Luego, $d^2(C'C^{-1}) = 1$ y en consecuencia $r' = d^2(C') = d^2(C) = r$. ∎

Notemos ahora que si C_1 y C_2 toman valores en un subgrupo A del grupo multiplicativo k^*, entonces $C_1C_2^{-1} \in C^2(G, A)$. Luego, en caso de ocurrir que $d^2(C_1C_2^{-1}) = 1$, tiene sentido hablar de la clase $[C_1C_2^{-1}] \in H^2(G, A)$. El siguiente teorema nos proporciona un criterio en términos de $H^2(G, A)$ para determinar si V y W son isomorfas. Esto representa una ventaja, ya que en muchas situaciones de interés A será un subgrupo *finito* del grupo multiplicativo de k^*.

Teorema 2.1.3 *$\phi : V \to W$ es un isomorfismo de k-álgebras, si y sólo si $d^2(C_1C_2^{-1}) = 1$, y $[C_1C_2^{-1}] \in \ker(i^2)$, donde $i_2 : H^2(G, A) \to H^2(G, k^*)$ denota el homomorfismo inducido en la cohomología por la inclusión $i : A \to k^*$.*

Prueba. Consideremos la secuencia exacta corta

$$1 \to A \xrightarrow{i} k \xrightarrow{\pi} k^*/A \to 1.$$

Esta secuencia induce otra secuencia exacta corta de complejos

$$1 \to C^\bullet(G, A) \xrightarrow{i_\bullet} C^\bullet(G, k^*) \xrightarrow{\pi_\bullet} C^\bullet(G, k^*/A) \to 1 \qquad ((*))$$

donde hemos identificado al cociente $C^\bullet(G, k^*)/C^\bullet(G, A)$ con $C^\bullet(G, k^*/A)$ vía el ismorfismo que envía a la clase de un elemento $h : G \to k^*$ en $\pi \circ h$. Por el lema del zig-zag, existe una secuencia exacta larga en cohomología

$$\cdots \to H^1(G, k^*) \xrightarrow{\pi_1} H^1(G, k^*/A) \xrightarrow{\delta} H^2(G, A) \xrightarrow{i_2} H^2(G, k^*) \to \cdots$$

Por la proposición anterior, V y W son isomorfas como k-álgebras graduadas sii $d^2(C_1C_2^{-1}) = 1$, y $[C_1C_2^{-1}] = 1$ en $H^2(G,k^*)$. Y esto último ocurre si y sólo si $i^2([C_1C_2^{-1}]) = 1$. ■

Como habíamos visto en el ejemplo 1.2.1, si G denota un grupo cíclico de orden n es cierto que $H^2(G,\mathbb{C}^*) = \mathbb{C}^*/(\mathbb{C}^*)^n = \{1\}$. De aquí que si V y W son álgebras G-graduadas *asociativas,* con constantes de estructura $C_1, C_2 : G \times G \to A \subset \mathbb{C}^*$, entonces $[C_1][C_2]^{-1} = 1$ y por tanto son isomorfas. Se verifica inmediatamente que $\mathbb{C}[t]/(t^n - 1) = \oplus_{r=0}^{n-1}\mathbb{C}t^r$ es un representante de la única clase de isomorfismos.

Si $k = \mathbb{R}$, entonces $H^2(G,\mathbb{R}^*) = \{1\}$, si n es impar, y es igual al grupo $\{1,-1\}$, si n es par. En el primer caso existe una sóla álgebra asociativa real, $\mathbb{R}[t]/(t^n - 1)$, y en el segundo a lo sumo dos. No es difícil ver que en este segundo caso hay exactamente dos no isomorfas: $\mathbb{R}[t]/(t^n - 1)$ y $\mathbb{R}[t]/(t^n + 1)$.

Por otro lado, si V y W son álgebras G-graduadas sobre un grupo finito G, con constantes de estructura $C_1, C_2 : G\times G \to A$, donde $|A|$ y $|G|$ sean relativamente primos, entonces del corolario (1.2.6) se sigue que $H^2(G,A) = \{1\}$. Del teorema anterior se sigue que si $d^2(C_1C_2^{-1}) = 1$ entonces V y W son isomorfas como álgebras graduadas. Pero $d^2(C_1C_2^{-1}) = d^2(C_1)d^2(C_2)^{-1} = r_1r_2^{-1}$, donde r_i es la función de asociatividad de C_i. Por tanto, $r_1 = r_2$ si y śolo si V y W son isomorfas. Hemos demostrado el siguiente teorema.

Teorema 2.1.4 (Primer teorema de clasificación) *1. Sobre los complejos hay exactamente una sola álgebra $\mathbb{Z}_n$-graduada* asociativa*, $\mathbb{C}[t]/(t^n - 1)$.*

2. *Sobre los números reales hay una sola álgebra $\mathbb{Z}_n$-graduada asociativa, $\mathbb{R}[t]/(t^n - 1)$, si n es impar, y exactamente dos no isomorfas, $\mathbb{R}[t]/(t^n - 1)$ y $\mathbb{R}[t]/(t^n + 1)$, si n es par.*

3. *Sean $W^1 = \oplus_{g\in G}W_g^1$, y $W^2 = \oplus_{g\in G}W_g^2$, álgebras graduadas sobre un grupo finito G. Fijemos bases B_1 y B_2 para W_1 y W_2, respectivamente. Sean $C_1, C_2 : G\times G \to A \subset k^*$ las constantes de estructura referidas a estas bases, y sean r_1,$r_2 : G^3 \to A$ las correspondientes funciones de asociatividad. Entonces, si $|A|$ y $|G|$ son enteros relativamente primos, se tiene que W^1 y W^2 son isomorfas como álgebras graduadas si y sólo si $r_1 = r_2$.*

4. *En particular, si W^1 y W^2 son* asociativas*, y si $|A|$ y $|G|$ son enteros relativamente primos, entonces W^1 y W^2 son isomorfas como álgebras graduadas, en cuyo caso podemos tomar como respresentante de la única clase de equivalencia al anillo grupo $k[G]$, donde las*

constantes de estructura $C : G \times G \to A$ es la función trivial $(a, b) \longmapsto C(a, b) = 1$, para todo $a, b \in G$.

2.2 Álgebras asociativas

El resultado central que nos permitirá relacionar las k-álgebras graduadas con cocientes del grupo anillo, es el siguiente.

Teorema 2.2.1 *Sea $W = \oplus_{g \in G} W_g$ una k-álgebra graduada asociativa, B una base fija y $C : G \times G \to A$ las constantes de estructura de W con respecto a esta base. Sea $A \times_C G$ la extensión de A por G construída en el ejemplo 1.1.1. Sea $R = k\,[A \times_C G]$ el anillo grupo sobre $A \times_C G$, y definamos el subespacio vectorial I generado por todos los elementos de la forma $I = \langle (\alpha, g) - \alpha(1, g) : \alpha \in A, g \in G \rangle$. Entonces $I \subset R$ es un ideal bilateral y R/I es una k-álgebra isomorfa a W.*

Prueba. Veamos que I es un ideal a izquierda, lo cual basta verificarlo en los generadores. Fijemos $(\beta, b) \in R$. Entonces

$$\begin{aligned}(\beta, b)((\alpha, a) - \alpha(1, a)) &= (\beta, b)(\alpha, a) - \alpha(\beta, b)(1, a) \\ &= (\beta a C(b, a), ab) - \alpha(\beta C(b, a), ab)\end{aligned}$$

Notemos que

$$(\beta C(b, a), ab) - \beta C(b, a)(1, ba) \in I, \tag{1}$$

$$(\alpha\beta C(b, a), ab) - \alpha\beta C(b, a)(1, ba) \in I. \tag{2}$$

Multiplicando a izquierda la ecuación (1) por α obtenemos

$$\alpha(\beta C(b, a), ab) - \alpha\beta C(b, a)(1, ba) \in I. \tag{3}$$

Luego $(2) - (3) \in I$. Esto es,

$$\begin{aligned}&(\alpha\beta C(b, a), ba) - \alpha\beta C(b, a)(1, ab) - \alpha(\beta C(b, a), ab) - \alpha\beta C(b, a)(1, ba) \\ = \; &(\beta a C(b, a), ab) - \alpha(\beta C(b, a), ab) \in I.\end{aligned}$$

Similarmente se prueba que I es un ideal a derecha, de lo cual se concluye que I es un ideal bilateral. Ahora sea $(\alpha, a) \in A \times_C G$ y definamos la función

$$\begin{aligned} \varphi : A \times_C G &\rightarrow W^* \\ (\alpha, a) &\rightarrow \alpha v_a \end{aligned}$$

donde W^* denota el conjunto de las unidades de W, es decir los elementos $w \in W$ para los cuales existe w^{-1} tal que $ww^{-1} = w^{-1}w = 1$. Veamos que φ es un homomorfismo de grupos.

$$\varphi((\alpha, a)(\beta, b)) = \varphi(\alpha\beta C(a, b), ab) = \alpha\beta C(a, b)v_{ab}$$

Por otro lado

$$\varphi(\alpha, a)\varphi(\beta, b) = \alpha v_a \beta v_b = \alpha\beta C(a, b)v_{ab}$$

Entonces

$$\begin{aligned} \varphi((\alpha, a)(\beta, b)) &= \varphi(\alpha, a)\varphi(\beta, b) \text{ y} \\ \varphi(\sum_{\lambda \in K} \lambda_{(\alpha,a)}(\alpha, a)) &= \sum_{\lambda \in K} \lambda_{(\alpha,a)}\alpha v_a. \end{aligned}$$

La propiedad universal del anillo grupo permite extender φ a una función k-lineal $\varphi : R \rightarrow W$. Veamos ahora que $I \subset Ker(\varphi)$. Notemos primero que

$$\begin{aligned} \varphi((\alpha, a) - \alpha(1, a)) &= \varphi(\alpha, a) - \varphi(\alpha(1, a)) \\ &= \varphi(\alpha, a) - \alpha\varphi(1, a) \\ &= \alpha v_a - \alpha 1.v_a \\ &= \alpha v_a - \alpha v_a \\ &= 0, \end{aligned}$$

Esto permite extender φ al cociente $\varphi : R/I \rightarrow W : \varphi(\sum \lambda_{(\alpha,a)}(\alpha, a)^{-}) = \sum \lambda_{(\alpha,a)}\alpha v_a$, donde "$-$" denota una clase de equivalencia. Por otro lado definamos la inversa de φ, como la función

k-lineal

$$\begin{aligned} \phi : W &\rightarrow R/I \\ v_a &\rightarrow (1,a)^- \end{aligned}$$

Veamos que ϕ es un homomorfismo de k-álgebras.

$$\begin{aligned} \phi(\sum_{a\in G} \lambda_a v_a \sum_{b\in G} \lambda_b v_b) &= \phi(\sum_{a,b\in G} \lambda_a \lambda_b C(a,b) v_{ab}) \\ &= \phi(\sum_{g\in G} (\sum_{a+b=g} C(a,b)\lambda_a\lambda_b) v_{ab}) \\ &= \sum_{g\in G} (\sum_{a+b=g} C(a,b)\lambda_a\lambda_b)(1,g)^- \end{aligned}$$

Por otro lado

$$\begin{aligned} \phi(\sum_{a\in G} \lambda_a v_a)\phi(\sum_{b\in G} \lambda_b v_b) &= (\sum_{a\in G} \lambda_a (1,a)^-)(\sum_{b\in G} \lambda_b (1,b)^-) \\ &= (\sum_{a,b\in G} \lambda_a\lambda_b (C(a,b),ab)^-) \\ &= \sum_{g\in G} (\sum_{a+b=g} \lambda_a\lambda_b)(C(a,b),g)^- \\ &= \sum_{g\in G} (\sum_{a+b=g} \lambda_a\lambda_b) C(a,b)(1,g)^- \end{aligned}$$

Finalmente, veamos que $\phi \circ \varphi = Id$ y $\varphi \circ \phi = Id$.

$$\begin{aligned} \varphi(\phi(\sum_{a\in G} \lambda_a v_a)) &= \phi(\sum_{a\in G} \lambda_a (1,a)^-) = \sum_{\lambda\in K} \lambda_{(1,a)} v_a = \sum_{a\in G} \lambda_a v_a \\ \phi(\varphi(\sum_{\lambda\in K} \lambda_{(\alpha,a)}(\alpha,a)^-)) &= \phi(\sum_{\lambda\in K} \lambda_{(\alpha,a)} \alpha v_a) = \sum_{a\in G} \lambda_{(\alpha,a)}(\alpha,a)^- \end{aligned}$$

Por tanto φ es un isomorfismo. ■

2.3 Clasificación de álgebras asociativas en el caso complejo.

Teorema 2.3.1 *Sea $W = \oplus_{g\in G} W_g$ una $\mathbb{C}$-álgebra G-graduadad y asociativa. Sea B una base y $C : G \times G \rightarrow A \subset \mathbb{C}$ las constantes de estructura con respecto a B. Sea $R = \mathbb{C}[A \times_C G]$. Entonces R es la representación regular de $A \times_C G$.*

Prueba. Sabemos que $R = V_1^{a_1} \oplus \cdots \oplus V_r^{a_r}$, donde cada V_i es una representación irreducible de $A \times_C G$. Por tanto

$$\chi_R(g) = \begin{cases} 0 \text{ si } g \neq 1 \\ |A \times_C G| \text{ si } g = 1 \end{cases}$$

Así, tenemos que

$$\begin{aligned} a_i &= \langle \chi_R, \chi_{V_i} \rangle = \frac{1}{|A \times_C G|} \sum_{g \in G} \overline{\chi_R(g)} \chi_{V_i}(g) \\ &= \frac{1}{|A \times_C G|} |A \times_C G| \, \chi_{V_i}(1) \\ &= \dim V_i. \end{aligned}$$

■

Teorema 2.3.2 *(Con la notación del teorema anterior) Existe un ismorfismo de $\mathbb{C}$-álgebras (olvidando la graduación)*

$$\begin{aligned} \varphi : \mathbb{C}[A \times_C G] &\rightarrow \oplus_{i=1}^r Hom_{\mathbb{C}}(V_i, V_i) \\ s &\mapsto (\psi_i)_{i=1,\ldots,r} \end{aligned}$$

donde $\psi_i : V_i \rightarrow V_i$ es el mapeo multiplicación por s.

Prueba. Claramente φ es un $\mathbb{C}$-homomorfismo de álgebras. Por otro lado, si $s.v_i = 0$ para todo $v_i \subset V_i \subset R$, $i = 1, \ldots, r$, entonces $st = 0$ para todo $t \in R$. Luego $s = 0$, lo cual muestra que φ es inyectivo. Notemos que

$$\dim_{\mathbb{C}} im(\varphi) = \dim_{\mathbb{C}} R = \dim_{\mathbb{C}}(\oplus_{i=1}^r Hom_{\mathbb{C}}(V_i, V_i))$$

Por tanto $im(\varphi) = \oplus_{i=1}^r Hom_{\mathbb{C}}(V_i, V_i)$, y en consecuencia φ es un isomorfismo. ■

Corolario 2.3.3 *W es isomorfa como $\mathbb{C}$-álgebra a un producto finito de álgebras de matrices $Mat_{n_i \times n_i}(\mathbb{C})$, donde $n_i = \dim V_i$.*

Prueba. Sea $J = \varphi(I)$, donde φ e I son como en el teorema 2.2.1. Entonces J se descompone como $J = J_1 \times \cdots \times J_r$, donde $J_i \subset Hom_{\mathbb{C}}(V_i, V_i)$ es un ideal bilateral. Por tanto

$$W \cong R/I = \oplus_{i=1}^{r} Hom_{\mathbb{C}}(V_i, V_i)/J_i.$$

Como cada una de las álgebras $Hom_{\mathbb{C}}(V_{ij}, V_{ij})$ es simple, se sigue que $J_i = 0$ ó $J_i = Hom_{\mathbb{C}}(V_i, V_i)$. Esto implica que

$$W \cong \oplus_{(ij)} Hom_{\mathbb{C}}(V_{ij}, V_{ij})$$

donde la suma ocurre sobre aquellos sumandos ij para los cuales $J_{ij} = (0)$. ■

De este teorema se siguen inmediantamente los siguientes dos corolarios.

Corolario 2.3.4 *Sea $W = \oplus_{g \in G} \mathbb{C} W_g$ una $\mathbb{C}$-álgebra G-graduada y asociativa. Entonces W es conmutativa si y solo si cada $n_{ij} = \dim V_{ij} = 1$ y por tanto $W \simeq \mathbb{C} \times \cdots \times \mathbb{C}$.*

Corolario 2.3.5 *Sea $W = \oplus_{g \in G} \mathbb{C} W_g$ una $\mathbb{C}$-álgebra G-graduada y asociativa. Entonces W es un anillo de división si y sólo si $W \cong \mathbb{C}$.*

2.4 Clasificación de álgebras asociativas en el caso real.

Sea G un grupo finito y sea R la representación regular real de $\mathbb{R}[G]$ sobre un espacio real de dimensión finita. Ya vimos que

$$R = V_1^{a_1} \oplus \cdots \oplus V_r^{a_r}$$

En este caso los caracteres forman una base ortogonal (pero no ortonormal) para $\mathbb{R}$.(ver la referencia [2]). Tenemos entonces que $\dim_{\mathbb{R}} V_i = \left\langle \chi_R, \chi_{V_i} \right\rangle = a_i \left\langle \chi_{V_i}, \chi_{V_i} \right\rangle$, para todo $i = 1, \ldots, r$. Por otro lado, veamos que

$$\left\langle \chi_{V_i}, \chi_{V_i} \right\rangle = \dim_{\mathbb{R}}(Hom_{\mathbb{R}}(V_i, V_i)^G).$$

Para esto utilizamos la identificación $Hom_{\mathbb{R}}(V_i, V_i)^G \cong (V_i^* \otimes V_i)^G$ y aplicamos la formula de proyección. Así,

$$\begin{aligned}
\dim Hom_{\mathbb{R}}(V_i, V_i)^G &= \dim_{\mathbb{R}}(V_i^* \otimes V_i)^G \\
&= \frac{1}{|G|}\sum_{g\in G}\chi_{V_i^*\otimes V_i}(g) \\
&= \frac{1}{|G|}\sum_{g\in G}\overline{\chi_{V_i}(g)}\chi_{V_i}(g) \\
&= \frac{1}{|G|}\sum_{g\in G}\chi_{V_i}(g)\chi_{V_i}(g) \\
&= \left\langle \chi_{V_i}, \chi_{V_i}\right\rangle .
\end{aligned}$$

Ahora, sea $D_i = Hom_{\mathbb{R}}(V_i, V_i)^G$. Este anillo consiste precisamente de los G-homomorfismos de V_i. Como cada V_i es irreducible bajo la acción de G, entonces el lema de Schur garantiza que D_i *es un anillo de división.* Cada V_i tiene estructura natural de D_i-módulo, dada por $\phi \cdot v_i = \phi(v_i)$, que restringido a $\mathbb{R}$, coincide con la multiplicación escalar. Como $\mathbb{R} \hookrightarrow D_i \hookrightarrow V_i$ vemos que

$$\dim_{D_i}(V_i)\dim_{\mathbb{R}}(D_i) = \dim_{\mathbb{R}}(V_i),$$

y obtenemos la relación

$$\begin{aligned}
a_i &= \frac{\left\langle \chi_R, \chi_{V_i}\right\rangle}{\left\langle \chi_{V_i}, \chi_{V_i}\right\rangle} = \frac{\dim_{\mathbb{R}} V_i}{\dim_{\mathbb{R}}(Hom_{\mathbb{R}}(V_i, V_i)^G)} \\
&= \frac{\dim_{\mathbb{R}} V_i}{\dim_{\mathbb{R}}(D_i)} = \dim_{D_i}(V_i).
\end{aligned}$$

Entonces podemos establecer un homomorfismo inyectivo entre los espacios vectoriales $\mathbb{R}[G]$ y $\oplus Hom_{D_i}(V_i, V_i)$, que es sobreyectivo ya que sus dimensiones coinciden. En efecto,

$$\begin{aligned}
\dim_{\mathbb{R}}(\oplus Hom_{D_i}(V_i, V_i)) &= \sum(\dim_{D_i} V_i)^2 \dim_{\mathbb{R}} D_i \\
&= \sum a_i^2 \dim_{\mathbb{R}} D_i \\
&= \dim_{\mathbb{R}}(\mathbb{R}[G]).
\end{aligned}$$

Hemos demostrado el siguiente teorema.

Teorema 2.4.1 *El grupo anillo $\mathbb{R}[G]$ es isomorfo a una suma directa finita de $\mathbb{R}$-álgebras de la forma $Hom_{D_i}(V_i, V_i)$.*

Como corolario obtenemos el siguiente teorema de clasificación en el caso real.

Teorema 2.4.2 *Sea $W = \oplus_{g\in G} W_g$ una $\mathbb{R}$-álgebra G-graduada y asociativa. Entonces W es isomorfa a un álgebra de la forma $L = \oplus_{i=1}^{r} Hom_{D_i}(V_i, V_i)$, donde D_i denota uno de los siguientes anillos de división: $\mathbb{R}, \mathbb{C}$, o $\mathbb{H}$, el anillo de los cuaterniones.*

Prueba. Sabemos que $W \simeq \mathbb{R}[A \times_C G]/J$, para un cierto ideal bilateral J. Del teorema anterior se sigue que

$$\mathbb{R}[A \times_C G]/J \simeq \oplus_{i=1}^{n} Hom_{D_i}(V_i, V_i)/J_i,$$

donde $J \simeq J_1 \times \cdots \times J_n$, con $D_i = Hom_{\mathbb{R}}(V_i, V_i)^{A\times_C G}$ es un anillo de división asociativo sobre los reales. Pero las únicas $\mathbb{R}$-álgebras de división (asociativas) sobre los reales son $\mathbb{R}, \mathbb{C}$ y $\mathbb{H}$ de donde se sigue el teorema. ■

2.5 Clasificación de álgebras complejas no asociativas

En esta sección daremos una clasificación completa de todas las álgebras complejas G-graduadas, *no necesariamente asociativas,* sobre grupos cíclicos finitos, para las cuales su función de asociatividad r es simétrica en las dos primeras componentes. Es decir, satisface $r(a, b, c) = r(b, a, c)$, para todo $a, b, c \in G$.

Comenzaremos haciendo una discusión general.

Sea G un grupo abeliano finito, $W = \oplus_{g\in G} W_g$ un álgebra G-graduada y $B = \{v_g : g \in G\}$ una base cualquiera para W. Consideremos el operador lineal T_g, con $g \in G$, "multiplicación a izquierda por v_g" de W en W. Es decir,

$$\begin{aligned} T_g : W &\rightarrow W \\ x &\rightarrow v_g \cdot x \end{aligned}$$

Entonces, si a y b son elementos de G, al aplicar los operadores T_a y T_b en cualquier vector v_g

de la base B se obtiene

$$\begin{aligned} T_a(T_b(v_g)) &= T_a(v_b v_g) \\ &= v_a(v_b v_g) \\ &= r(a,b,g)(v_a v_b)v_g \\ &= r(a,b,g)C(a,b)v_{ab}v_g \\ &= r(a,b,g)C(a,b)T_{ab}(v_g) \end{aligned}$$

Por tanto

$$T_{ab}(v_g) = r(a,b,g)^{-1}C(a,b)^{-1}T_a(T_b(v_g)) \tag{2.2}$$

En forma similar, si intercambiamos a por b se obtiene:

$$T_{ba}(v_g) = r(b,a,g)^{-1}C(b,a)^{-1}T_b(T_a(v_g)). \tag{2.3}$$

Como $T_{ab} = T_{ba}$, ya que G es abeliano, se sigue entonces que

$$T_a(T_b(v_g)) = r(a,b,g)C(a,b)r(b,a,g)^{-1}C(b,a)^{-1}T_b(T_a(v_g)).$$

Y como estamos suponiendo que $r(a,b,g) = r(b,a,g)$, vemos que

$$T_a(T_b(v_g)) = q(a,b)T_b(T_a(v_g)),$$

y por tanto, si x es *cualquier* vector de W se deduce que

$$T_b(T_a(x)) = q(b,a)T_a(T_b(x)). \tag{2.4}$$

Sea $W = \oplus_{g\in G} W_g$ una $\mathbb{C}$-álgebra G-graduada sobre un grupo cíclico $G = \langle a : a^n = 1\rangle$ de orden n. Sea w_a un elemento no nulo arbitrario en la componente homogénea W_a. Definamos inductivamente $w_{a^k} = w_a \cdot w_{a^{k-1}}$. De esta definición inductiva se sigue que $w_{a^0} = \alpha$, para cierto $\alpha \neq 0$ en $\mathbb{C}$. Definamos $v_{a^k} = \beta^k w_{a^k}$, donde β es una raíz n-ésima cualquiera de α^{-1}, es decir

$\beta^n = 1/\alpha$. Claramente, si $k = n$, vemos que $v_{a^0} = \beta^n w_{a^0} = \beta^n \alpha = 1$. Además, es obvio que

$$v_a v_{a^{k-1}} = \beta^k w_a w_{a^{k-1}} = \beta^k w_{a^k} = v_{a^k},$$

A la base $B = \{1, v_a, \ldots, v_{a^{n-1}}\}$ la llamaremos la *base estándar* para W. *En la discusión que sigue, las constantes de estructura* $c_B(a^r, a^k)$, *serán denotadas por brevedad como* $c(a^r, a^k)$. Notemos que $c(a, a^r) = 1$, para todo r.

Como T_a envía a cada v_{a^k} en $v_{a^{k+1}}$, entonces T_a permuta cícilicamente la base B. Se sigue sin dificultad que el polinomio minimal para T_a es precisamente $Y^n - 1 = 0$. Por tanto los valores propios de T_a son exactamente las raíces n-ésimas de la unidad, que denotaremos por $\{\omega_1, \ldots, \omega_n\}$. Para cada $1 \leq j \leq n$, definamos $z_j = \sum_{k=0}^{n-1} \omega_j^k v_{a^k}$. Notemos que si $t = s \bmod n$ entonces $\omega_j^t v_{a^t} = \omega_j^s v_{a^s}$, ya que si $t = s + nq$ entonces

$$\omega_j^t v_{a^t} = \omega_j^{nq} \omega_j^s v_{a^s} = 1 \cdot \omega_j^s v_{a^s}.$$

En consecuencia la sumatoria $\sum_{k=0}^{n-1} \omega_j^k v_{a^k}$ puede escribirse sin ambiguedad como $\sum_{k \in \mathbb{Z}_n} \omega_j^k v_{a^k}$.

Veamos ahora que ${\omega_j}^{-1}$ es un valor propio asociado al vector propio z_j. En efecto

$$\begin{aligned} T_a(z_j) &= \sum_{k \in \mathbb{Z}_n} \omega_j^k v_a v_{a^k} = {\omega_j}^{-1} \sum_{k+1 \in \mathbb{Z}_n} {\omega_j}^{k+1} v_{a^{k+1}} \\ &= {\omega_j}^{-1} \sum_{s \in \mathbb{Z}_n}^{n} \omega_j^s v_{a^s} = {\omega_j}^{-1} z_j. \end{aligned}$$

(En esta última suma tomamos $s = k + 1$).

Por otro lado, de la ecuación (2.4) se obtiene

$$\begin{aligned} T_b(T_a(z_j)) &= q(b,a) T_a(T_b(z_j)) \\ T_b({\omega_j}^{-1} z_j) &= q(b,a) T_a(T_b(z_j)) \\ {\omega_j}^{-1} T_b(z_j) &= q(b,a) T_a(T_b(z_j)) \\ q(a,b) {\omega_j}^{-1} T_b(z_j) &= T_a(T_b(z_j)). \end{aligned}$$

Por tanto $T_b(z_j)$ es un vector propio asociado al valor propio $q(a,b){\omega_j}^{-1}$. Como T_a tiene n-

valores propios distintos, existen ω_i y z_i tales que ${\omega_i}^{-1} = q(a,b){\omega_j}^{-1}$ y $T_b(z_j) = \delta_{b,j} z_i$, para algún escalar $\delta_{b,j} \neq 0$ en $\mathbb{C}$. Si tomamos $b = a^r$ vemos entonces que

$$\begin{aligned}
T_{a^r}(z_j) &= T_{a^r}(\sum_{k\in\mathbb{Z}_n} \omega_j^k v_{a^k}) = \sum_{k\in\mathbb{Z}_n} \omega_j^k C(a^r,a^k) v_{a^{r+k}} && (2.5)\\
&= \omega_j^{-r} \sum_{k+r\in\mathbb{Z}_n}^{n-1} \omega_j^{k+r} C(a^r,a^k) v_{a^{r+k}} && (2.6)\\
&= \omega_j^{-r} \sum_{s\in\mathbb{Z}_n} \omega_j^s C(a^r,a^{s-r}) v_{a^s} && (2.7)
\end{aligned}$$

(haciendo $s = k + r$). Por otro lado,

$$\begin{aligned}
T_{a^r}(z_j) &= \delta_{a^r,j} z_i = \delta_{a^r,j} \sum_{s\in\mathbb{Z}_n} \omega_i^s v_{a^s}\\
&= \sum_{s\in\mathbb{Z}_n} \delta_{a^r,j} q(a^r,a)^s \omega_j^s v_{a^s} && (2.8)
\end{aligned}$$

Igualando coeficientes en las ecuaciones (2.7) y (2.8) se obtiene

$$\omega_j^{s-r} C(a^r,a^{s-r}) = \delta_{a^r,j} q(a^r,a)^s \omega_j^s$$

y por tanto

$$C(a^r,a^{s-r}) = \delta_{a^r,j} q(a^r,a)^s {\omega_j}^r. \qquad (2.9)$$

En particular, si $s = r$, vemos que $1 = C(a^r,a^0) = \delta_{a^r,j} q(a^r,a)^r {\omega_j}^r$. Luego $\delta_{a^r,j} = q(a,a^r)^r {\omega_j}^{-r}$. Sustituyendo en (2.9) se obtiene

$$C(a^r,a^{s-r}) = q(a,a^r)^r \omega_j^{-r} q(a^r,a)^s \omega_j^r,$$

y por tanto $C(a^r,a^{s-r}) = q(a^r,a)^{s-r}$. Si hacemos $k = s - r$ se obtiene que

$$C(a^r,a^k) = q(a^r,a)^k = C(a^r,a)^k C(a,a^r)^{-k} = C(a^r,a)^k,$$

esta última ecuación es cierta debido a que en la base estándar $C(a,a^r) = 1$. Por tanto

$$\begin{aligned}
r(a^r,a^s,a^t) &= C(a^s,a)^t C(a^{r+s},a)^{-t} C(a^r,a)^{s+t} C(a^r,a)^{-s} && (2.10)\\
&= [C(a^s,a)C(a^r,a)C(a^{r+s},a)^{-1}]^t && (2.11)
\end{aligned}$$

Hemos demostrado el siguiente teorema.

Teorema 2.5.1 *Sea* $G = \langle a^r : r = 0, \ldots, n-1 \rangle$ *un grupo cíclico de orden* n, *y sea* $W = \oplus_{r=0}^{n-1} W_{a^r}$, *un álgebra graduada compleja sobre* G, *para la cual su función de asociatividad* r *es simétrica en las dos primeras componentes. Sea* B *una base estándar para* W. *Entonces* W *queda completamente determinada por la funcion* $f : G \to A$, *definida por* $f(a^r) = c(a^r, a)$. *De aquí se deduce que existen exactamente* $|A|^{n-2}$ *álgebras graduadas complejas sobre* G, *no isomorfas entre sí.*

Ejemplo 2.5.1 *Sea* $\mathbb{Z}_4 = \langle a, a^2, a^3, a^4 = 1 \rangle$ *y* $W = \oplus_{r=0}^{3} W_{a^r}$, *una* $\mathbb{C}$*-álgebra graduada sobre* $\mathbb{Z}_4$ *y* B *una base estándar. Sea* $A = \{1, -1\}$. *El polinomio minimal para* T_a *es precisamente* $Y^4 - 1 = 0$, *y por tanto sus valores propios son exactamente las raíces cuartas de la unidad* $\{\omega_1 = -i, \omega_2 = -1, \omega_3 = i, \omega_4 = 1\}$. *Es fácil ver que los vectores propios asociados a estos valores propios son*

$$\begin{aligned} z_1 &= 1 + iv - v_2 - iv^3 \\ z_2 &= 1 - v + v^2 - v^3 \\ z_3 &= 1 - iv - v^2 + iv^3 \\ z_4 &= 1 + v + v^2 + v^3 \end{aligned}$$

de tal forma que

$$\begin{aligned} T_a(z_1) &= -iz_1 \\ T_a(z_2) &= -z_2 \\ T_a(z_3) &= iz_3 \\ T_a(z_4) &= z_4 \end{aligned}$$

Caso 1 : *Supongamos que* $C(a^2, a) = -1$ *y* $C(a^3, a) = 1$. *Por tanto*

$$\begin{aligned} T_a(T_{a^2}(z_1)) &= -T_{a^2}(T_a(z_1)) \\ T_a(T_{a^2}(z_1)) &= iT_{a^2}(z_1) \end{aligned}$$

Entonces $T_{a^2}(z_1)$ *es un vector propio asociado al valor propio* i,*es decir,* $T_{a^2}(z_1) = \beta(a^2, 1)z_3$. *Luego*

$$\beta(a^2, 1) = q(a, a^2)^2\omega_1^{-2} = (-1)^2(i)^{-2} = -1$$

y las constantes de estructuras están dadas por

$$\begin{aligned} C(a^2, a^2) &= q(a^2, a)^2 = 1 \\ C(a^2, a^3) &= q(a^2, a)^3 = -1 \\ C(a^2, a) &= q(a^2, a) = -1 \end{aligned}$$

Similarmente, $T_{a^2}(z_2)$ *es un vector propio asociado al valor propio* 1, *es decir,* $T_{a^2}(z_2) = \beta(a^2, 2)z_4$, *con* $\beta(a^2, 2) = 1$. *Y* $T_{a^2}(z_3)$ *es un vector propio asociado al valor propio* $-i$, *es decir,* $T_{a^2}(z_3) = \beta(a^2, 3)z_1$,*con* $\beta(a^2, 3) = -1$. *Finalmente,* $T_{a^2}(z_4)$ *es un vector propio asociado al valor propio* -1 : $T_{a^2}(z_4) = \beta(a^2, 4)z_2$, *con* $\beta(a^2, 4) = 1$. *Ahora, sea* $b = a^3$; *como* $q(a, a^3) = 1$, *entonces*

$$\begin{aligned} T_a(T_{a^3}(z_1)) &= T_{a^3}(T_a(z_1)) \\ T_a(T_{a^3}(z_1)) &= -iT_{a^3}(z_1) \end{aligned}$$

Entonces $T_{a^3}(z_1)$ *es un vector propio asociado al valor propio* $-i$, *es decir,* $T_{a^3}(z_1) = \beta(a^3, 1)z_1$. *Luego*

$$\beta(a^3, 1) = q(a, a^3)^3\omega_1^{-3} = (1)^3(i)^{-3} = i,$$

y las constantes de estructuras están dadas por

$$\begin{aligned} C(a^3, a) &= q(a^3, a) = 1 \\ C(a^3, a^2) &= q(a^3, a)^2 = 1 \\ C(a^3, a^3) &= q(a^3, a)^3 = 1. \end{aligned}$$

Similarmente, $T_{a^3}(z_2)$ *es un vector propio asociado al valor propio* -1*. Es decir,* $T_{a^3}(z_2) = \beta(a^3, 2)z_2$*, con* $\beta(a^3, 2) = -1$*. Y* $T_{a^3}(z_3)$ *es un vector propio asociado al valor propio* i *:* $T_{a^3}(z_3) = \beta(a^3, 3)z_3$*, con* $\beta(a^3, 3) = -i$*. Finalmente,* $T_{a^3}(z_4)$ *es un vector propio asociado al valor propio* $1 : T_{a^3}(z_4) = \beta(a^3, 4)z_3$*, con* $\beta(a^3, 4) = 1$*. La siguiente tabla muestra las constantes de estructura para esta álgebra.*

$C_{\mathbb{Z}_4}$	1	a	a^2	a^3
1	1	1	1	1
a	1	1	1	1
a^2	1	-1	1	-1
a^3	1	1	1	1

De manera análoga se analizan los siguientes tres casos

caso 2: $q(a, a^2) = -1$ y $q(a, a^3) = -1$

caso 3: $q(a, a^2) = 1$ y $q(a, a^3) = 1$

caso 4: $q(a, a^2) = 1$ y $q(a, a^3) = -1$

En cada caso obtenemos las constantes de estructura para cada una de estas álgebras

$C'_{\mathbb{Z}_4}$	1	a	a^2	a^3
1	1	1	1	1
a	1	1	1	1
a^2	1	-1	1	-1
a^3	1	-1	1	-1

$C''_{\mathbb{Z}_4}$	1	a	a^2	a^3
1	1	1	1	1
a	1	1	1	1
a^2	1	1	1	1
a^3	1	1	1	1

$C'''_{\mathbb{Z}_4}$	1	a	a^2	a^3
1	1	1	1	1
a	1	1	1	1
a^2	1	1	1	1
a^3	1	-1	1	-1

En consecuencia, tenemos $|A|^{n-2} = (2)^2$ algebras graduadas sobre $\mathbb{Z}_4$.

Teorema 2.5.2 *Sean W_1, W_2 álgebras $\mathbb{Z}_n$-graduadas sobre $\mathbb{C}$ o $\mathbb{R}$ con constantes de estructura C_1 y C_2 en bases estándar B_1 y B_2, respectivamente y función de asociatividad r, simétrica en las primeras dos componentes. Entonces $W_1 \cong W_2$ si y solo si $C_1(a^r, a) = C_2(a^r, a)$, para todo $1 \leq r \leq n$.*

Prueba. Por un teorema anterior sabemos que $W_1 \cong W_2$ si y solo si $d^2(C_1 C_2^{-1}) = 1$ o equivalentemente $d^2C_1 = d^2C_2$. Esto es, $r_1 = r_2$. Ahora, si $r_1 = r_2$ entonces la ecuación (2.11) es cierta para todo t. En particular, para $t = 1$. Definamos $f_i : G \to A$ por $f_i(a^r) = C_i(a^r, a)$. Tomando la primera derivación tenemos que

$$d^1 f_i(a^r, a^s) = f_i(a^s) f_i(a^{r+s})^{-1} f_i(a^r).$$

Entonces, $r_1 = r_2$ si y solo si $d^1 f_1 = d^1 f_2$, lo cual equivale a que $(f_1 f_2^1) \in Ker(d^1)$. Pero

$$\begin{aligned} Ker(d^1) &= H^1(G, A) = \{h : G \to A : h(a)h(b)h(ab)^{-1} = 1\} \\ &= \{h : G \to A : h \text{ es un homomorfismo de grupos}\}. \end{aligned}$$

Entonces $f_1 f_2^{-1} = h$ para algún homomorfismo de grupos h. Por tanto $f_1 = hf_2$, es decir

$$C_1(a^r, a) = h(a)C_2(a^r, a), \text{ para todo } 1 \leq r \leq n-1.$$

Si $r = 1$ tenemos que $1 = C_1(a, a) = h(a)C_2(a, a)$, lo cual implica que $h(a) = 1$, para todo $a \in G$. En conclusión $C_1(a^r, a) = C_2(a^r, a)$ para $1 \leq r \leq n-1$. ■

2.6 Preguntas abiertas

Con el propósito de continuar este trabajo surgen los siguientes proyectos:

1. Extender la clasifición de álgebras G-graduadas para grupos abelianos sin la condición de simetría en la función r.

2. Extender el caso de grupos cíclicos al caso donde G es abeliano, preservando la simetría de la función r.

3. Investigar la formula de Kunneth para obtener resultados cohomológicos para una clasificación más general.

Bibliografía

[1] Atiyah, M. F.and C.T.C. Walls, Cohomology of Groups, from J.W.S Cassel, Algebraic Number Theory, Thompson Book Company, Washington D. C, (1967).

[2] David S. Dummit-Richard M.Foote, Abstract Algebra, 2nd ed, Editorial Prentice-Hall do Brasil, Ltda, Rio de Janeiro.

[3] A. Babakhanian, Cohomological methods in grup theory, Marcel Dekker Inc., (1972).

[4] L.A. Wills Toro, Symmetry transformations with noncommutative and nonassociative parameters, Internat. Jour. Theor. Phys. 36 No 12, 2963-2996 (Dec. 1997).

[5] L.A Wills-Toro, T. Craven, and J.D Vélez, Cohomology of deformation parameters of diagonal noncommutative nonassociative graded algebras. Acta Mathematica Academiae Paedagogiace Nyíregyháziensis, Vol. 24, No 3, pp 271-277 (2008).

[6] L.A Wills-Toro, T. Craven, and J.D Vélez,Graded Lie algebras and q-commutative and r-associative parameters. Sao Paulo Journal of Mathematical Sciences 3, 2 (2009).