TESIS DE LICENCIATURA

Representaciones de los grupos simétricos

Gastón Andrés García

Director: Dr. Nicolás Andruskiewitsch

Codirector: Dr. Fernando Cukierman

Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires

Marzo 2001

Índice general

Introducción

La noción de grupo fue introducida por E. Galois hacia 1829, si bien está implícita en obras de Lagrange y Gauss. Su importancia no fue reconocida durante un largo período, hasta que Felix Klein le dio un lugar fundamental en su interpretación de la geometría no euclideana. A fines del siglo XIX, la teoría de grupos finitos inicia un vigoroso desarrollo a través de los trabajos de Frobenius y Burnside, y más adelante de Schur.

Un problema fundamental de la teoría es determinar todas las representaciones de dimensión finita de un grupo dado G, sobre un cuerpo algebraicamente cerrado K. Este problema no sólo es interesante en sí mismo y por sus aplicaciones en otros campos, sino que es importante para entender la estructura interna del grupo G. Las posibles soluciones de estos problemas se encuadran en dos casos radicalmente diferentes: cuando la característica del cuerpo es cero o no divide al orden del grupo G, y cuando la característica de K divide al orden de G.

En el primer caso, toda representación es completamente reducible, esto es, es suma directa de representaciones irreducibles; donde la cantidad de representaciones irreducibles es igual a la cantidad de clases de conjugación del grupo G y las dimensiones de las representaciones irreducibles dividen al orden del grupo. Este material es expuesto en el capítulo 1. Sin embargo, el problema de describir explícitamente todas las representaciones irreducibles del grupo fijo G es mucho más complicado en cada caso particular. El caso fundamental del grupo simétrico $\mathbb{S}_n$ es estudiado en detalle en el capítulo 2.

En el segundo caso, es decir cuando la característica del cuerpo divide a orden del grupo, hay representaciones que no son completamente reducibles y la teoría es mucho más difícil. En este trabajo, esencialmente en el capítulo 3, nos concentramos en estudiar las representaciones irreducibles del grupo G usando el método de Brauer. A fin de completar el estudio de las representaciones irreducibles del grupo simétrico, exponemos en el último capítulo la descripción de éstas sobre cuerpos de característica positiva. Si bien no se conoce dicha descipción en forma explícita para todos los grupos simétricos, con lo visto aquí nos alcanza para exponer las representaciones modulares de $\mathbb{S}_5$ sobre $\mathbb{F}_2$, $\mathbb{F}_3$ y $\mathbb{F}_5$.

Capítulo 1

Representaciones Lineales de Grupos Finitos

En este capítulo analizaremos las representaciones lineales de grupos finitos sobre un cuerpo K. Exceptuando las primeras nociones básicas, supondremos a partir del lema de Schur que K es algebraicamente cerrado. Serán de suma importancia las condiciones sobre la característica del cuerpo, aunque en gran parte de esta sección se supondrá que la característica es cero. En tal caso, sin pérdida de generalidad, supondremos que el cuerpo es $\mathbb{C}$. Comenzaremos con algunas definiciones y propiedades básicas de la teoría.

1.1. Definiciones

En lo que sigue, K será un cuerpo.

Definición 1 *Sean G un grupo y V un espacio vectorial sobre K. Una* **representación lineal** *de G en V es un homomorfismo ρ del grupo G en el grupo $GL(V)$ de isomorfismos de V. Es decir, a cada elemento $x \in G$ se le asocia un elemento $\rho(x) \in GL(V)$ de modo que*

$$\rho(st) = \rho(s)\rho(t), \quad \forall\ s,t \in G\ .$$

Es claro que si e es el elemento neutro de G se tiene que

$$\rho(e) = I \quad \text{ y que } \quad \rho(s^{-1}) = (\rho(s))^{-1}.$$

Se notará (ρ, V) para enfatizar el hecho de que la representación ρ de G es sobre el espacio lineal V. A dicho espacio lineal V se lo llamará *espacio de representación* y a su dimensión el *grado* de la representación.

Definición 2 *Sean G un grupo y X un conjunto. Una* **acción** *de G sobre X es un homomorfismo $s : G \to S(X)$, donde $S(X)$ es el grupo de permutaciones de elementos de X. Esto es, a cada elemento $g \in G$ se le asigna una aplicación biyectiva $s(g)$ del conjunto X en sí mismo tal que*

$$s(g_1g_2) = s(g_1)s(g_2), \quad \forall\ g_1, g_2 \in G.$$

Cuando es claro a qué acción nos referimos, notaremos gx en lugar de $s(g)(x)$. Si X tiene una estructura de espacio vectorial sobre K, decimos que la acción es *lineal* si $s(g) \in GL(X)$. Esto implica que

$$\begin{array}{ll} g(v+w) = g(v) + g(w), & \forall\ v, w \in X, \quad g \in G, \\ g(\lambda v) = \lambda g(v), & \forall\ \lambda \in K, \quad g \in G. \end{array}$$

En este caso, X se denomina un **G-módulo**. Basta recordar la definición 1 para ver que esta estructura de G-módulo define una representación (s, X) de G sobre X. Recíprocamente, si (ρ, V) es una representación de G, entonces V adquiere una estructura de G-módulo, donde la acción de G sobre V esta definida por el morfismo ρ tal que $gv = \rho(g)(v), \quad \forall g \in G, \quad v \in V$. Cuando sea conveniente, usaremos esta correspondencia para notar las representaciones como G-módulos.

Sea (ρ, V) una representación de G de grado finito. Tomemos (e_i) una base de V y sea R(s) la matriz de $\rho(s)$ con respecto a esta base, entonces se tiene que

$$det(R(s)) \neq 0, \quad R(st) = R(s)R(t), \quad s, t \in G.$$

Si $r_{ij}(s)$ son los coeficientes de la matriz R(s), la segunda fórmula se escribe

$$r_{ik}(st) = \sum_j r_{ij}(s).r_{jk}(t), \quad \text{para todo } i, k.$$

Recíprocamente, si disponemos de matrices inversibles $R(s) = (r_{ij}(s))$ que verifican las identidades anteriores tenemos una representación lineal ρ de G en V. En este caso diremos que se tiene una representación en forma matricial de G en V.

Definición 3 *Sean $(\rho, V^{'})$ y $(\rho^{'}, V^{'})$ dos representaciones lineales de un grupo G en dos espacios vectoriales sobre K, V y $V^{'}$ respectivamente. Un* **morfismo de representaciones** *es una aplicación lineal $\varphi : V \to V^{'}$ de K espacios vectoriales que verifica*

$$\varphi\rho(s) = \rho^{'}(s)\varphi \quad \forall\ s \in G.$$

Es decir, φ transforma ρ en $\rho^{'}$; a esta aplicación frecuentemente se la llama *entrelazamiento*. De acuerdo a la notación de G-módulos, los morfismos de representaciones son aplicaciones lineales que preservan la acción de G sobre V, por tanto se los llamará morfismos de G-módulos o directamente *G-morfismos*.

La definición anterior es más clara si se ve de la siguiente manera: si (ρ, V) y $(\rho^{'}, V^{'})$ se dan en forma matricial por $R(s)$ y $R^{'}(s)$ respectivamente, el morfismo se traduce en una matriz T tal que

$$TR(s) = R^{'}(s)T \quad \forall\ s \in G.$$

Si φ resulta ser un isomorfismo lineal, diremos que es un isomorfismo de representaciones y en este caso para la forma matricial se tiene que, al ser T una matriz inversible, la siguiente identidad

$$R^{'}(s) = TR(s)T^{-1} \quad \forall\ s \in G.$$

De esta manera, dos representaciones isomorfas se pueden identificar; en particular, tienen el mismo grado. Es claro que si tenemos una representación (ρ, V) dada en forma matricial con respecto a dos bases distintas de V $R(s)$ y $R^{'}(s)$, estas representaciones en forma matricial resultan isomorfas, siendo φ el isomorfismo dado por el cambio de base.

Cabe preguntarse cuándo un subespacio W de un espacio V hereda la estructura de G-módulo de V. Para esto sólo basta que W sea invariante por la acción del grupo G, es decir que W sea un G-submódulo; o sea si $w \in W$ entonces $\rho(s)(w) \in W, \forall\ s \in G$. En efecto, la restricción $\rho|_W(s)$ es un automorfismo de W para todo

$s \in G$ y como $\rho|_W(st) = \rho|_W(s).\rho|_W(t)$ tenemos que $\rho|_W : G \to GL(W)$ es una representación lineal de G sobre W. En esta situación se dice que $(\rho|_W, W)$ es una *subrepresentación* de (ρ, V).

La palabra representación sugiere que, dada una representación matricial, los elementos del grupo G se pueden ver como matrices o, en otras palabras, que existe un isomorfismo del grupo dado con algún grupo de las matrices. En los casos donde el grupo G tiene una estructura complicada, podría resultar que una representación matricial lineal sea la única manera simple de describirlo. Sin embargo, debemos enfatizar que una representación lineal no siempre da un isomorfismo entre el grupo G y algún subgrupo de $GL_m(K)$. La razón es que una misma matriz puede corresponder a distintos elementos de G, y esto ocurre si y sólo si existen elementos en G distintos del elemento neutro que tiene como imagen a la matriz identidad.

El conjunto de los elementos de G tal que la imagen por la representación matricial R es la matriz identidad es un subgrupo normal de G que se denomina el *núcleo* de la representación R y se denota $ker(R)$. Cuando ocurre que $ker(R) = G$, es decir, la imagen de todos los elementos de G por R es la matriz identidad, diremos que R es una **representación trivial** de G.

Sea (ρ, V) una representación de G sobre K, definimos la **componente trivial** de G al G-submódulo de V dado por

$$W = \{v \in V : \rho(g)(v) = v, \forall\ g \in G\}.$$

1.2. Ejemplos

a) Sea $K = \mathbb{C}$. Una representación de grado 1 de un grupo no es más que un morfismo $\rho : G \to \mathbb{C}^*$, donde $\mathbb{C}^*$ es el grupo multiplicativo de los complejos no nulos. Estas representaciones se denominan *caracteres multiplicativos*. Como G tiene orden finito, todos sus elementos son de orden finito, luego las imágenes $\rho(s)$ de ρ deben ser raíces de la unidad; en particular $|\rho(s)| = 1$. Por ejemplo, sea $\mathbb{Z}_n$ el grupo aditivo de los restos de la división por n en $\mathbb{Z}$ y consideremos la siguiente representación: sea $w \in \mathbb{C}^*$ una raíz n-ésima de la unidad,

$$\begin{aligned}&\rho : \mathbb{Z}_n \to \mathbb{C}^*,\\ &\rho(x) = w^x, \qquad \forall\ x \in \mathbb{Z}_n.\end{aligned}$$

En particular, si w_1 y w_2 son raíces n-ésimas de la unidad tal que $w_1 \neq w_2$, entonces $\rho_{w_1} \neq \rho_{w_2}$. En efecto, si $\rho_1, \rho_2 : G \to \mathbb{C}^*$ son dos representaciones, entonces $\rho_1 \cong \rho_2 \Leftrightarrow \rho_1 = \rho_2$.

Demostración:
Una implicación es trivial, demostremos la otra. Si $\rho_1 \cong \rho_2$ entonces existe un $\lambda \in \mathbb{C}$ tal que $\rho_1(x).\lambda = \lambda.\rho_2(x)$, pero esto implica que $\rho_1 = \rho_2$ como se quería demostrar. $\square$

b) Sea n el orden de G, y sea V un espacio vectorial sobre K de dimensión n; sea $(e_t)_{t\in G}$ una base de V indicada por los elementos de G. Definamos la siguiente representación: si $s \in G$, sea $\rho(s)$ el endomorfismo de V que transforma e_t en e_{st}; es claro que resulta una representación lineal de G. Esta representación se llama la **representación regular** de G. Como $e_s = \rho(s)(e_1)$, los transformados de e_1 forman una base de V. Recíprocamente, si (ρ', W) es una representación de G para la cual existe un vector w tal que $\{\rho'(s)(w)\}_{s\in G}$ sea una base de W; entonces W es isomorfa a la representación regular vía el isomorfismo:

$$\begin{aligned}&\tau : V \to W,\\ &\tau(e_s) = \rho'(s)(w), \quad \forall\ s \in G.\end{aligned}$$

Sea M el subespacio de dimensión 1 generado por el elemento $x = \sum_{s\in G} e_s$. Como $\rho(s)(x) = x$ para todo $s \in G$, tenemos que $(\rho|_M, M)$ es una subrepresentación de la representación regular, isomorfa a la representación trivial; en particular, si el orden del grupo es mayor o igual a dos, la representación regular siempre contiene una subrepresentación propia no nula.

c) Tomemos el grupo diedral de orden 6, $\mathbb{D}_3$, generado por dos elementos s y ρ con relaciones

$$s^2 = 1,\ \rho^3 = 1,\ s.\rho.s = \rho^2.$$

Así $\mathbb{D}_3 = \{1,\ \rho,\ \rho^2,\ s,\ s.\rho,\ s.\rho^2\}$. Sea V el espacio vectorial sobre K de dimensión 6 con base

$$B = \{v_1, v_\rho, v_{\rho^2}, v_s, v_{s.\rho}, v_{s.\rho^2}\}$$

inducido por la representación regular. Luego, la acción de ρ está dada por:

$$\rho.v_1 = v_\rho, \qquad \rho.v_\rho = v_{\rho^2}, \qquad \rho.v_{\rho^2} = v_1$$

$$\rho.v_s = v_{s.\rho^2}, \quad \rho.v_{s.\rho} = v_s, \quad \rho.v_{s.\rho^2} = v_{s.\rho}.$$

Análogamente se puede dar la acción de s y así conocer la acción del grupo $\mathbb{D}_3$ sobre V. Es claro que la forma matricial de la representación dará matrices de permutación para cada elemento $x \in \mathbb{D}_3$. Por ejemplo, la matriz $R(\rho) \in GL(V)$ viene dada por:

$$R(\rho) = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

d) Análogamente, consideremos ahora el grupo diedral de orden $2n$, $\mathbb{D}_n$ definido por los generadores ρ, s con relaciones $s^2 = 1,\ \rho^n = 1,\ s\rho s = \rho^{n-1}$. Es claro que para definir una representación sólo basta hacerlo sobre los generadores, sea entonces $\tau : \mathbb{D}_n \to GL(2, \mathbb{R})$ definida por:

$$\tau(s) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tau(\rho) = \begin{pmatrix} cos(\frac{2\pi}{n}) & -sen(\frac{2\pi}{n}) \\ sen(\frac{2\pi}{n}) & cos(\frac{2\pi}{n}) \end{pmatrix}.$$

Se deduce de las fórmulas trigonométricas de adición que para todo $t, r \in \mathbb{R}$ se tiene

$$\begin{pmatrix} cos(t+r) & -sen(t+r) \\ sen(t+r) & cos(t+r) \end{pmatrix} = \begin{pmatrix} cos(t) & -sen(t) \\ sen(t) & cos(t) \end{pmatrix} \begin{pmatrix} cos(r) & -sen(r) \\ sen(r) & cos(r) \end{pmatrix}.$$

Por tanto, esta representación real se puede ver como los movimientos rígidos de un polígono regular de n lados, donde $\tau(\rho)$ es la rotación en un ángulo de $\frac{2\pi}{n}$ y $\tau(s)$ es la simetría con respecto al eje de las abscisas.

e) Consideremos (ρ_1, V_1) y (ρ_2, V_2) dos representaciones de G sobre K. Sabemos que el conjunto $V = V_1 \oplus V_2$ hereda una estructura de K espacio vectorial tomando las operaciones coordenada a coordenada. Análogamente, las acciones de G sobre ambos espacios de representación inducen una representación de G en la suma directa definiendo la acción de G coordenada a coordenada, es decir $\rho(g)(v, w) = (\rho_1(g)(v), \rho_2(g)(w))$. Por tanto, la suma directa de G-módulos hereda una estructura de G-módulo. Si las dimensiones de V_1 y V_2 son n y m respectivamente, la representación $(\rho, V_1 \oplus V_2)$ tendrá grado $n + m$.

f) Sean V_1 y V_2 espacios vectoriales sobre K. Se llama producto tensorial de V_1 y V_2 a un K espacio vectorial $V_1 \otimes V_2$ provisto de una aplicación bilineal

$$V_1 \times V_2 \to V_1 \otimes V_2,$$

$$(x_1, x_2) \mapsto x_1 \otimes x_2,$$

la cual es universal; es decir, para toda aplicación bilineal $\beta : V_1 \times V_2 \to W$, siendo W un K espacio vectorial, existe una única aplicación *lineal*

$$\psi : V_1 \otimes V_2 \to W,$$

$$x_1 \otimes x_2 \mapsto \beta(x_1, x_2),$$

tal que el siguiente diagrama resulta conmutativo

$$\begin{tikzcd} V_1 \times V_2 \arrow[r] \arrow[dr, "\beta"'] & V_1 \otimes V_2 \arrow[d, dashed, "\exists ! \psi"] \\ & W \end{tikzcd} . \tag{1}$$

Se demuestra que tal espacio existe y que es único salvo isomorfismos. Es fácil ver que $dim(V_1 \otimes V_2) = dim(V_1).dim(V_2)$

Si (ρ_1, V_1) y (ρ_2, V_2) son dos representaciones lineales de un grupo finito G, de la misma manera que en el ejemplo anterior, las acciones de G sobre V_1 y V_2 inducen sobre el producto tensorial $V_1 \otimes V_2$ una estructura de G-módulo definida por:

$$\rho : G \to V_1 \otimes V_2,$$

$$\rho(s)(x_1 \otimes x_2) = \rho_1(s)(x_1) \otimes \rho_2(s)(x_2), \quad x_1 \in V_1, \quad x_2 \in V_2.$$

Es decir, el producto tensorial de G-módulos es un G-módulo.

g) Supongamos que G es un grupo de permutaciones de un conjunto X y K^X el espacio vectorial de aplicaciones de X en K. Si $f \in V$ y $s \in G$, definimos la acción de G sobre K^X como

$$\rho : G \to K^X,$$

$$(\rho(s)(f))(x) = f(s^{-1}x), \quad \forall x \in X, \quad s \in G.$$

Como $\rho(s)(f+g) = \rho(s)(f) + \rho(s)(g)$ y $\rho(s)(\lambda f) = \lambda \rho(s)(f)$, tenemos que $\rho(s)$ depende linealmente de f; es decir, $\rho(s)$ es un automorfismo lineal de K^X en si mismo $\forall\ s \in G$. Más aún, se tiene que

$$\begin{aligned} (\rho(st)(f))(x) &= f((st)^{-1}x) \\ &= f(t^{-1}s^{-1}x) \\ &= (\rho(t)(f))(s^{-1}x) \\ &= (\rho(s)\rho(t)(f))(x), \quad \forall\ s,t \in G,\ x \in X,\ f \in K^X. \end{aligned}$$

Por tanto, K^X tiene una estructura de G-módulo.

h) Observar que K^X admite ciertos subespacios que son naturalmente G-submódulos. Por ejemplo,

1) $K^{(X)} = \{f \in K^X$ / sop(f) es finito$\}$

En efecto, el hecho de que $K^{(X)}$ sea un G-submódulo se deduce de la igualdad $sop(\rho(g)f) = g.(sop(f))$; es decir que $\rho(g)(f)$ tiene soporte finito $\forall\ g \in G,\ f \in K^{(X)}$ y por tanto $\rho(g)(f) \in K^{(X)}, \forall\ g \in G$.

2) Si $K = \mathbb{C}$ y X es un espacio topológico, decimos que una representación es *continua* si vale que el isomorfismo $\rho(g)$ es continuo como función de K^X en K^X para todo $g \in G$. Luego, el subespacio de K^X definido por $C(X, \mathbb{C}) = \{f : X \to \mathbb{C} : f \text{ es continua}\}$ resulta ser un G-submódulo.

3) En el caso particular de que X sea un espacio vectorial sobre K, sea

$$X^* = \{f : X \to K : f \text{ es lineal sobre } K\}.$$

Si la acción de G es lineal sobre X, este subespacio de K^X es claramente invariante por la acción de G y la representación que induce se denomina la *representación dual* de G sobre X.

1.3. Completa Reducibilidad

Recordando un poco de álgebra lineal, dado un espacio vectorial V de dimensión finita y un subespacio W, siempre se podía encontrar un subespacio $W^{'}$ tal que $V = W \oplus W^{'}$. Mas aún, $W^{'}$ es el núcleo de la proyección $\pi : V \to W$, donde $\pi(x) = w$, para todo $x = w + w^{'} \in V$. Recíprocamente, sea $\pi \in GL(V)$ una proyección, es decir $\pi^2 = \pi$, siempre se tiene que $V = ker(\pi) \oplus im(\pi)$. Si la proyección es sobre W, entonces $W = im(\pi)$ y de aquí se deduce que V es suma directa de W más el núcleo de esta aplicación lineal π. De esta manera se establece una correspondencia biunívoca entre los proyectores de V sobre W y los *complementos* $W^{'}$ de W en V. En esta sección veremos que si W tiene una estructura de G-módulo y la característica del cuerpo no divide al orden del grupo, entonces se puede encontrar un subespacio complementario que sea invariante por la acción de G.

Para entender mejor la noción de completa reducibilidad comencemos con un ejemplo. Sea $\mathbb{Z}_n$ el grupo aditivo de las clases de restos modulo n. Consideremos la representación:

$$\begin{array}{ll} \rho : \mathbb{Z}_n \to GL_m(\mathbb{C}), & \\ \rho(1) = T, & \qquad T \in GL_m(\mathbb{C}). \end{array}$$

Al ser ρ un morfismo, se debe tener que $T^n = I$. Fijando la base canónica de $\mathbb{C}^m$, asociemos a cada isomorfismo de $GL_m(\mathbb{C})$ su matriz inversible de $m \times m$. Luego, al isomorfismo T le corresponde una matriz inversible M tal que $M^n = I$. Por tanto, su polinomio característico q divide a $p = X^n - 1$. Como las raíces de p son todas de multiplicidad 1, se tiene que las raíces de q son todas de multiplicidad 1. Por tanto, M resulta diagonalizable y sus autovalores son raíces n-ésimas de la unidad. Luego, $\exists\ P \in GL_m(\mathbb{C})$ tal que $PMP^{-1} = D$ donde D es una matriz diagonal cuyos elementos no nulos en la diagonal principal son las raíces de p. De esto se deduce que $PM^i = D^iP$ para todo $i \in \mathbb{Z}$.

Esto dice que si consideramos $\rho^{'} : \mathbb{Z}_n \to GL_m(\mathbb{C})$ definida por $\rho^{'}(x) = D^x$, tenemos que P es un isomorfismo de representaciones. Luego podemos identificar ρ con $\rho^{'}$.

Al ser D diagonal, es fácil ver que

$$\rho^{'} = \rho_{w_1} \oplus \rho_{w_2} \oplus .... \oplus \rho_{w_m},$$

aquí los $w_i,\ i = 1, ..., m$ son los elementos de la diagonal de D y $(\rho_{w_i}, \mathbb{C})$ son los caracteres multiplicativos dados por $\rho_{w_i}(x) = {w_i}^x, \forall\ x \in \mathbb{Z}_n$. Por tanto, tenemos que

$$\rho \cong \rho_{w_1} \oplus \rho_{w_2} \oplus .... \oplus \rho_{w_m}.$$

En conclusión, toda representación $(\rho, \mathbb{C}^m)$ de $\mathbb{Z}_n$ es isomorfa a una suma directa de $\rho_{w_1}, ..., \rho_{w_m}$, donde w_i son raíces n-esimas de la unidad. Más aún, por el ejemplo *a)* tenemos que $\rho_{w_i} \cong \rho_{w_j}$ si y sólo si $w_i = w_j,\ \forall\ i, j$.

El siguiente teorema es esencial para mostrar que ésta es la situación general, es decir que toda representación sobre un cuerpo K de característica cero se puede escribir como suma directa de otras más simples.

Teorema 1.1 *(Teorema de Maschke).*

Sean G un grupo finito, K un cuerpo cuya característica no divide al orden del grupo y V un K espacio vectorial. Sean $\rho : G \to GL(V)$ una representación lineal de G en V y W un subespacio vectorial de V estable por la acción de G. Existe entonces un complemento W^0 de W en V que es estable por la acción de G.

Demostración:
Sea n el orden de G. Sabemos que existe un subespacio $V^{'}$ en V que es complemento de W. Sea π el proyector de V sobre W tal que V' es su núcleo. Es claro que $V = W \oplus V^{'}$, pero $V^{'}$ no tiene porque ser un G-submódulo. Para encontrar un complemento invariante por la acción de G, tomemos el promedio π^0 de los transformados de π por los elementos de G:

$$\pi^0 = \frac{1}{n} \sum_{t \in G} \rho(t)\pi\ \rho(t)^{-1}$$

Como π manda V en W y $\rho(t)$ deja invariante W para todo $t \in G$, entonces π^0 manda V en W. Por otro lado, si $x \in W$, $\rho(t)^{-1}(x) \in W$, de donde se tiene que $\pi\ \rho(t)^{-1}(x) = \rho(t)^{-1}(x)$ y que $\rho(t)\pi\ \rho(t)^{-1}(x) = x$, o sea que $\pi^0(x) = x$. En particular, se deduce que ${\pi^0}^2 = \pi^0$. Luego, π^0 es un proyector de V sobre W al cual le corresponde un cierto subespacio W^0 complementario de W. Para ver que W^0 es un G-submódulo basta ver que se verifica $\rho(t)\pi^0 = \pi^0\rho(t),\ \forall t \in G$. En efecto, si $x \in W^0$ y $t \in G$, entonces $\rho(t)\pi^0(x) = \pi^0\rho(t)(x)$, pero como $\pi^0(x) = 0$ tenemos que $\pi^0\rho(t)(x) = 0$ y esto implica que $\rho(t)(x) \in W^0$, es decir que W^0 es un G-submódulo. Veamos entonces que $\rho(s)\pi^0 = \pi^0\rho(s), \forall s \in G$.

$$\begin{aligned}\rho(s)\pi^0\rho(s)^{-1} &= \tfrac{1}{n}\textstyle\sum_{t \in G} \rho(s)\rho(t)\pi\ \rho(t)^{-1}\rho(s)^{-1} \\ &= \tfrac{1}{n}\textstyle\sum_{t \in G} \rho(st)\pi\ \rho(st)^{-1} \\ &= \pi^0.\end{aligned}$$

□

Observación: Manteniendo las notaciones y las hipótesis del teorema anterior, sea $x \in V$ y sean w y w^0 sus proyecciones sobre W y W^0 respectivamente. Entonces, $\rho(s)(x) = \rho(s)(w + w^0) = \rho(s)(w) + \rho(s)(w^0)$; como W y W^0 son invariantes por la acción de G, $\rho(s)(w) \in W$ y $\rho(s)(w^0) \in W^0$ y por tanto $\rho(s)(w)$ y $\rho(s)(w^0)$ son las proyecciones de $\rho(s)(x)$. De ello se deduce que las representaciones W y W^0 son suficientes para conocer la representación V, ya que $V = W \oplus W^0$ y todo elemento de V se identifica con un par (w, w^0) tal que $w \in W$ y $w^0 \in W^0$. Si ambas subrepresentaciones se dan en forma matricial por R(s) y $R^0(s)$, la forma matricial de $V = W \oplus W^0$ viene dada por

$$\begin{pmatrix} R(s) & 0 \\ 0 & R^0(s) \end{pmatrix}. \qquad (2)$$

Definición 4 *Una representación lineal (ρ, V) de un grupo G se dice* **irreducible** *si $V \neq 0$ y V no contiene subespacios estables por la acción de G, excepto 0 y V. Es decir, V no contiene G-submódulos no triviales.*

Observación: Si la característica del grupo no divide al orden de G entonces la definición anterior, equivale a decir que V no es suma directa de dos G-submódulos propios.

Con esta definición queda claro entonces que toda representación de grado 1 resulta irreducible. Al principio de esta sección vimos como toda representación de $\mathbb{Z}_n$ se descompone como suma directa de representaciones irreducibles de dimensión 1. Más adelante veremos que esto se cumple para todo G grupo abeliano finito.

Teorema 1.2 *Sean G un grupo finito y K un cuerpo tal que su característica no divide al orden de G. Toda representación de G de dimensi'on finita es suma directa de representaciones irreducibles.*

Demostración:
Se demuestra este resultado por inducción sobre la dimensión de V. Si dim(V)=0, no hay nada que demostrar. Supongamos que $dim(V) \geq 1$ y que el teorema vale para todo V tal que $dim(V) < n$. Si (ρ, V) es irreducible no hay nada que probar. Si (ρ, V) no es irreducible, entonces V contiene a un G-submódulo $V^{'}$ propio, por el teorema 1.1 y la observación que le sigue, sabemos que existe $V^{''}$ un G-submódulo de V tal que $V = V^{'} \oplus V^{''}$, donde $dim(V^{'}) < dim(V)$ y $dim(V^{''}) < dim(V)$. Por hipótesis inductiva tenemos que $(\rho_{V'}, V^{'})$ y $(\rho_{V''}, V^{''})$ son suma directa de representaciones irreducibles, por tanto, al ser V suma directa de estas dos, resulta ser que (ρ, V) es también suma directa de representaciones irreducibles, como se quería demostrar. □

Observación: Usando el lema de Zorn, es fácil ver que *toda* representación de G de dimensión infinta es suma directa de representaciones irreducibles.

Observación: Podemos preguntarnos si la descomposición que nos da el teorema anterior es única. Es claro que para la representación trivial $\rho(s) = 1$ para todo $s \in G$ esto no es así, ya que todo espacio vectorial se puede descomponer como suma directa de rectas y éstas no están unívocamente determinadas. Sin embargo veremos más adelante que el número de representaciones irreducibles isomorfas a una representación irreducible dada no depende de la descomposición elegida.

Observación: Si consideramos a las representaciones de G como G-módulos, el teorema anterior dice que, si la característica del cuerpo no divide al orden del grupo, entonces todo G-módulo es suma directa de G-submódulos simples.

Definición 5 *Sea K un anillo conmutativo y G un grupo. Consideremos el conjunto*

$$K[G] = \left\{ \sum_{g \in G} \lambda_g.g : \quad \lambda_g \in K, \ \text{con } \lambda_g = 0, \ \text{salvo finitos } g \right\},$$

con las siguientes operaciones:

$$\sum_{g\in G} \lambda_g.g \quad + \quad \sum_{g\in G} \mu_g.g = \quad \sum_{g\in G}(\lambda_g + \mu_g).g,$$

$$(\sum_{g\in G} \lambda_g.g \quad)(\sum_{g\in G} \mu_g.g) = \quad \sum_{g\in G}(\sum_{h,k\in G, \ h.k=g} \lambda_h.\mu_k)g.$$

Es claro que, con las operaciones antes definidas, $K[G]$ resulta un anillo con unidad $1.e$, tal que e es el elemento neutro del grupo. Más aún, $K[G]$ es una K-álgebra sobre G que se denomina el álgebra de grupo de G.

Sea (ρ, V) una representación de G sobre K. Entonces el espacio de representación V hereda una estructura de $K[G]$-módulo a izquierda vía la acción:

$$(\sum_{g\in G} \lambda_g.g)(v) := \sum_{g\in G} \lambda_g.\rho(g)v, \quad \forall \ v \in M, \ g \in G.$$

De esta manera, toda representación es un $K[G]$-módulo. Recíprocamente, dado M un $K[G]$-módulo, se induce sobre M una representación de G, es decir, M resulta ser un espacio de representación de G. La acción de G está dada por

$$\rho(g).v \;=\; (1.g).v, \quad \forall\; g \in G,\; v \in M.$$

Los axiomas que definen la representación se verifican fácilmente por tener M una estructura de $K[G]$-módulo.

Sean (ρ, V) la representación regular de un grupo finito G y $(e_g)_{g\in G}$ una base de V indexada por elementos de G. El $K[G]$-módulo inducido por la representación regular resulta isomorfo a $K[G]$ como módulo a izquierda sobre si mismo, via el isomorfismo de $K[G]$-módulos inducido por la aplicación $\tau(e_g) = g$ sobre la base de V. Es decir, si extendemos la definición de la aplicación sobre la base en forma lineal sobre K tenemos que

$$\begin{aligned}&\tau : V \to K[G],\\ &\tau(\textstyle\sum_{g\in G} \lambda_g.e_g) = \sum_{g\in G} \lambda_g.g.\end{aligned}$$

Además, nos queda que el isomorfismo τ conmuta con la acción de G. En efecto,

$$h.\tau(e_g) = \; h.g = \; hg = \; \tau(e_{hg}) = \; \tau(h.e_g).$$

Por tanto, τ resulta un isomorfismo de $K[G]$-módulos.

En conclusión, si consideramos a toda representación de G como un $K[G]$-módulo, el teorema anterior nos dice que todo $K[G]$-módulo de dimensión finita es suma directa de $K[G]$-módulos simples. Esto quiere decir que, si la característica del cuerpo no divide al orden del grupo, el álgebra de grupo $K[G]$ resulta semisimple.

Consideremos ahora algunos ejemplos para entender mejor la relación del álgebra de grupo con la representación regular de G:

a) Consideremos el espacio vectorial de dimensión finita

$$(K[G])^* = \{f : K[G] \to K : \text{f es lineal}\}.$$

Luego, por la definición del álgebra de grupo $K[G]$, para conocer un elemento de este conjunto basta con decir cuanto vale sobre los elementos de G; en particular, si $f \in K^G$ definimos $\overline{f} \in (K[G])^*$ por

$$\overline{f}(\textstyle\sum_{g\in G} \lambda_g.g) = \sum_{g\in G} \lambda_g.f(g).$$

De esta manera, se tiene una aplicación entre K^G y $(K[G])^*$ que por definición resulta un isomorfismo lineal. Por tanto, se tiene que $K^G \cong (K[G])^*$, como G-módulos.

b) La estructura de grupo de G induce un endomorfismo ρ tal que

$$\rho : G \to G,$$

$$\rho(s)(t) = s^{-1}ts, \;\forall\; s, t \in G.$$

De manera muy semejante al ejemplo anterior, este endomorfismo define sobre $K[G]$ una acción lineal del grupo definida por:

$$g.(\textstyle\sum_{x\in G} \lambda_x.x) = (\sum_{x\in G} \lambda_x.\rho(g)(x)) = \sum_{x\in G} \lambda_x.g^{-1}.x.g, \quad \forall\; g \in G.$$

Por tanto, se tiene una representación de G $(ad, K[G])$ dada por

$$ad(s)(t) = s^{-1}ts, \;\forall\; s, t \in G,$$

que se denomina la **representación adjunta**.

Para finalizar la discusión de completa reducibilidad, veremos que si la característica del cuerpo K no divide al orden del grupo, toda representación irreducible de G es isomorfa a una subrepresentación de la representación regular. De esta manera se podría conocer el número de representaciones irreducibles. En la siguiente sección se desarrollará una herramienta muy útil para este propósito.

Teorema 1.3 *Sean G un grupo finito y K un cuerpo tal que su característica no divide al orden de G. Toda representación irreducible (ρ, S) de G es isomorfa a una subrepresentación de la representación regular.*

Demostración:
Sea S el espacio de representación y sea $x \in S$ no nulo. Notaremos la acción de G sobre S como $\rho(g)(t) = g.t, \forall\ t \in S$. Consideremos

$$K[G]x = \{\textstyle\sum_{g\in G} \lambda_g(g.x) :\ \lambda_g \in K\}.$$

Es claro que $K[G]x$ es invariante por la acción de G y que $x \in K[G]x$. Al ser (ρ, S) irreducible y K[G]x un G-submódulo de S, tenemos que $K[G]x = S$. Sea (φ, V) la representación regular de G, y sea $\pi : V \to S$ la aplicación lineal suryectiva definida de la siguiente manera: si $w \in V$, entonces w se escribe de la forma $\sum_{g\in G} \lambda_g.v_g$ para ciertos $\lambda_g \in K$. Entonces sea

$$\pi(\textstyle\sum_{g\in G} \lambda_g.v_g) := \sum_{g\in G} \lambda_g(g.x).$$

Mediante un simple cálculo se puede ver que π conmuta con la accíon de G, es decir, π resulta ser un morfismo de representaciones. En efecto,

$$\begin{aligned} \pi(h.\textstyle\sum_{g\in G} \lambda_g.v_g) &= \pi(\textstyle\sum_{g\in G} \lambda_g h.v_g) = \pi(\textstyle\sum_{g\in G} \lambda_g.v_{hg}) \\ &= \textstyle\sum_{g\in G} \lambda_g(h.g.x) = h.(\textstyle\sum_{g\in G} \lambda_g.(g.x)) \\ &= h.\pi(\textstyle\sum_{g\in G} \lambda_g.v_g). \end{aligned}$$

Sea K=ker(π), siguiendo la demostración del teorema de completa reducibilidad se sigue que K es un G-módulo que admite un complemento L, invariante por la acción de G tal que $V = K \oplus L$.

Sea f:= $\pi|_L : L \to S$ la aplicación lineal definida por la restricción de π al subespacio L. Como ker(f)=0, se tiene que f es un inyectiva. Al ser S irreducible, $f \neq 0$ e im(f) un G-submódulo de S, se tiene que im(f)=S lo que implica que f es suryectiva. Por tanto, f resulta ser un isomorfismo de G-módulos entre L y S, es decir, (ρ, S) es isomorfa a una subrepresentación de la representación regular. □

1.4. Teoría de caracteres

Una vez que sabemos que toda representación de un grupo finito G sobre un cuerpo K, tal que su característica no divide al orden del grupo, nos interesa conocer la cantidad de representaciones irreducibles involucradas en la descomposición en suma directa y la cantidad de sumandos isomorfos a una representación irreducible dada. Para encontrar los G-submódulos simples de un G-módulo V, basta con encontrar subespacios invariantes por la acción de G, que resulten irreducibles como espacios de representación. Estos son fáciles de hallar una vez que se conocen los autovectores asociados a los isomorfismos $\rho(x), \forall\ x \in G$. Sin embargo, veremos que sólo es necesario conocer la suma de los autovalores de cada uno de ellos.

Definición 6 *Si* (ρ, V) *es una representación de G, su* **carácter** χ_V *es una función a valores complejos sobre el grupo G definida por*

$$\chi_V(g) = Tr(\rho|_V(g)).$$

En particular, cuando la representación es de dimensión 1, los isomorfismos $\rho(g)$ son escalares no nulos $\forall\, g \in G$. Luego, el carácter está definido por $\chi(g) = \rho(g)$ y verifica que $\chi(gh) = \chi(g)\chi(h), \forall\, h, g \in G$. Por tanto, el carácter resulta un morfismo de grupos entre G y el grupo de los escalares no nulos de K; es decir, χ es un carácter multiplicativo.

La aparición de la traza en la definición aporta importantes propiedades:

Proposición 1.1 *Si* χ *es el carácter de una representación* ρ *de dimensión n, entonces*

$$\begin{array}{ll} a) & \chi(1) = n, \\ b) & \chi(s^{-1}) = \overline{\chi(s)}, \\ c) & \chi(tst^{-1}) = \chi(s). \end{array}$$

Demostración:
a) Como $\rho(1) = I$ y $Tr(I) = n$ por ser V de dimensión n, es claro que $\chi(1) = n$.

b) Al ser G de orden finito y ρ una representación, tenemos que $\rho(s)$ es de orden finito para todo $s \in G$. Luego sus autovalores $\lambda_1, ..., \lambda_n$ son raíces de la unidad de módulo 1. Entonces

$$\begin{aligned} \overline{\chi(s)} &= \overline{Tr(\rho(s))} = \textstyle\sum_{i=1}^{n} \overline{\lambda_i} \\ &= \textstyle\sum_{i=1}^{n} {\lambda_i}^{-1} = Tr(\rho(s)^{-1}) \\ &= \chi(s^{-1}). \end{aligned}$$

Para demostrar *c)* no hace falta más que agregar que para todo par A, B de endomorfismos de GL(V) se cumple la fórmula $Tr(AB) = Tr(BA)$. □

Definición 7 *Decimos que una función f sobre G es una* **función central** *si cumple que* $f(st) = f(ts)\ \forall\, s, t \in G$.

Observación: Equivalentemente, f es una función central si verifica que $f(t^{-1}st) = f(s)$. En particular, la función resulta constante sobre las orbitas definidas por la acción de G sobre sí mismo a través de la conjugación. Por este motivo también se las suele llamar *función de clases.*

Proposición 1.2 *Sean* (ρ_1, V_1) *y* (ρ_2, V_2) *dos representaciones lineales de G, y sean* χ_{V_1} *y* χ_{V_2} *sus caracteres. Entonces*

a) El carácter $\chi_{V_1 \oplus V_2}$ *de la representación suma directa* $V_1 \oplus V_2$ *viene dado por* $\chi_{V_1} + \chi_{V_2}$.

b) El carácter $\chi_{V_1 \otimes V_2}$ *de la representación producto tensorial* $V_1 \otimes V_2$ *viene dado por* $\chi_{V_1} . \chi_{V_2}$.

Demostración:
Expresemos ρ_1 y ρ_2 en forma matricial R_1 y R_2 para tener un mejor manejo de sus caracteres. Como vimos antes, la forma matricial de $V_1 \oplus V_2$ es

$$\begin{pmatrix} R_1(s) & 0 \\ 0 & R_2(s) \end{pmatrix}, \tag{3}$$

de donde se deduce fácilmente que $Tr(R(s)) = Tr(R_1(S)) + Tr(R_2(s))\ \forall\ s \in G$, es decir que

$$\chi_{V_1 \oplus V_2}(s) = \chi_1(s) + \chi_2(s).$$

Para demostrar *b)* fijemos $\{u_i\}_{i=1}^n$ y $\{v_i\}_{i=1}^m$ bases de V_1 y V_2 respectivamente, tal que las formas matriciales sean de la forma $R_1(s) = (r_{ij})$ y $R_2(s) = (t_{ij})$. Luego, $\{u_i \otimes v_j\}_{i,j}$ es una base para el producto tensorial y si

$$R_1(s)(u_i) = \sum_{k=1}^n r_{ik}(s).u_k, \quad R_2(s)(v_j) = \sum_{l=1}^m t_{jl}(s).v_l,$$

entonces

$$\begin{aligned} R(s)(u_i \otimes v_j) &= R_1(s)(u_i) \otimes R_2(s)(v_j) \\ &= \sum_{k=1}^n r_{ik}(s).u_k \otimes \sum_{l=1}^m t_{jl}(s).v_l \\ &= \sum_{k,l} r_{ik}.r_{jl}(s).u_k \otimes v_l. \end{aligned}$$

Por definición se tiene que

$$\chi_{V_1}(s) = \sum_{i=1}^n r_{ii}(s), \qquad \chi_{V_2}(s) = \sum_{j=1}^m t_{jj}(s),$$

$$\chi_{V_1 \otimes V_2}(s) = \sum_{i,j} r_{ii}.t_{jj}(s) = \quad (\sum_{i=1}^n r_{ii}(s)).(\sum_{j=1}^m t_{jj}(s)).$$

Por tanto, tenemos que $\chi_{V_1 \otimes V_2}(s) = \chi_{V_1}(s).\chi_{V_2}(s)$ como se quería probar. □

1.4.1. Lema de Schur y algunas fórmulas

Salvo que se mencione lo contrario, supondremos de aquí en más que el cuerpo es algebraicamente cerrado.

Lema 1.1 *(Lema de Schur).*

Sean (ρ_1, V_1) y (ρ_2, V_2) dos representaciones irreducibles de G y sea f una aplicación lineal de V_1 en V_2 tal que $\rho_2(s)f = f\rho_1(s)\ \forall s \in G$.

a) Si (ρ_1, V_1) y (ρ_2, V_2) no son isomorfas, entonces f=0.

b) Si $V_1 = V_2$ y $\rho_1 = \rho_2$, entonces f es una homotecia, es decir, un múltiplo escalar de la identidad.

Demostración:
Si $f = 0$ no hay nada que demostrar. Supongamos que $f \neq 0$ y sea N su núcleo. Dado $x \in N$, $\rho_2(s)(f(x)) = f(\rho_1(s)(x)) = 0$, esto implica que $\rho_1(s)(x) \in N\ \forall\ s \in G$, y esto implica que N es G-estable. Como V_1 es un espacio de representación irreducible, debe ser que $N = V_1$ *o* $N = 0$. El primer caso fue descartado desde el principio, por tanto N=0 y f resulta un monomorfismo. El mismo argumento muestra que si M es la imagen de f, entonces $M = V_2$ *o* $M = 0$; el segundo caso es el mismo que el primero anterior que fue descartado, luego debe ser que $M = V_2$, es decir f es un epimorfismo. Por tanto, f es un isomorfismo de V_1 en V_2 quedando la parte *a)* demostrada.

Supongamos ahora que $V_1 = V_2$ y que $\rho_1 = \rho_2$. Al estar trabajando sobre un cuerpo algebraicamente cerrado, sabemos que existe un $\lambda \in K$ que es un autovalor de f. Sea $f' = f - \lambda.I$; como λ es un valor propio de f, tenemos que el núcleo N de f' es no nulo. Por otra parte, es claro que $\rho_2(s)f' = f'\rho_1(s)\ \forall\ s \in G$, es decir, f' conmuta con la acción de G. Siguiendo los razonamientos anteriores se deduce que $N = V_1$ y por tanto $f' = f - \lambda.I = 0$.

Es decir, f es una homotecia. □

A partír de ahora, supondremos que la característica del cuerpo es cero y que $g = |G|$, el orden de G.

Corolario 1.1 *Sean (ρ_1, V_1) y (ρ_2, V_2) dos representaciones irreducibles de G sobre K. Sea h una aplicación lineal de V_1 en V_2 y sea*

$$h^0 = \frac{1}{g} \sum_{t \in G} (\rho_2(t))^{-1} h \rho_1(t).$$

Entonces

a) Si (ρ_1, V_1) y (ρ_2, V_2) no son isomorfas, entonces $h^0 = 0$.

b) Si $V_1 = V_2$, $\rho_1 = \rho_2$, entonces h^0 es una homotecia de razón $\frac{1}{n} Tr(h)$, siendo $n = dim(V_1)$.

Demostración:
Gran parte del corolario se deduce de manera inmediata del lema de Schur verificando simplemente la condición $\rho_2(s) h^0 = h^0 \rho_1(s) \ \forall \ s \in G$. Veamos

$$\begin{aligned} (\rho_2(s))^{-1} h^0 \rho_1(s) &= \frac{1}{g} \sum_{t \in G} (\rho_2(s))^{-1} (\rho_2(t))^{-1} h \rho_1(t) \rho_1(s) \\ &= \frac{1}{g} \sum_{t \in G} (\rho_2(ts))^{-1} h \rho_1(ts) \\ &= h^0. \end{aligned}$$

En el caso que $h^0 \neq 0$, $V_1 = V_2$ y $\rho_1 = \rho_2$, tenemos que h^0 es un escalar por la identidad. Luego, $Tr(\lambda.I) = n.\lambda$ y como

$$\begin{aligned} Tr(h^0) = &\ \frac{1}{g} \sum_{t \in G} Tr((\rho_2(t))^{-1}.h.\rho_1(t)) \\ &= \frac{1}{g} \sum_{t \in G} Tr(h) \\ &= Tr(h), \end{aligned}$$

tenemos que $n.\lambda = Tr(h)$. Por tanto debe ser $\lambda = \frac{Tr(h)}{n}$. □

Veamos ahora que significa el corolario 1.1 cuando las representaciones (ρ_1, V_1) y (ρ_2, V_2) se dan en forma matricial, $R_1(s) = (r_{ij}(s))$ y $R_2(s) = (t_{kl}(s))$.

Corolario 1.2 *Supongamos que, tomando las bases correspondientes a cada espacio, la matriz de la aplicación lineal h definida anteriormente es de la forma (x_{ki}) y la matriz de h^0 es de la forma (x^0_{ki}). Entonces,*

i) En las condiciones del ítem a) del corolario anterior tenemos que

$$\frac{1}{g} \sum_{s,j,l} t_{kl}(s^{-1}).r_{ji}(s) = 0, \quad \textit{cualesquiera que sean } i, j, k, l.$$

ii) En las condiciones del ítem b) del corolario anterior tenemos que

$$\begin{aligned} \frac{1}{g} \sum_{s,j,l} t_{kl}(s^{-1}).r_{ji}(s) &= \frac{1}{n} \delta_{ki}.\delta_{lj} \\ &= \begin{cases} \frac{1}{n} & \textit{si } i = k \textit{ y } j = l \\ 0 & \textit{en otro caso} \end{cases} \end{aligned}$$

Demostración:
Por la definición de h^0 se tiene que

$$x^0_{i_2 i_1} = \frac{1}{g}\sum_{s,j,k} t_{kl}(s^{-1}).x_{lj}.r_{ji}(s).$$

El segundo miembro de esta igualdad es una forma lineal en las variables x_{lj}; en el caso del ítem *a)* tenemos que esta forma lineal se anula para todo sistema de valores x_{lj}, por tanto sus coeficientes deben ser nulos, es decir

$$\frac{1}{g}\sum_{s,j,l} t_{kl}(s^{-1}).r_{ji}(s) = 0, \quad \text{cualesquiera que sean } i,k,j,l.$$

Suponiendo ciertas las condiciones del ítem *b)* tenemos que $h^0 = \lambda.I$, es decir, $x^0_{ki} = \lambda.\delta_{ki}$ donde $\lambda = \frac{Tr(h)}{n}$. Entonces

$$\lambda = \frac{1}{n}\sum \delta_{lj}.x_{lj}.$$

Considerando las igualdades anteriores se deduce que

$$x^0_{ki} = \frac{1}{g}\sum_{s,j,l} t_{kl}(s^{-1}).x_{lj}.r_{ji}(s) = \frac{1}{n}\sum_{j,l} \delta_{ki}.\delta_{lj}.x_{lj}.$$

Por tanto, igualando coeficiente a coeficiente se obtiene

$$\frac{1}{g}\sum_{s,j,l} t_{kl}(s^{-1}).r_{ji}(s) = \frac{1}{n}\sum_{j,l} \delta_{ki}.\delta_{lj},$$

como se quería probar. □

Supongamos por un momento que $K = \mathbb{C}$. Eligiendo convenientemente una base, podemos suponer que las matrices $(t_{kl}(s))$ son unitarias. Entonces tenemos que $t_{kl}(s^{-1}) = \overline{t_{kl}(s)}$, por tanto el corolario anterior se puede ver como relaciones de ortogonalidad de *caracteres*. Para ello, debemos introducir una noción de producto interno:

Sean φ y ψ dos funciones de G a valores complejos, definimos entonces una aplicación

$$(-,-) : \mathbb{C}^G \times \mathbb{C}^G \to \mathbb{C},$$

$$(\psi,\varphi) = \frac{1}{g}\sum_{t\in G} \psi(t)\overline{\varphi(t)}, \quad \text{siendo g el orden de G.}$$

Es claro que esta aplicación es lineal en la primera variable, semilineal en la segunda y que $(\varphi,\varphi) > 0$ si $\varphi \neq 0$; en particular, resulta un producto escalar.

Teorema 1.4 *a) Si χ_V es el carácter de una representación irreducible (ρ, V), entonces*

$$(\chi_V, \chi_V) = 1.$$

b) Si χ_V y $\chi_{V'}$ son dos caracteres de dos representaciones irreducibles no isomorfas, entonces $(\chi_V, \chi_{V'}) = 0$.

Demostración:
Supongamos que la dimensión del espacio de representación V es n. Luego, teniendo en cuenta la definición de producto interno, tenemos que

$$(\chi_V, \chi_V) = \frac{1}{g}\sum_{t\in G} \chi_V(t)\overline{\chi_V(t)} = \frac{1}{g}\sum_{t\in G} \chi_V(t)\chi_V(t^{-1}).$$

Si consideramos ρ en forma matricial $R(t) = (r_{ij}(t))$, tenemos que $\chi(t) = \sum_{t\in G} r_{ii}(t)$ deduciéndose entonces la siguiente igualdad:

$$(\chi_V, \chi_V) = \frac{1}{g}\sum_{t,i,j} r_{ii}(t)r_{jj}(t^{-1}).$$

Por el corolario anterior sabemos que $\frac{1}{g}\sum_{t\in G} r_{ii}(t)r_{jj}(t^{-1})$ es igual a 0 si $i \neq j$ y $\frac{1}{n}$ si $i = j$, entonces se tiene que

$$\frac{1}{g}\sum_{t,i,j} r_{ii}(t)r_{jj}(t^{-1}) = \frac{1}{g}\sum_{t,i}\frac{1}{n} = \frac{1}{g}\sum_{t\in G} 1 = 1.$$

Por tanto $(\chi_V, \chi_V) = 1$, como se quería demostrar.

Análogamente, se demuestra la parte *b)* escribiendo la igualdad en forma matricial y usando el corolario anterior. En efecto, si (ρ, V) y (ρ', V') son dos representaciones irreducibles no isomorfas cuyas formas matriciales viene dadas por $R(s) = (r_{ij})_{ij}$ y $R'(s) = (r'_{ij})_{ij}$ respectivamente, por la parte *a)* del corolario anterior vale que

$$(\chi_V, \chi_{V'}) = \frac{1}{g}\sum_{t,i,j} r_{ii}(t){r_{jj}}'(t^{-1}) = 0, \quad \text{para todo i, j.}$$

Es decir, χ_V y $\chi_{V'}$ son ortogonales con respecto a este producto escalar. □

Este teorema nos da una forma de conocer la cantidad de representaciones isomorfas a una representación irreducible dada:

Teorema 1.5 *Sea (ρ, V) una representación lineal de G de carácter χ_V, y descompongamos a V en suma directa de G-módulos simples.*

$$V = W_1 \oplus W_2 \oplus \ldots \oplus W_k.$$

Entonces, si (ρ, W) es una representación irreducible de carácter χ_W, el número de W_i isomorfas a W viene dado por (χ_W, χ_V).

Demostración:
Por la proposición 1.2 sabemos que el carácter χ_V se escribe de la forma

$$\chi_V = \chi_{W_1} + \chi_{W_2} + \cdots + \chi_{W_k}.$$

Por tanto $(\chi_W, \chi_V) = (\chi_W, \chi_{W_1}) + (\chi_W, \chi_{W_2}) + \cdots + (\chi_W, \chi_{W_k})$ y por el teorema anterior sabemos que (χ_W, χ_{W_i}) es 1 si son isomorfas y 0 si no lo son, luego (χ_W, χ_V) da la cantidad de W_i que son isomorfas a W. □

Observación: Como el producto escalar antes definido es independiente de la descomposición en suma directa de representaciones irreducibles, tenemos que el número de representaciones irreducibles (ρ_i, W_i) isomorfas a (ρ, W) no depende de la descomposición elegida. A este número se lo llama multiplicidad de W en V o "número de veces que W está en V". De esta manera, se adquiere un sentido de unicidad en la descomposición en suma directa de representaciones irreducibles.

Sean $\chi_1, \chi_2, ..., \chi_k$ los caracteres de las clases de isomorfismos de representaciones irreducibles de G y $(\rho_1, W_1), (\rho_2, W_2), ..., (\rho_k, W_k)$ representantes para cada clase, de grados $n_1, ..., n_k$ respectivamente.

Entonces, todo espacio de representación V es isomorfo a una suma directa

$$V \cong m_1W_1 \oplus m_2W_2 \oplus \ldots \oplus m_kW_k, \quad \text{donde } m_i \in \mathbb{N}.$$

Luego, el carácter χ_V de (ρ, V) es igual a $m_1\chi_1 + m_2\chi_2 + ... + m_k\chi_k$, donde $m_i = (\chi_V, \chi_i)$. Por las relaciones de ortogonalidad se tiene que

$$(\chi_V, \chi_V) = \textstyle\sum_{i=1}^{k} m_i^2.$$

Esto da lugar al siguiente teorema que provee un criterio de irreducibilidad muy útil:

Teorema 1.6 *Si χ_V es el carácter de una representación (ρ, V), entonces $(\chi_V, \chi_V) = 1$ si y sólo si V es irreducible*

Demostración:
Si $(\chi_V, \chi_V) = \sum_{i=1}^{k} m_i^2 = 1$ entonces debe ser que uno de los m_i es igual a 1 y todo los demás son nulos. Luego $\chi_V = \chi_i$ y por el corolario 1.3 tenemos que $V \cong W_i$, es decir, (ρ, V) es irreducible.

Si (ρ, V) es irreducible, por el teorema 1.4 tenemos que $(\chi_V, \chi_V) = 1$ como se quería demostrar. □

Definición 8 *Sean (ρ, V) una representación de G, (ρ, W) una subrepresentación irreducible. Supongamos que la descomposición de V en suma directa de irreducible es $V = W_1 \oplus W_2 \oplus \ldots \oplus W_k$ y que (ρ_i, W_i), con $i = 1, \ldots, s$, son representaciones irreducibles de G isomorfas a (ρ, W). La* **componente isotípica** *de tipo W es el espacio de representación dado por*

$$\overline{W} = \textstyle\bigoplus_{i=1}^{s} W_i, \quad W_i \cong W.$$

Si U es una subrepresentación irreducible de U isomorfa a W, entonces $U \subseteq \overline{W}$. En efecto, como U es una representación irreducible y $U \cap \overline{W}$ es una subrepresentación de U, debe ser que

$$U \cap \overline{W} = 0 \quad \text{ó} \quad U \cap \overline{W} = U.$$

Luego, si U no está incluida en $\overline{W}$ tenemos que $U \cap \overline{W} = 0$; en particular, queda definido el siguiente G-módulo $W^* = \overline{W} \oplus U$. Al ser el espacio de representaciones completamente reducible $(car(K) = 0)$, existe un G-submódulo U' de V tal que $V = W^* \oplus U'$. Por definición, sabemos que U' no contiene ninguna representación irreducible isomorfa a W, luego tenemos una nueva descomposición de V en suma directa $V = \bigoplus_{i=1}^{s} W_i \oplus U \oplus U'$, que tiene distinta cantidad de representaciones irreducibles isomorfas a W, lo cual es absurdo. Por tanto, debe ser que $U \subseteq \overline{W}$.

En particular, del párrafo anterior se deduce que la componente isotípica no depende de la descomposición en suma directa de representaciones irreducibles.

De esta manera, se obtiene una descomposición de la representación regular que no depende de elecciones de representantes de clases de isomorfismos de representaciones irreducibles. Esta es la *descomposición canónica* de la representación regular (V, ρ) y está dada por

$$V = V_1 \oplus V_2 \oplus \ldots \oplus V_k, \qquad \text{donde } V_i \text{ son las componentes isotípicas de V.}$$

Además de poder reconocer si una representación es irreducible a través de su carácter, también podemos determinar si dos representaciones dadas son isomorfas o no.

Corolario 1.3 *Dos representaciones (ρ_1, V) y (ρ_2, W) son isomorfas si y sólo si tienen el mismo carácter.*

Demostración:
Sean (ρ_1, V) y (ρ_2, W) dos representaciones de G sobre K. Si las *representaciones* son isomorfas entonces

existe un isomorfismo $\tau : V \to W$ tal que $\rho_2(s)\tau = \tau\rho_1(s), \forall\ s \in G$. Luego, $Tr(\rho_2(s)) = Tr(\tau\rho_1(s)\tau^{-1}) = Tr(\rho_1(s)), \forall\ s \in G$, es decir que $\chi_V(s) = \chi_W(s)$.

Si ambas representaciones tienen el mismo carácter, por el teorema anterior contienen el mismo número de veces a cualquier representación irreducible dada. Esto dice que sus descomposiciones en suma directa de representaciones irreducibles son isomorfas; en particular, las representaciones resultan isomorfas.

$\square$

Estos resultados confirman la idea de que, cuando el cuerpo es algebraicamente cerrado y su característica no divide al orden del grupo, el carácter de una representación "caracteriza" dicha representación, permitiendo de esta forma reducir el estudio de representaciones al de caracteres.

Lema 1.2 *Sean V un G-módulo y $(V_i)_{1\leq i\leq n}$ una familia de G-submódulos de V irreducibles tales que V_i no es isomorfa a V_j, si $i \neq j$. Entonces la suma $\sum_{i=1}^n V_i$ es una suma directa.*

Demostración:
Demostraremos el lema por inducción en la cantidad de elementos de la familia. Si la cantidad de submódulos irreducibles es 1, es decir, si V_1 es irreducible, no hay nada que probar. Supongamos que es cierto para n y probémoslo para $n+1$, o sea, que $\sum_{i=1}^{n+1} V_i$ es una suma directa. Es claro que

$$\begin{aligned}\textstyle\sum_{i=1}^{n+1} V_i &= \textstyle\sum_{i=1}^{n} V_i + V_{n+1}\\ &= \textstyle\bigoplus_{i=1}^{n} V_i + V_{n+1}.\end{aligned}$$

Luego, para demostrar que la suma es directa, basta probar que $V_{n+1} \cap \sum_{i=1}^n V_i = 0$. Sean χ_i los caracteres irreducibles correspondientes a los espacios de representación V_i, donde $1 \leq i \leq n+1$. Entonces, es claro que el carácter correspondiente al espacio de representación $\sum_{i=1}^n V_i$ está dado por $\sum_{i=1}^n \chi_i$. Por tanto,

$$\left(\textstyle\sum_{i=1}^n \chi_i,\ \chi_{n+1}\right) = \textstyle\sum_{i=1}^n (\chi_i,\ \chi_{n+1}) = 0,$$

puesto que los espacios de representación V_i, $1 \leq i \leq n+1$ son no isomorfos entre sí. En particular, se deduce que la suma $\sum_{i=1}^{n+1} V_i$ es directa. $\square$

Como una consecuencia inmediata del lema anterior tenemos el siguiente

Corolario 1.4 *Si $(V_i)_{1\leq i\leq N}$ es una familia de G-submódulos irreducibles de V, tales que V_i no es isomorfo a V_j, si $i \neq j$, entonces $N \leq dim(V)$.*

Demostración:
Supongamos que V_i es un G-módulo simple no nulo, luego $1 \leq dim(V_i)$. Entonces

$$N = 1 + 1 + \cdots + 1 \leq \quad \textstyle\sum_{i=1}^n dim(V_i) \quad \leq dim(V).$$

$\square$

Sabemos que toda representación irreducible es isomorfa a una subrepresentación de la representación regular (ρ, V); en particular si el grupo tiene orden finito, entonces la dimensión del espacio de representación V es finita y del corolario anterior se deduce que

Corolario 1.5 *Hay sólo un número finito de clases de isomorfismos de representaciones irreducibles.*

Se sigue que hay un número finito de caracteres irreducibles. Esto también surge de las relaciones de ortogonalidad $(\chi_V,\ \chi_W) = \delta_{V,\ W}$, si $V,\ W$ son irreducibles, puesto que

$$\{\chi_V :\ V \text{ es irreducible}\},$$

es un sistema ortonormal de funciones de clases.

Notemos que toda la información que necesitamos sobre las representaciones de G viene dada por una representación, luego basta conocer bien esta representación para caracterizar al grupo. Analicemos entonces algunos hechos sobre la representación regular:

Proposición 1.3 *El carácter φ de la representación regular viene dado por la siguiente fórmula:*

$$\begin{aligned} \varphi(1) &= g, && \text{siendo g el orden de G.} \\ \varphi(s) &= 0, && \text{si } s \neq 1. \end{aligned}$$

Demostración:
Sea V un espacio vectorial de dimensión g, fijemos una base $(e_s)_{s\in G}$ indexada por elementos de G. La representación regular viene dada por su acción sobre la base: $\rho(t)(e_s) = e_{ts}$. Si $t \neq 1$ entonces $ts \neq s, \forall\ s \in G$ y por tanto, los elementos de la diagonal de la matriz de $\rho(t)$ son todos nulos; en particular $Tr(\rho(t)) = 0$, es decir, $\varphi(t) = 0$ para todo $t \neq 1 \in G$. Si t=1, se tiene que $\rho(1)(e_s) = e_s$, por tanto $Tr(\rho(1)) = g$, es decir $\varphi(1) = g$. $\square$

Antes dijimos que toda representación irreducible es isomorfa a una subrepresentación de la representación regular y que la cantidad de estas representaciones es finita. Esto quiere decir que toda representación irreducible está contenida por lo menos una vez en la representación regular y hay a lo sumo tantas como el orden del grupo, si éste es finito. El siguiente corolario da la cantidad de veces que la regular lo contiene:

Corolario 1.6 *Cada representación irreducible (ρ_i, W_i) está contenida en la representación regular un número de veces igual a su grado n_i.*

Demostración:
Por el teorema 1.5, este número viene dado por (χ_i, φ), donde φ es el carácter de la representación regular. Luego,

$$(\chi_i, \varphi) = \frac{1}{g}\sum_{t\in G} \chi_i(t)\varphi(t^{-1}) = \frac{1}{g}\chi_i(1)g = \chi_i(1) = n_i$$

$\square$

De esta manera, si V es el espacio de representación de dimensión n inducido por la representación regular se tiene que

$$V \cong n_1W_1 \oplus n_2W_2 \oplus \ldots \oplus n_kW_k.$$

y por tanto su carácter será

$$\varphi = n_1\chi_1 + \cdots + n_k\chi_k. \tag{4}$$

Luego, usando las relaciones de ortogonalidad se deduce que

$$\sum_{i=1}^{k} n_i^2 = g.$$

En efecto, aplicada a 1 la igualdad (4) nos da que $g = \varphi(1) = \sum_{i=1}^{k} n_i\chi_i(1) = \sum_{i=1}^{k} n_i^2$. La igualdad anterior desempeña un papel importante en la teoría ya que permite saber cuando se encuentran *todas* las representaciones irreducibles del grupo G.

Resumamos en un ejemplo lo visto hasta aquí: Sea $\mathbb{S}_3$ el grupo de permutaciones de tres elementos. Hallemos todas las representaciones irreducibles de $\mathbb{S}_3$ sobre $\mathbb{C}$.

Sabemos que el orden del grupo es $3! = 6$, entonces si $W_1, \ldots, W_k$ son las representaciones irreducibles de grados $n_1, \ldots, n_k$ respectivamente, debe ser que $6 = {n_1}^2 + \cdots + {n_k}^2$.

La idea es encontrar algunas representaciones irreducibles y luego probar que son todas. Consideremos primero la representación trivial de G sobre un espacio U de dimensión 1. Entonces $\rho_U : \mathbb{S}_3 \to \mathbb{C}^*$ y esta definida por $\rho(\sigma) = 1, \forall\, \sigma \in \mathbb{S}_3$. Por ser unidimensional, esta representación resulta irreducible; en particular se verifica trivialmente que $(\chi_U, \chi_U) = 1$. En efecto,

$$(\chi_U, \chi_U) = \tfrac{1}{6} \textstyle\sum_{\sigma \in \mathbb{S}_3} \chi_U(\sigma)\chi_U(\sigma^{-1}) = \tfrac{1}{6} \sum_{\sigma \in \mathbb{S}_3} 1 = 1.$$

Para encontrar las representaciones irreducibles restantes, definiremos a continuación representaciones del grupo simétrico $\mathbb{S}_n$ para todo n sobre un cuerpo arbitrario K. En particular, estas definiciones nos darán los $\mathbb{S}_3$-módulos simples que estamos buscando.

Por diversos motivos que se verán más adelante, a cada permutación queremos asociarle un signo ± 1 de manera tal que quede definido un morfismo de grupos. Hay varias maneras de hacer esto, sin embargo, lo haremos de la manera tradicional evitando demostraciones engorrosas.

Sean $\sigma \in \mathbb{S}_n$ y $\{e_1, \ldots, e_n\}$ la base canónica de $\mathbb{Z}^n$. Consideremos la transformación lineal $\pi(\sigma)$ definida por

$$\pi(\sigma) : \mathbb{Z}^n \to \mathbb{Z}^n, \quad (\pi(\sigma))(e_i) = e_{\sigma(i)}.$$

Definimos entonces la función signo $sg : \mathbb{S}_n \to \pm 1$ de la siguiente manera

$$sg(\sigma) = det(\pi(\sigma)).$$

Es claro que la función signo resulta un morfismo de grupos y, por ser el determinante una función multilineal y alternada, para toda trasposición $\tau \in \mathbb{S}_n$ se verifica que $sg(\tau) = -1$.

En particular, si $\sigma = \tau_1\tau_2 \ldots \tau_m$ es un producto de trasposiciones, entonces $sg(\sigma) = (-1)^m$. Por una cuestión de terminología, llamaremos a las permutaciones *pares* si $sg(\sigma) = 1$ e *impares* si $sg(\sigma) = -1$. Las permutaciones pares constituyen el núcleo de sg, que se denomina el *grupo alternado* $\mathcal{A}_n$.

El morfismo sobre $\mathbb{S}_n$ se denomina la función **signo o signatura**. Como el morfismo no depende de la escritura de la permutación σ como producto de ciclos, su cálculo es bastante fácil, ya que como toda permutación se puede escribir como producto de trasposiciones, su signatura será $(-1)^m$, siendo m la cantidad de trasposiciones involucradas en la escritura.

Consideremos ahora la representación sobre un espacio U' de dimensión 1, dada por

$$\rho_{U'}(\sigma) = sg(\sigma),$$

Esta representación de $\mathbb{S}_n$ se denomina la **representación signo**; de manera análoga a la representación trivial es una representación irreducible por ser unidimensional.

Si n es impar y el cuerpo K es de característica cero, estas dos representaciones resultan no isomorfas, ya que todo isomorfismo lineal sobre K es un múltiplo escalar de la identidad y estas dos representaciones no son una múltiplo de la otra.

De esta manera, como suponemos que $K = \mathbb{C}$ en nuestro ejemplo, hemos encontrado otro $\mathbb{S}_3$-módulo irreducible. Para encontrar todas las representaciones irreducibles de $\mathbb{S}_3$ no isomorfas entre sí basta encontrar una representación irreducible de dimensión 2 o cuatro representaciones irreducibles de dimensión 1 no isomorfas entre sí, ni a las anteriores.

Consideremos el subespacio de K^n definido por:

$$V = \{(x_1, \ldots, x_n) \in K^3 : \ x_1 + \cdots + x_n = 0\}.$$

La acción de $\mathbb{S}_n$ sobre V está dada por:

$$\rho_V : \mathbb{S}_n \to GL(V),$$

$$\rho_V(\sigma)(x_1, \ldots, x_n) = (x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

Es claro que V es de dimensión $n-1$ y que la acción de G es estable sobre V. Por tanto, (ρ_V, V) resulta una representación de G de grado $n-1$ sobre K. Esta representación se denomina la **representación estándar** de $\mathbb{S}_n$.

Veamos que ésta es una representación irreducible de $\mathbb{S}_3$ si $K = \mathbb{C}$. Sea χ_V su carácter. Luego basta verificar que $(\chi_V, \chi_V) = 1$. Por definición, sabemos que

$$\chi_V(\sigma) = Tr(\rho_V(\sigma)|_V) \quad \text{y que} \quad (\chi_V, \chi_V) = \textstyle\sum_{\sigma \in \mathbb{S}_3} \chi_V(\sigma)\overline{\chi_V(\sigma)}.$$

Entonces, fijemos una base de V y calculemos la traza de cada elemento $\rho_V(\sigma)$, $\sigma \in \mathbb{S}_3$. Sea $B = \{(1, 0, -1),\ (0, 1, -1)\}$, mediante un simple cálculo se puede ver que B es base de V y que la forma matricial de ρ_V y su carácter χ_V están dados por:

$$\rho_V(id) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \chi_V(id) = 2,$$

$$\rho_V(1\ 2) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \chi_V(1\ 2) = 0,$$

$$\rho_V(1\ 3) = \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}, \qquad \chi_V(1\ 3) = 0,$$

$$\rho_V(2\ 3) = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}, \qquad \chi_V(2\ 3) = 0,$$

$$\rho_V(1\ 2\ 3) = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \qquad \chi_V(1\ 2\ 3) = -1,$$

$$\rho_V(1\ 3\ 2) = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \qquad \chi_V(1\ 3\ 2) = -1.$$

Por tanto se tiene que $(\chi_V, \chi_V) = \frac{1}{6}\sum_{\sigma \in \mathbb{S}_3} \chi_V(\sigma)\overline{\chi_V(\sigma)} = 1$; en particular, V resulta irreducible.

Observar que ésta es la representación discutida anteriormente para $\mathbb{D}_3 \cong \mathbb{S}_3$ la cual da las permutaciones de un triángulo equilátero. Veremos más adelante que la representación estándar de $\mathbb{S}_n$ es una representación irreducible de dimensión $n-1$, siempre y cuando la característica del cuerpo no divide al orden del grupo.

Entonces, si W es el espacio de representación de dimensión 6 inducido por la representación regular y φ su carácter, debe ser que

$$W \cong U \oplus U^{'} \oplus 2V,$$

$$\varphi = \chi_U + \chi_{U'} + 2\chi_V.$$

En consecuencia, tenemos que la representación trivial (ρ_U, U), la representación signo $(\rho_{U'}, U^{'})$ y la representación estándar (ρ_V, V) son todas las representaciones irreducibles de $\mathbb{S}_3$ sobre $\mathbb{C}$ salvo isomorfismos.

1.4.2. Número de representaciones irreducibles

En el parágrafo anterior vimos que la cantidad de clases de isomorfismo de representaciones irreducibles de un grupo finito es finita y es igual a la cantidad de clases de isomorfismos de subrepresentaciones irreducibles de la representación regular. Como otra aplicación del lema de Schur y de la teoría de caracteres daremos su número exacto. Recordamos que $g = |G|$ y que K es algebraicamente cerrado y de característica cero.

Proposición 1.4 *Sean f una función de clases definida en G y (ρ, V) una representación lineal de G. Sea ρ_f el endomorfismo de V definido por la fórmula:*

$$\rho_f = \textstyle\sum_{t\in G} f(t)\rho(t).$$

Si V es irreducible, de grado n y de carácter χ_V, entonces ρ_f es una homotecia de razón λ, donde

$$\lambda = \tfrac{1}{n}\textstyle\sum_{t\in G} f(t)\chi_V(t) = \tfrac{g}{n}(\chi_V, \overline{f}).$$

Demostración:
Por el lema se Schur, sabemos que ρ_f es una homotecia si se verifica que $\rho(s)\rho_f = \rho_f\rho(s), \forall\ s \in G$. Por tanto, calculemos $(\rho(s))^{-1}\rho_f\rho(s)$:

$$(\rho(s))^{-1}\rho_f\rho(s) = \textstyle\sum_{t\in G} f(t)(\rho(s))^{-1}\rho(t)\rho(s) = \sum_{t\in G} f(t)(\rho(s^{-1}ts)),$$

si tomamos $u = s^{-1}ts$ y lo aplicamos a la igualdad anterior, tenemos que

$$\begin{aligned}(\rho(s))^{-1}\rho_f\rho(s) &= \textstyle\sum_{u\in G} f(sus^{-1})\rho(u)\\ &= \textstyle\sum_{u\in G} f(t)\rho(u)\\ &= \rho_f, \quad \forall\ s\in G.\end{aligned}$$

Como la traza de una homotecia de razón λ debe ser $\lambda.n$ y la traza de ρ_f es

$$Tr(\rho_f) = \textstyle\sum_{t\in G} f(t)Tr(\rho(t)) = \sum_{t\in G} f(t)\chi_V(t),$$

debe ser que

$$\lambda = \tfrac{1}{n}\textstyle\sum_{t\in G} f(t)Tr(\rho(t)) = \tfrac{g}{n}(\chi_V, \overline{f}),$$

como se quería demostrar. $\square$

Consideremos el espacio vectorial H de las funciones de clases de G. Es claro que los caracteres $\chi_1, ..., \chi_k$ de las clases de isomorfismo de las representaciones irreducibles de G son elementos de H; más aún, veremos que forman una base de este espacio vectorial.

Teorema 1.7 *Los caracteres $\chi_1, ..., \chi_k$ de las clases de isomorfismo de las representaciones irreducibles forman una base ortonormal de H.*

Demostración:
Por el teorema 1.4 sabemos que los caracteres $\chi_1, ..., \chi_k$ forman un sistema ortonormal con respecto al producto interno que se definió en las secciones anteriores. Luego, falta sólo demostrar que este sistema es completo.

Supongamos que existe una función $f \in H$ que es ortonormal a $\chi_j, \forall\ j = 1, ..., k$ y demostremos que debe ser nula.

Sea (ρ, V) una representación de G, y sea $\rho_{\overline{f}}$ definido por:

$$\rho_{\overline{f}} = \sum_{t \in G} \overline{f(t)} \rho(t).$$

La proposición anterior muestra que $\rho_{\overline{f}}$ es nula si V es irreducible; se V no es irreducible, decomponiéndolo es suma directa de irreducibles se deduce que $\rho_{\overline{f}}$ es nula sobre V.

Apliquemos este resultado a la representación regular (ρ, R) y calculemos la imagen del vector e_1 de la base por $\rho_{\overline{f}}$:

$$\rho_{\overline{f}}(e_1) = \sum_{t \in G} \overline{f(t)} \rho(t)(e_1) = \sum_{t \in G} \overline{f(t)} e_t.$$

Como $\rho_{\overline{f}}$ es nula sobre R, esta igualdad implica que $f(t) = 0, \forall\ t \in G$; es decir que f es nula y entonces $\{\chi_1, ..., \chi_k\}$ es un sistema ortonormal. $\square$

Recordemos la acción de G sobre sí mismo dada por la representación adjunta, esto es

$$ad(s)(t) = s^{-1} t s, \forall\ s, t \in G.$$

Esta acción se denomina conjugación y divide a G en *órbitas* de conjugación. Si un elemento de G es imagen de otro por la representación adjunta, diremos que estos elementos son conjugados.

Teorema 1.8 *El número de clases de isomorfismo de representaciones irreducibles de G es igual al número de clases de conjugación de G. En particular, la cantidad de clases de isomorfismo de representaciones irreducibles divide al orden de G.*

Demostración:
Supongamos que $C_1, ..., C_h$ son las clases de conjugación de G. Es fácil ver que una función f es de clases si y sólo si es constante en cada una de las clases $C_1, ..., C_h$. En consecuencia, tal función esta determinada por h valores $\lambda_1, ..., \lambda_h$ que se pueden elegir arbitrariamente. Por tanto, la dimensión del espacio vectorial H de funciones de clases es igual a h. Por otra parte, debido al teorema anterior, sabemos que esta dimensión es igual a la cantidad de clases de isomorfismo de representaciones irreducibles, luego debe ser que $h = k$ como se quería demostrar. $\square$

Como rápida consecuencia del teorema se obtiene algunas fórmulas:

Sean $s \in G$, c_s el número de elementos de la clase de conjugación de s y f_s la función que asigna el valor 1 a todo elemento de esta clase y 0 a los demás. Por definición esta función resulta de clases, por tanto se tiene que existen $x_1, ...x_k \in K$ tal que

$$f_s = \sum_{i=1}^{h} x_i \chi_i, \quad \text{donde } x_i = (f_s, \chi_i) = \tfrac{c_s}{g} \overline{\chi_i(s)}.$$

Entonces, para todo $t \in G$ vale que

$$f_s(t) = \tfrac{c_s}{g} \sum_{i=1}^{h} \overline{\chi_i(s)} \chi_i(t).$$

Luego, por la definición de f_s, tenemos que

$$\sum_{i=1}^{h} \overline{\chi_i(s)} \chi_i(t) = \tfrac{c_s}{g}, \quad \text{si } t \in C_s,$$

$$\sum_{i=1}^{h} \overline{\chi_i(s)} \chi_i(t) = 0 \qquad \text{si } t \notin C_s.$$

Una aplicación del teorema anterior es la siguiente:

Proposición 1.5 *Sea G un grupo finito. G es conmutativo si y sólo si todas sus representaciones irreducibles son de dimensión 1.*

Demostración:
Supongamos que G es conmutativo y que (ρ, V) es una representación irreducible de G, luego $st = ts, \forall\ s, t \in G$, y como ρ es un morfismo de grupos, vale que $\rho(s)\rho(t) = \rho(t)\rho(s), \forall\ s, t \in G$. Según el lema de Schur, $\rho(t)$ es una homotecia para todo $t \in G$ y por tanto todo subespacio vectorial de V es estable por la acción de G; como V es irreducible debe ser que $dim(V) = 1$.

Supongamos ahora que todas las representaciones de G son de dimensión 1 y probemos que G es conmutativo. Si g es el orden de G, entonces $g = \sum {n_i}^2$, donde los n_i designan los grados de las representaciones irreducibles. Como aquí los n_i son todos iguales a 1, se deduce que la cantidad de clases de isomorfismo de representaciones irreducibles es igual a g. Por otra parte, sabemos que este número es igual a la cantidad de clases de conjugación de G, por tanto hay tantas clases de conjugación como elementos de G y esto sólo es posible si G es conmutativo. □

Sea V una representación de G de dimensión finita. Por lo hecho anteriormente, sabemos que el carácter χ_V de V es una combinación lineal de coeficientes positivos de los caracteres de las representaciones irreducibles. Veremos en los siguientes capítulos que es bastante productivo extender la idea al caso en que los coeficientes son enteros no necesariamente positivos. Este paso significativo fue tomado por Brauer, en su trabajo sobre la aplicación de la teoría de representaciones aplicada al estudio de las L- funciones de Artin. Definimos entonces

$$ch\ KG = \bigoplus_i \mathbb{Z} \cdot \chi_i = \{\sum_i a_i \chi_i : a_i\ \in \mathbb{Z}\}.$$

Definición 9 *A los elementos de ch KG los llamaremos* **caracteres virtuales** *de G sobre K.*

Es fácil ver que este conjunto tiene una estructura de anillo, cuyas operaciones están inducidas por la suma directa y el producto tensorial de las representaciones de G sobre K.

Para facilitar el manejo de las representaciones de un grupo finito G dado, se suele incorporar toda la información básica de los caracteres de las representaciones irreducibles de G en una tabla. Esta tabla se denomina *tabla de caracteres*. Veamos como se construye a través de un ejemplo:

Sea G=$\mathbb{S}_3$ el grupo de permutaciones de tres elementos. Sabemos que su orden es $3! = 6$ y que las representaciones irreducibles son la trivial (ρ_U, U) y la representación signo $(\rho_U^{'}, U^{'})$, ambos de grado 1 y la representación estándar (ρ_V, V) de grado 2, cuyos caracteres son $\chi_U,\ \chi_{U'},\ \chi_V$ respectivamente.

La tabla se compone de las clases de conjugación C_i de G (usualmente dadas por un elemento de la clase), en el borde superior, la cantidad de elementos en cada clase de conjugación sobre ésta, los G-módulos simples sobre el borde izquierdo y en cada lugar correspondiente, el valor de los caracteres χ_W evaluados en cada clase de conjugación C_i.

Sabemos que $\mathbb{S}_3$ tiene tres clases de conjugación dadas por $C_1 = [id],\ C_2 = [1\ 2],\ C_3 = [1\ 2\ 3]$. Es claro que, por ser (ρ_U, U) la representación trivial, χ_U toma los valores (1, 1, 1) en las clases de conjugación, mientras que el carácter $\chi_{U'}$ de la representación signo toma los valores (1, -1, 1). Por un ejemplo anterior, sabemos que el carácter χ_V de la representación estándar viene dado por (2, 0, -1). En conclusión, la tabla de caracteres será:

	1	3	2
$\mathbb{S}_3$	id	(1 2)	(1 2 3)
la trivial U	1	1	1
signo $U^{'}$	1	-1	1
la estándar V	2	0	-1

.

1.4.3. Propiedades de integriadad de los caracteres

Definición 10 *Sean R un anillo conmutativo y A una R-álgebra. Decimos que un elemento $\alpha \in A$ es* **íntegro** *sobre R si existe un polinomio mónico $f(X) \in R[X]$ tal que $f(\alpha) = 0$.*

Diremos que un elemento s de K es íntegro si s es íntegro sobre $\mathbb{Z}$. Por ejemplo, es bien sabido que si $a \in \mathbb{Q}$ es un elemento íntegro entonces $a \in \mathbb{Z}$.

Proposición 1.6 *Si χ es el carácter de una representación ρ de G, entonces $\chi(s)$ es íntegro para todo $s \in G$.*

Demostración:
Por definición, $\chi(s)$ es la traza del endomorfismo $\rho(s)$, que es igual a la suma de autovalores de $\rho(s)$. Si $g = |G|$, entonces $\rho(s)^g = \rho(s^g) = I$, lo cual implica que los autovalores de $\rho(s)$ son raíces de la unidad y por tanto elementos íntegros. Se sabe que los elementos íntegros forman un subanillo de K; en particular, $\chi(s)$ es íntegro.
□

Proposición 1.7 *Sean χ el carácter de una representación irreducible ρ de grado d, y C una clase de conjugación de G. Entonces $\frac{1}{d}\sum_{s\in C}\chi(s)$ es íntegro.*

Demostración:
Sea $Cent_K(G)$ y $Cent_{\mathbb{Z}}(G)$ los centros de $K[G]$ y $\mathbb{Z}[G]$, respectivamente. Es claro que los elementos $e_C = \sum_{s\in C} s$ forman una base de $Cent_K(G)$. Por otra parte, $e_C \in Cent_{\mathbb{Z}}(G)$, que es un $\mathbb{Z}$-módulo de tipo finito; entonces e_C resulta ser un elemento íntegro. Ahora bien, por ser ρ una representación de G, define un morfismo

$$\rho : K[G] \to End(W).$$

Por el lema de Schur, la imagen de $Cent_K(G)$ por este morfismo sólo contiene homotecias. Entonces $\rho(e_C) = \lambda I$, siendo λ un elemento íntegro. Tomando trazas a ambos lados de la igualdad tenemos

$$d \cdot \lambda = \sum_{s\in C}\chi(s),$$

de donde

$$\lambda = \frac{1}{d}\sum_{s\in C}\chi(s),$$

lo cual demuestra la proposición. □

Daremos a continuación un importante teorema que facilita la búsqueda de representaciones irreducibles.

Teorema 1.9 *(Frobenius).*

Sean G un grupo finito de orden g y W un espacio de representación irreducible de G de dimensión d. Entonces d es un divisor de g.

Demostración:
Si χ es el carácter asociado a la representación $(\rho,\ W)$, sabemos que $(\chi, \chi) = 1$; al explicitar esta igualdad

obtenemos

$$\begin{aligned}\frac{g}{d} &= \frac{1}{d}\sum_{s\in G}\chi(s^{-1})\chi(s)\\ &= \frac{1}{d}\sum_{C\in\mathbb{C}}(\sum_{s\in C}\chi(s^{-1})\chi(C))\\ &= \frac{1}{d}\sum_{C\in\mathbb{C}}\chi(C)\sum_{s\in C}\chi(s^{-1}),\end{aligned}$$

que podemos poner en la forma

$$\frac{g}{d} = \sum_{C}\chi(s^{-1})(\sum_{t\in C}\frac{\chi(t)}{d}),$$

El segundo miembro de la igualdad anterior es íntegro por las proposiciones antes demostradas. Como $\frac{g}{d}\in\mathbb{Q}$, tenemos que $\frac{g}{d}\in\mathbb{Z}$; por tanto d es un divisor de g, como se quería demostrar. □

1.5. Representaciones Inducidas

Si H es un subgrupo de G, cualquier representación (ρ, V) de G se restringe a una representación de H, que se denota $Res_H^G\ V$ o simplemente $Res\ V$, si H está fijo. En esta sección describiremos una importante construcción que produce representaciones de G de las representaciones de H. Supongamos que (ρ, V) es una representación de G, y W un subespacio de V que es invariante por la acción de H, *i.e.* $h.W = W\ \forall h\in H$. Para cualquier $g\in G$, el subespacio $g.W = \{g.w:\ w\in W\}$ depende únicamente de la coclase a izquierda gH de g módulo H, ya que $gh.W = g.(h.W) = g.W,\ \forall\ h\in H$. Para una coclase $\sigma\in G/H = \{gH:\ g\in G\}$, escribimos $\sigma.W$ para denotar este subespacio de V.

Definición 11 *Sean V una representación de G, y $W\subseteq V$ un subespacio H-invariante. Decimos que V está* **inducida** *por W si todo elemento de V se puede escribir de manera única como suma de elementos de los trasladados $\sigma.W$, es decir,*

$$V = \bigoplus_{\sigma\in G/H}\ \sigma.W.$$

En este caso, escribimos $V = Ind_H^G\ W = Ind\ W$.

Ejemplos

a) La representación de permutación asociada a la acción a izquierda de G sobre G/H es inducida por la representación trivial de H sobre W. Donde V tiene base $\{e_\sigma : \sigma\in G/H\}$, y $W = \mathbb{C}.e_H$, siendo H la coclase trivial.

En efecto, W es un subespacio de V que resulta invariante por la acción de H y por definición, sabemos que $V = \bigoplus_{\sigma\in G/H}\mathbb{C}.e_\sigma$. Como la acción de G sobre V definida sobre la base está dada por $g.e_\sigma = e_{g.\sigma} = e_\tau,\ \forall\ g\in G$, se tiene que, si $\sigma = g.H$ para algún $g\in G$,

$$e_\sigma = e_{g.H} = g.e_H = g^{'}.e_H, \quad \forall\ g,\ g^{'}\in\sigma.$$

Por tanto, $V = \bigoplus_{\sigma\in G/H}\ \sigma.\mathbb{C}.e_H$; es decir, $V = Ind_H^G\ W$.

b) La representación regular (ρ, W) de H induce la representación regular (ρ, V) de G. Aquí, la base de V está dada por $B = \{e_g:\ g\in G\}$ mientras que la base de W está dada por $B_H = \{e_h:\ h\in H\}$.

Resulta evidente que W es un H-submódulo de V ya que la acción de todo elemento $x \in H$ permuta los elementos de la base B_H. Luego, basta verificar la igualdad

$$V = \bigoplus_{\sigma \in G/H} \ \sigma.W \ .$$

Por ser V y W espacios de representación de la representación regular sobre G y H respectivamente, tenemos que

$$V = \bigoplus_{g \in G} \ \mathbb{C}.e_g, \quad W = \bigoplus_{h \in H} \ \mathbb{C}.e_h. \tag{5}$$

Veamos como actúa una coclase de G$/H$ sobre W: Tomemos un representante g_σ de la coclase $\sigma \in G/H$, entonces $g_\sigma.e_h = e_{g_\sigma h}, \ \forall \ h \in H$. Por tanto, la acción de g_σ transforma la base B_H en $B_{g_\sigma H} = \{e_{g_\sigma h} : \ h \in H\}$.

Es claro que si ${g_\sigma}'$ es otro representante de la coclase σ, entonces $B_{g_\sigma H} = B_{{g_\sigma}' H}$. Luego, la base no depende del representante elegido y por tanto da como resultado una base del espacio $\sigma.W$. De las igualdades en (4), se deduce que $V = \bigoplus_{\sigma \in G/H} \ \sigma.W$, es decir, $V = Ind_H^G \ W$.

Hemos dado dos ejemplos de representaciones de H que inducen representaciones ya conocidas de G. Esto lleva a preguntarnos lo siguiente: ¿dada cualquier representación de H, existe la representación inducida de G?. La siguiente proposición no sólo nos da la respuesta, sino que también aporta una manera de construirla.

Proposición 1.8 *Existe una representación de G y sólo una (salvo isomorfismos) inducida por una representación cualquiera de H prefijada.*

Demostración:
Sea W el espacio de representación de H correspondiente a la representación prefijada, entonces W admite una estructura de $\mathbb{C}[H]$-módulo a izquierda. Por otra parte, la inclusión $\mathbb{C}[H] \hookrightarrow \mathbb{C}[G]$ induce sobre $\mathbb{C}[G]$ una estructura de $\mathbb{C}[H]$-módulo a derecha, vía la restricción de la multiplicación a derecha en el álgebra $\mathbb{C}[G]$. Luego, $V_0 = \mathbb{C}[G] \otimes_{\mathbb{C}[H]} \ W$ admite una estructura de $\mathbb{C}[G]$-módulo a izquierda.

El grupo G opera en V_0 de la siguiente manera: a cada $s \in G$ se le asocia el endomorfismo $s \otimes 1$ de V_0. Es claro que, si restringimos esta acción de G a la acción de H, W resulta un $\mathbb{C}[H]$-submódulo de V_0. Por otra parte, sabemos que $\mathbb{C}[G]$ es un $\mathbb{C}[H]$-módulo libre a derecha, que admite como base un sistema de representantes S de G$/H$; por tanto $V_0 = \bigoplus_{s \in S} \ s.W$, que es lo que se quería probar. La unicidad resulta inmediata, ya que si $\overline{V} = \bigoplus_{\sigma \in G/H} \sigma.W$ es otra representación inducida, la inclusión $s.W \hookrightarrow \sigma.W$ sobre cada sumando define un isomorfismo de representaciones de V_0 en $\overline{V}$.

Por tanto, toda representación (ρ, V) de G que es inducida por la representación de H es isomorfa a V_0, esto es

$$Ind_H^G \ W \cong \mathbb{C}[G] \otimes_{\mathbb{C}[H]} \ W.$$

$\square$

Definición 12 *De aquí en adelante, llamaremos a $\mathbb{C}[G] \otimes_{\mathbb{C}[H]} \ W$ la representación inducida por W.*

Usando la construcción de la representación inducida, se deduce su transitividad. Es decir, si G es un grupo, H_2 un subgrupo y H_1 un subgrupo de H_2, entonces la representación de G inducida por la de H_1 es equivalente a la representación que se obtiene induciendo primero la de H_1 en H_2 y luego la de H_2 en G.

En efecto, supongamos que (ρ_1, W_1) es la representación de H_1 y que $V = Ind_{H_1}^G \ W_1$, por tanto debe ser que $V = \mathbb{C}[G] \otimes_{\mathbb{C}[H_1]} \ W_1$. Sea $W_2 = \mathbb{C}[H_2] \otimes_{\mathbb{C}[H_1]} \ W_1$ la representación de H_2 inducida por la de H_1 y $V^{'} = \mathbb{C}[G] \otimes_{\mathbb{C}[H_2]} \ W_2$ la representación de G inducida por la de H_2. Debemos ver que $V^{'} \cong V$, y esto se deduce de un simple cálculo. A saber,

$$\begin{aligned} V' &= \mathbb{C}[G] \otimes_{\mathbb{C}[H_2]} W_2 \\ &= \mathbb{C}[G] \otimes_{\mathbb{C}[H_2]} (\mathbb{C}[H_2] \otimes_{\mathbb{C}[H_1]} W_1) \\ &\cong \mathbb{C}[G] \otimes_{\mathbb{C}[H_1]} W_1 \\ &\cong V, \end{aligned}$$

como se quería demostrar.

Como consecuencia inmediata de la definición tenemos la siguiente proposición.

Proposición 1.9 *Sea V una representación de G tal que $V = \bigoplus_i W_i$, donde*

a) G permuta los W_i,

b) G los permuta transitivamente.

Sea $H \subseteq G$ el estabilizador de W_{i_0}, para un i_0 fijo. Entonces H opera en W_{i_0}, y esta representación induce la representación V de G.

Recordemos que el estabilizador de un espacio de representación W es un subgrupo de G y está definido por $\{g \in G : \ g.w = w, \ \forall \ w \in W\}$.

Observación: Si la representación V es irreducible, la condición *b)* es consecuencia de la condición *a)*, pues $\sum_{s\in G} s.W_{i_0}$ es un subespacio invariante no nulo de V, y por tanto igual a V.

Para seguir con la descripción de las representaciones inducidas debemos demostrar la siguiente proposición de carácter técnico.

Proposición 1.10 *Sean W un espacio de representación de H, U un espacio de representación de G, y supongamos que $V = Ind_H^G \ W$. Entonces cualquier morfismo de H-módulos $\varphi : W \to U$ se extiende de manera única a un morfismo de G-módulos $\overline{\varphi} : V \to U$; es decir,*

$$Hom_H(W, Res\ U) \cong Hom_G(Ind\ W, U).$$

En particular, esta propiedad universal determina $Ind\ W$ salvo isomorfismos canónicos.

En otras palabras, como la aplicación Ind define un funtor de la categoría ${}_H\mathcal{M}$ de H-módulos en la categoría ${}_G\mathcal{M}$ de G-módulos y la aplicación Res un funtor entre las categorías de G-módulos y H-módulos,

$$Ind : \ {}_H\mathcal{M} \to \ {}_G\mathcal{M},$$

$$Res : \ {}_G\mathcal{M} \to \ {}_H\mathcal{M},$$

la proposicíon anterior afirma que los funtores Ind y Res resultan ser funtores adjuntos.

Demostración:
Sabemos que $V = \bigoplus_{\sigma \in G/H} \ \sigma.W$, luego basta definir $\overline{\varphi}$ sobre cada espacio $\sigma.W$. Entonces, definimos $\overline{\varphi}$ como la siguiente composición:

$$\sigma.W \xrightarrow{g_\sigma^{-1}} W \xrightarrow{\varphi} U \xrightarrow{g_\sigma} U\,. \tag{6}$$

Esta definición no depende del representante $g_\sigma \in \sigma$ debido a que φ es H-lineal.

Veamos a través de un simple cálculo que $\overline{\varphi}$ resulta G-lineal. Para esto, basta verificar que lo es sobre cada espacio $\sigma.W$. Sean $g \in G$, g_σ un representante de $\sigma \in G/H$, y supongamos que $g.g_\sigma = g_\tau,$ donde $\tau \in G/H$. Luego, tenemos que

$$\overline{\varphi}(g.g_\sigma w) \quad = \overline{\varphi}(g_\tau w), \quad \forall\ w \in W.$$

Como $g_\tau.w \in \tau.W$, por definición de la aplicación vale

$$\begin{aligned} \overline{\varphi}(g.g_\sigma w) \quad &= g_\tau.\varphi(g_\tau^{-1}.g_\tau w), \quad \forall\ w \in W, \\ &= g_\tau.\varphi(w) \\ &= g.g_\sigma.\varphi(w) \\ &= g.\overline{\varphi}(g_\sigma.w), \quad \forall\ w \in W. \end{aligned}$$

La unicidad se deduce inmediatamente usando la definición sobre los espacios $\sigma.W,\ \sigma \in G/H$.

□

1.5.1. Carácter de una representación inducida

Sean H un subgrupo de G, (ρ, W) una representación de H de carácter χ_W, y V la representación de G inducida por W; queremos determinar el carácter χ_V de V. Un elemento $x \in G$ define un automorfismo de V que permuta los $s.W,\ s \in G/H$; por consiguiente, su traza es la suma de las trazas de las restricciones de este automorfismo a los $s.W$ que deja invariantes, lo cual equivale a la relación $s^{-1}xs \in H$; de donde

$$\chi_V(x) = Tr_V(x) = \textstyle\sum_{\{s\in G/H,\ s^{-1}xs\in H\}} Tr_{s.W}(x).$$

De la conmutatividad del diagrama

$$\begin{tikzcd} W \arrow[r, "s^{-1}xs"] \arrow[d, "s"'] & W \arrow[d, "s"] \\ s.W \arrow[r, "x"] & s.W \end{tikzcd} \tag{7}$$

resulta que $Tr_{s.W}(x) = Tr_W(s^{-1}xs),\ \forall x \in G$, y por tanto

$$\chi_V(x) = \tfrac{1}{|H|} \textstyle\sum_{\{s\in G,\ s^{-1}xs\in H\}} Tr_W(s^{-1}xs). \tag{8}$$

Por ser los caracteres de las representaciones irreducibles una base ortonormal de las funciones de clases, la fórmula (8) se extiende por linealidad, obteniendo la siguiente definición.

Definición 13 *Si f es una función de clases de H definimos la función* **inducida** *$Ind\ f$ como*

$$Ind\ f(x) = \tfrac{1}{|H|} \textstyle\sum_{\{s\in G,\ s^{-1}xs\in H\}} f(s^{-1}xs). \tag{9}$$

Además, si ψ es una función de clases de G, notamos Res ψ a la restricción de la función $\psi|_H$ sobre el subgrupo H.

El siguiente teorema debido a Frobenius muestra la fuerte relación entre ambas funciones.

Teorema 1.10 *(Reciprocidad de Frobenius).*

Si φ y ψ son funciones de clases de H y G respectivamente, entonces los productos escalares $(\varphi, Res\ \psi)_H$ y $(Ind\ \varphi, \psi)_G$ son iguales.

Demostración:
La demostración de este teorema consiste en la realización explícita de los cálculos. A saber, de la definición de $(Ind\ \varphi, \psi)_G$ y de $Ind\ \varphi$ resulta inmediatamente que

$$(Ind\ \varphi, \psi)_G = \frac{1}{gh} \sum_{\{y^{-1} \in G,\ z^{-1}y^{-1}z \in H\}} \psi(y)\varphi(z^{-1}y^{-1}z),$$

donde $g =$ orden de G y $h =$ orden de H. Si hacemos el cambio de variables $z^{-1}y^{-1}z = x^{-1},\ x \in H$, la igualdad anterior en cuestión es evidente,

$$\begin{aligned}
(\psi, Ind\ \varphi)_G &= \frac{1}{gh} \sum_{\{zxz^{-1} \in G,\ x^{-1} \in H\}} \psi(zxz^{-1})\varphi(x^{-1}) \\
&= \frac{1}{gh} \sum_{\{zxz^{-1} \in G,\ x^{-1} \in H\}} \psi(x)\varphi(x^{-1}) \\
&= \frac{1}{gh} . g \sum_{\{x \in H\}} \psi(x)\varphi(x^{-1}) \\
&= (Res\ \psi, \varphi)_H .
\end{aligned}$$

□

En particular, el teorema anterior se podía haber demostrado en el caso en que ψ y φ son caracteres, ya que estos forman una base ortonormal del espacio vectorial de funciones de clases. Sean V_1 y V_2 son dos espacios de representación de G de dimensión finita y χ_{V_1}, χ_{V_2} sus caracteres. Se deduce fácilmente del lema de Schur y de la definición del producto interno y de sus propiedades la siguiente igualdad:

$$(\chi_{V_1}, \chi_{V_2}) = dim\ Hom_G\ (V_1, V_2). \tag{10}$$

Sean χ_V y χ_W los caracteres de las representaciones (ρ_1, V) de G y (ρ_2, W) de H respectivamente. Entonces, el teorema anterior dice que

$$(\chi_W, Res\ \chi_V)_H = (Ind\ \chi_W, \chi_V)_G.$$

Esta igualdad se deduce inmediatamente de la igualdad (10) y de la proposición 1.10. En efecto, tenemos que

$$(\chi_W, Res\ \chi_V)_H = dim\ Hom_H\ (W, Res\ V),$$

$$(Ind\ \chi_W, \chi_V)_G = dim\ Hom_G\ (Ind\ W, V).$$

Como $Hom_H(W, Res\ V) = Hom_G(Ind\ W, V)$; en particular tienen la misma dimensión, es decir que

$$(\chi_W, Res\ \chi_V)_H = (Ind\ \chi_W, \chi_V)_G.$$

□

Observación: Este teorema expresa que las aplicaciones Ind y Res son aplicaciones *adjuntas* respecto de los productos internos sobre las funciones de clases de H y de G respectivamente.

Un caso particular del teorema 1.10, es la siguiente proposición:

Proposición 1.11 *Sean W y V sendas representaciones irreducibles de H y G. Entonces, el número de veces que $Res\ V$ contiene a W es igual al número de veces que $Ind\ W$ contiene a V.*

La *Reciprocidad de Frobenius* puede ser usada para encontrar los caracteres de G si los caracteres de H son conocidos.

Por ejemplo, supongamos que $G = \mathbb{S}_3$ y consideremos $H = \mathbb{S}_2$ como subgrupo de $\mathbb{S}_3$. Es claro que $W = V_2$ el espacio de la representación estándar de $\mathbb{S}_2$, resulta isomorfo al espacio $U^{'}$ de la representación signo de $\mathbb{S}_2$. Por otro lado, sabemos que las representaciones irreducibles de $\mathbb{S}_3$ son la representación trivial (ρ_{U_3}, U_3), la representación signo $(\rho_{U_3'}, U_3^{'})$ y la representación estándar (ρ_{V_3}, V_3); las cuales restringidas a H dan las representaciones (ρ_{U_2}, U_2), $(\rho_{U_2'}, U_2^{'})$ y $(\rho_{U_2 \oplus U_2'}, U_2 \oplus U_2^{'})$ respectivamente.

En efecto, como tenemos sólo dos órbitas de conjugación en $\mathbb{S}_2$, sabemos que hay sólo dos clases de isomorfismo de representaciones irreducibles. Como U_2 no es isomorfa a $U_2^{'}$, debe ser que la restricción de V_3 es isomorfa a una suma directa de combinaciones de ambas. Consideremos los subespacios W_2 y $W_2^{'}$ de V_3 generados por los vectores $(1,\ 1,\ -2)$ y $(1,\ -1,\ 0)$ respectivamente. Es claro que estos espacios son estables por la acción de $\mathbb{S}_2$ y a través de simples cálculos se deduce que

$$Res_H\ V_3 = W_2 \oplus W_2^{'} \quad = U_2 \oplus U_2^{'}.$$

Siendo la acción de H sobre W_2 la trivial y sobre $W_2^{'}$ la dada por el signo.

Entonces, para calcular $Ind_H^G\ V_2$, debemos calcular los productos internos

$$(Ind\ \chi_{V_2}, \chi_{V_3}), \quad (Ind\ \chi_{V_2}, \chi_{U_3}), \quad \text{y} \quad (Ind\ \chi_{V_2}, \chi_{U_3'}).$$

Por Frobenius sabemos que los podemos calcular de la siguiente manera:

$$(\chi_{V_2}, Res\ \chi_{V_3}) = 1,$$

$$(\chi_{V_2}, Res\ \chi_{U_3}) = (\chi_{V_2}, \chi_{U_2}) = 0,$$

$$(\chi_{V_2}, Res\ \chi_{U_3'}) = (\chi_{V_2}, \chi_{U_2'}) = 1.$$

Por tanto, tenemos que $Ind_H^G\ V_2 = V_3 \oplus U_3^{'}$.

1.5.2. Restricción a los subgrupos

Sean H y K subgrupos de G y (ρ, W) una representación lineal de H, y $V = Ind_H^G\ W$ la representación inducida de G. Nos proponemos determinar la *restricción* $Res_K\ V$ de V a K.

Elijamos primero un conjunto de representantes S de las clases dobles de G módulo (H, K); es decir, G es la unión disjunta de los conjuntos $KsH,\ s \in S$. Equivalentemente escribiremos $s \in K|G/H$. Dado $s \in S$, sea $H_s = sHs^{-1} \cap K$; donde H_s resulta un subgrupo de K.

Si definimos
$$\rho_s(x) = \rho(s^{-1}xs), \quad x \in H_s,$$

obtenemos un homomorfismo $\rho_s : H_s \to GL(W)$. Al espacio vectorial correspondiente a esta representación lineal de H_s lo llamaremos W_s. Como H_s es un subgrupo de K, tenemos definida la representación $Ind_{H_s}^K\ W_s$.

Proposición 1.12 *La representación $Res_K\ Ind_H^G\ W$ es isomorfa a la suma directa de las representaciones $Ind_{H_s}^K\ W_s,\ s \in K|G/H$.*

Demostración:
Por ser V una representación inducida, sabemos que es igual a una suma directa de los transformados $s.W,\ s \in G/H$. Sea $V(s)$ el subespacio generado por los transformados $x.W,\ x \in KsH$; entonces V es suma directa de los espacios $V(s)$, donde dichos espacios son estables por la acción K. Luego, el teorema se reduce a probar que $V(s)$ es K-isomorfa a $Ind_{H_s}^K\ W_s$.

El subgrupo de K formado por los elementos x tal que $x(s.W) = s.W$ es igual a H_s, y $V(s)$ es suma directa de los transformados $x(s.W),\ x \in K/H_s$; es decir, $V(s) = Ind_{H_s}^K\ s.W$. Por tanto, sólo falta ver que $s.W$ es H_s-isomorfa a W_s; pero esto es inmediato, pues el isomorfismo buscado es

$$s : W_s \to s.W, \quad w \mapsto s.w, \quad \forall\ w \in W_s.$$

□

Cabe preguntarse bajo qué condiciones una representación inducida resulta irreducible. Para responderlo, aplicaremos el caso anterior a $K = H$. Si $s \in G,\ H_s$ es el subgrupo $s^{-1}Hs \cap H$ de H; luego, la representación ρ de H define por restricción a H_s una representación $Res_s\ \rho$.

Proposición 1.13 *La representación inducida $V = Ind_H^G\ W$ es irreducible si y sólo si se verifican las siguientes condiciones:*

a) W es irreducible,

b) Para todo $s \in G, s \notin H$, las representaciones ρ_s y $Res_{H_s}\ \rho$ de H_s no tienen ninguna componente en común (es decir, sus caracteres son ortogonales).

Demostración:
Sean χ_V el carácter de la representación inducida y χ_W el carácter de la representación de H; donde $\chi_V = Ind\ \chi_W$. Por lo hecho hasta ahora, sabemos que V es irreducible si y sólo si $(\chi_V, \chi_V)_G = 1$ y que vale la igualdad $(\chi_V, \chi_V)_G = dim\ Hom_G(V, V)$. Por tanto, aplicando la fórmula de Frobenius se tiene que

$$(\chi_V, \chi_V)_G = (Res\ \chi_V, \chi_W)_H.$$

De acuerdo a la proposición anterior, debe ser que

$$Res\ \chi_V = \textstyle\sum_{\{x \in H|G/H\}} Ind_{H_s}^H(\rho_x).$$

Aplicando otra vez la fórmula de Frobenius se obtiene que

$$(\chi_V, \chi_V)_G = \textstyle\sum_{\{x \in H|G/H\}} d_x, \quad d_x = (\rho_x, Res_x(\rho))_{H_s}.$$

Para $x = 1,\ d_x = (\rho, \rho)_{H_s} \geq 1$. Luego, para que $(\chi_V, \chi_V)_G = 1$ es necesario y suficiente que $d_1 = 1$ y que $d_x = 0$ para todo $x \neq 1$ módulo (H, H); es decir, para todo $x \notin H$. Pero esto es precisamente lo que se pide en *a)* y en *b).* □

Para el caso en que H es un subgrupo normal se tiene el siguiente corolario:

Corolario 1.7 *Sean H un subgrupo normal de G y (ρ, W) una representación de H. Entonces $V = Ind_H^G\, W$ es irreducible si y sólo si (ρ, W) es irreducible y no es isomorfa a ninguna de sus represenatciones conjugadas ρ_s, $\forall\ s \notin H$.*

Para finalizar este capítulo, enunciaremos un teorema de Artin y un corolario que caracterizan a los subgrupos que inducen las representaciones del grupo G; ambas demostraciones se pueden encontrar en [S].

Recordemos que $ch\ KG$ es el anillo de caracteres virtuales de G sobre K. Supongamos que $K = \mathbb{C}$ y notemos al anillo $ch\ \mathbb{C}G$ simplemente por $R(G)$. Si H es un subgrupo de G, la operación restricción define un morfismo de anillos

$$Res:\ R(G) \to R(H).$$

Análogamente, la operación inducción Ind_H^G define un morfismo de anillos

$$Ind:\ R(H) \to R(G).$$

Teorema 1.11 *(E. Artin)*

Sea X una familia de subgrupos de G. Entonces, son equivalentes

a) La unión de los conjugados de los subgrupos pertenecientes a X es igual a G.

b) La imagen de la aplicación $Ind:\ \bigoplus_{\{H \in X\}} R(H) \to R(G)$ tiene índice finito.

c) Para todo carácter χ de G, existen elementos $(\psi_H)_{H \in X}$, $\psi_H \in R(H)$, y un número natural $d \geq 1$ tales que

$$d.\chi = \sum_{\{H \in X\}} Ind_H^G \psi_H.$$

En particular, la familia de los subgrupos cíclicos de G verifica *a).* Por tanto,

Corolario 1.8 *Todo carácter de G es combinación lineal a coeficientes en $\mathbb{Q}$ de caracteres inducidos por caracteres de subgrupos cíclicos de G.*

Capítulo 2

Representaciones del grupo simétrico

En este capítulo describiremos las representaciones irreducibles de los grupos simétricos sobre un cuerpo K algebraicamente cerrado y de característica cero. Haremos uso de algunas nociones básicas desarrolladas en el capítulo anterior aunque los grupos simétricos gozan de propiedades especiales que hacen posible que esta sección esté, en su gran parte, autocontenida.

La teoría de representaciones de los grupos simétricos fue en un principio estudiada por Frobenius y Schur, y luego desarrollada en una larga serie de trabajos por Young.

Análogamente al capítulo anterior, comenzaremos con algunas definiciones básicas y propiedades correspondientes a los grupos simétricos.

2.1. El grupo simétrico

Una función biyectiva del conjunto $\mathbb{I}_n = \{1,\ 2, \ldots,\ n\}$ en sí mismo se denomina una **permutación** de n números. El conjunto de permutaciones de n números, munido de la operación composición usual de funciones, tiene una estructura de grupo. Este grupo se denomina el **grupo simétrico** de grado n y se denota con $\mathbb{S}_n$; en particular, $\mathbb{S}_n$ está definido para todo $n \geq 0$ y su orden es $n!$. La composición de permutaciones la notaremos como la composición de funciones.

Observación: Notar que una función de $\mathbb{I}_n$ en $\mathbb{I}_n$ es biyectiva si y sólo si es inyectiva, si y sólo si es suryectiva.

Más generalmente, dado un conjunto X definimos $\mathbb{S}_X = \{f : X \to X,\ f \text{ biyectiva}\}$. Si $Y \hookrightarrow X$, entonces $\mathbb{S}_Y$ se identifica naturalmente con un subgrupo de $\mathbb{S}_X$. En particular, si $Y \hookrightarrow X,\ Z \hookrightarrow X$, siendo $Y \cap Z = 0$, entonces el producto cartesiano $\mathbb{S}_Y \times \mathbb{S}_Z$ entre ambos conjuntos también se identifica con un subgrupo de $\mathbb{S}_X$. Por ejemplo, $\mathbb{S}_{\{1,\ 2\}} \times \mathbb{S}_{\{3,\ 4\}} \hookrightarrow \mathbb{S}_4$, siendo $X = \mathbb{I}_4,\ Y = \{1,\ 2\}$ y $Z = \{3,\ 4\}$.

En la práctica es común escribir cada permutación σ como

$$\sigma = \begin{pmatrix} 1 & 2 & 3... & ...n \\ \sigma(1) & \sigma(2) & \sigma(3)... & ...\sigma(n) \end{pmatrix}.$$

Si fijamos $\sigma \in \mathbb{S}_n$, tenemos una acción del grupo aditivo $\mathbb{Z}$ en $\mathbb{I}_n$ dada por $j \cdot x = \sigma^j(x)$. Una órbita de esta acción para $x \in \mathbb{I}_n$ es simplemente

$$O_x = \{y \in \mathbb{I}_n : \exists j,\ \sigma^j(x) = y\}.$$

Estas órbitas se denominan *ciclos* de la permutación σ y se escriben de la siguiente manera

$$(i_1\ i_2\ \ldots i_k) \quad \text{donde } \sigma(i_1) = i_2,\ \sigma(i_2) = i_3 \ldots \sigma(i_k) = i_1.$$

Luego, $\mathbb{I}_n$ se puede descomponer como una unión disjunta de órbitas dadas por la acción de $\mathbb{Z}$, y por tanto como una unión disjunta de ciclos. La acción de σ sobre $\mathbb{I}_n$ se representa como el producto de ciclos disjuntos.

Por ejemplo, el ciclo (1 3 2) representa la permutación σ dada por

$$\sigma(1) = 3, \quad \sigma(3) = 2 \quad \text{y} \quad \sigma(2) = 1.$$

Además tenemos que $\sigma^2(1) = 2,$ y que $\sigma^3(1) = 1$. Luego, $\{1,\ 3,\ 2\}$ es la órbita de 1 dada por la accíon de $\mathbb{Z}$ sobre $\mathbb{I}_n$.

Consideremos la permutación σ dada por

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}.$$

Como $\sigma^2(1) = 4,\ \sigma^3(1) = 1,$ y $\sigma^2(2) = 2$, las órbitas de 1 y de 2 por la acción de $\mathbb{Z}$ son $\{1,\ 3,\ 4\}$ y $\{2,\ 5\}$ respectivamente; en particular, σ admite la siguiente escritura

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2. \end{pmatrix} = (1\ 3\ 4)(2\ 5).$$

Por una cuestión de notación, generalmente los 1-ciclos se omiten cuando se escribe una permutación; en particular, si una permutación σ intercambia dos números diferentes $a,\ b$ de $\mathbb{I}_n$ y deja todos los demás fijos, entonces σ se denomina una *trasposición* y se escribe como $\sigma = (a\ b)$. Por ejemplo,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 4 & 2. \end{pmatrix} = (2\ 5).$$

Como para todo ciclo $(i_1\ i_2 ... \quad ...n)$ se tiene que

$$(i_1\ i_2 ... \quad ...i_n) = (i_1\ i_2)(i_1\ i_3) ... \quad ...(i_1\ i_n),$$

entonces toda permutación se puede escribir como producto de trasposiciones. Más aún, como cualquier trasposición $(a\,b)$ con $a < b$ se puede escribir como un conjugado de $(b-1\ b)$ por $\tau = (b-2, b-1)(b-3, b-2) \ldots (a, a+1)$, es decir $(a\ b) = \tau^{-1}(b-1\ b)\tau$, se deduce la siguiente propiedad:

Proposición 2.1 *Las trasposiciones $(x-1\ x)$ si $1 < x \leq n$ generan $\mathbb{S}_n$.*

Definición 14 *Decimos que $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_j)$ es una* **partición** *de n si se cumplen las siguientes condiciones*

i) $\lambda_i \in \mathbb{N}_0, \qquad \forall\ i = 1, ..., j,$

ii) $\lambda_1 \geq \lambda_2 \geq ...... \geq \lambda_j,$

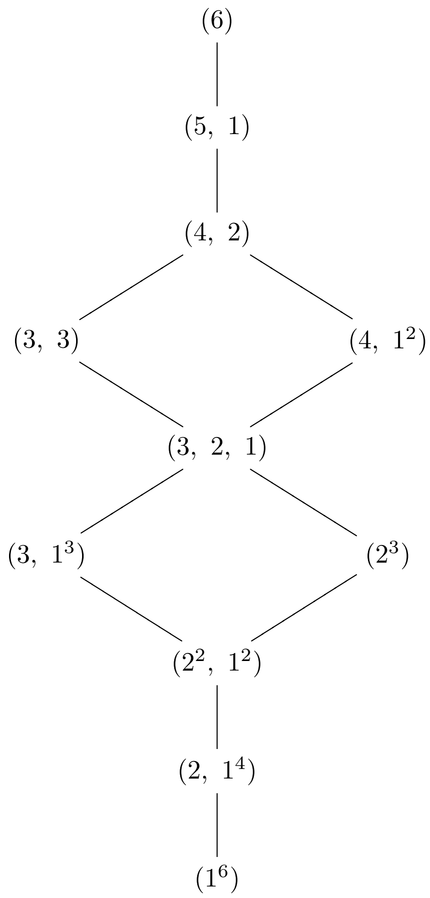
iii) $\sum_{i=1}^{j} \lambda_i = n.$

El conjunto de particiones de n acepta un orden parcial y un orden total, a saber

Definición 15 *Si μ y λ son particiones de n, decimos que μ domina a λ, y escribimos $\mu \geq \lambda$, si para todo j se tiene que*

$$\sum_{i=1}^{j} \mu_i \geq \sum_{i=1}^{j} \lambda_i.$$

Es claro que este orden es un orden parcial sobre el conjunto de particiones de n. Las relaciones de orden parcial entre los elementos de las particiones de 6 se muestran en el siguiente arbol:



Este orden es el que más se adecúa a nuestro propósito; sin embargo, a menudo utilizaremos un orden total $\prec$ sobre el conjunto de particiones dado por la siguiente definición:

Definición 16 *Si μ y λ son particiones de n, escribimos $\mu \succ \lambda$ si y sólo si para el menor j tal que $\mu_j \neq \lambda_j$ se tiene que $\mu_j \geq \lambda_j$. Este orden se denomina el orden lexicográfico.*

Es fácil ver que el orden total $\prec$ contiene al orden parcial $<$, en el siguiente sentido: si $\mu > \lambda$ entonces $\mu \succ \lambda$. Sin embargo, la recíproca no es cierta.

A continuación damos la relación de orden total entre los elementos en el conjunto de particiones de 6:

$$(6) \succ (5,\ 1) \succ (4,\ 2) \succ (4,\ 1,\ 1) \succ (3,\ 3) \succ (3,\ 2,\ 1) \succ (3,\ 1,\ 1,\ 1) \succ$$

$$\succ (2,\ 2) \succ (2,\ 2,\ 1,\ 1) \succ (2,\ 1,\ 1,\ 1,\ 1) \succ (1,\ 1,\ 1,\ 1,\ 1,\ 1).$$

Observación: El único uso que se le da a este orden total es para especificar el orden que se toma para ubicar las columnas en la tabla de caracteres de $\mathbb{S}_n$.

Una permutación σ se dice de **tipo** λ si las órbitas del grupo generado por σ tienen órdenes $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_j$; o sea, los ciclos disjuntos de σ tienen longitud $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_j$. Por ejemplo, si $\sigma = (1\ 3\ 4)(2\ 5) \in \mathbb{S}_5$, entonces σ es de tipo $(3,\ 2,\ 0,\ 0,\ 0,\ldots)$. Para describir los tipos, se usarán algunas abreviaciones como las siguientes:

$$(3,\ 2,\ 0,\ 0,\ 0,\ldots) = (3,\ 2)$$

$$(4,\ 2,\ 2,\ 2,\ 0,\ 0,\ 0,\ldots) = (4,\ 2,\ 2,\ 2) = (4,\ 2^3).$$

Esto es, se suprimen los ceros al final del tipo y se indican con exponentes las repeticiones de igual longitud.

Proposición 2.2 *Dos elementos $\sigma,\ \tau\ \in \mathbb{S}_n$ son conjugados si y sólo si tienen el mismo tipo.*

Demostración:
Es claro que si σ y τ son conjugados, entonces las órbitas de los grupos generados por ambos tienen el mismo orden, luego deben tener el mismo tipo. Esto es, si $\mu \in \mathbb{S}_n$ tal que $\sigma = \mu\tau\mu^{-1}$, y $\tau = \tau_1\tau_2\ldots\tau_k$ entonces

$$\begin{aligned} \sigma &= \mu\tau_1\tau_2\ldots\tau_k\mu^{-1} \\ &= \mu\tau_1\mu^{-1}\mu\tau_2\mu^{-1}\ldots\mu\tau_k\mu^{-1}. \end{aligned}$$

Como $\mu\tau_i\mu^{-1}$ es un ciclo disjunto de $\mu\tau_j\mu^{-1}$ si τ_i y τ_j son ciclos disjuntos, la igualdad del tipo se deduce del hecho que el orden de la órbita del grupo generado por τ_i es el mismo que el de la órbita del grupo generado por $\mu\tau_i\mu^{-1}$.

Supongamos ahora que σ y τ tienen el mismo tipo. Descompongamos al conjunto $\mathbb{I}_n$ como unión disjunta de las órbitas determinadas por σ y τ respectivamente. Luego,

$$\mathbb{I}_n = \textstyle\coprod_{i=1}^{r} X_i, \quad \text{donde } X_i \text{ son órbitas dadas por } \sigma,\ |X_i| \leq |X_{i+1}|,$$

$$\mathbb{I}_n = \textstyle\coprod_{i=1}^{s} X_i', \quad \text{donde } X_i' \text{ son órbitas dadas por } \tau,\ |X_i'| \leq |X_{i+1}'|.$$

Por tanto, como σ y τ tiene el mismo tipo, debe ser que $r = s$ y que $|X_i'| = |X_i|$ para todo $i = 1, ..., r$. Elegimos entonces r biyecciones $\mu_i : X_i' \to X_i$ tal que cada una hace conmutar al diagrama

$$\begin{tikzcd} X_i' \arrow[r, "\tau"] \arrow[d, "\mu_i"] & X_i' \arrow[d, "\mu_i"] \\ X_i \arrow[r, "\sigma"'] & X_i \end{tikzcd} ,$$

siendo

$$X_i = \{x_i,\ \sigma(x_i),\ \sigma^2(x_i), \ldots,\ \sigma^k(x_i)\}$$

$$X_i' = \{x_i,\ \tau(x_i),\ \tau^2(x_i), \ldots,\ \tau^k(x_i)\}.$$

Luego, definimos μ de la siguiente manera

$$\mu = \textstyle\coprod_{i=1}^{r} \mu_i : \mathbb{I}_n \to \mathbb{I}_n.$$

Claramente se verifica que $\sigma = \mu\tau\mu^{-1}$, ya que se cumple para cada órbita. □

Es claro que toda partición se puede ver como el tipo de alguna permutación en $\mathbb{S}_n$. Por tanto, se tiene el siguiente

Corolario 2.1 *El número de clases de conjugación de $\mathbb{S}_n$ es igual al número de particiones de n.*

Sabemos que, para todo grupo finito G, el número de clases de isomorfismo de $\mathbb{C}[G]$-módulos simples es igual al número de clases de conjugación de G, entonces

Corolario 2.2 *La cantidad de clases de isomorfismo de representaciones irreducibles de $\mathbb{S}_n$ es igual al número de particiones de n.*

Por tanto, nuestro objetivo es construir una representación irreducible de $\mathbb{S}_n$ para cada partición dada.

Ejemplo

Existe una representación natural de $\mathbb{S}_n,\ n \geq 2$, que se desprende del hecho que este grupo permuta los elementos del conjunto $\mathbb{I}_n$. Consideremos un espacio vectorial W sobre K de dimensión n, cuya base esté dada por ciertos vectores $\{e_1,\ e_2, \ldots,\ e_n\}$. Dejemos actuar $\mathbb{S}_n$ sobre la base por $\sigma(e_i) = e_{\sigma(i)}$; extendiendo esta acción linealmente se obtiene una representación del grupo simétrico que denotaremos $M^{(n-1,\ 1)}$. Este $\mathbb{S}_n$-módulo, en general, no resulta irreducible ya que es fácil encontrar un $\mathbb{S}_n$-submódulo propio de $M^{(n-1,\ 1)}$; en efecto, el subespacio vectorial U de W generado por el elemento $w = \sum_{i=1}^{n} e_i$ es invariante por la acción de $\mathbb{S}_n$, que actúa trivialmente sobre él.

Como el cuerpo K es de característica cero, se puede encontrar un complemento de U que sea estable por la acción de $\mathbb{S}_n$. En particular, si $K = \mathbb{C}$, en el capítulo anterior hemos dado la descomposición de $\mathbb{C}^3$ como suma directa de espacios de representación dados por la trivial y la estándar, es decir $\mathbb{C}^3 = U \oplus V$. Esto ocurre en general; si consideramos el espacio vectorial

$$V = \{(x_1, x_2, \ldots, x_n) \in \mathbb{C}^n :\ x_1 + x_2 + \cdots + x_n = 0\},$$

es fácil ver que es un $\mathbb{S}_n$-submódulo de $\mathbb{C}^n$ y que tiene dimensión $n-1$. Tomando la base canónica de $\mathbb{C}^n$ y el $\mathbb{S}_n$-submódulo trivial U, es claro que $U \cap V = 0$. Entonces

$$\mathbb{C}^n = U \oplus V,$$

y V resulta ser un complemento de U que es estable por la acción de $\mathbb{S}_n$.

Notemos que V resulta siempre un $\mathbb{S}_n$-módulo sin importar el cuerpo de base. Este $\mathbb{S}_n$-módulo se denomina módulo de **Specht** y generalmente se nota como $S^{(n-1,\ 1)}$. Más adelante, veremos que este módulo es irreducible y corresponde a la partición $(n-1,\ 1)$ de n.

En la proxima sección se mostrará una forma de construir módulos de representación de $\mathbb{S}_n$, entre ellos los módulos de Specht, que son irreducibles y están parametrizados por las particiones de n. Para ello debemos introducir primero la terminología y la notación correcta.

2.2. Diagramas, tableros y tabloides

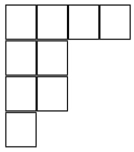
Definición 17 *Si λ es una partición de n, entonces un* **diagrama de Young** $[\lambda]$ *es el conjunto*

$$[\lambda] = \{(i,\ j) :\ i, j \in \mathbb{Z},\ 1 \leq i,\ 1 \leq j \leq \lambda_i\}.$$

Si $(i,\ j) \in [\lambda]$, entonces $(i,\ j)$ se denomina un nodo de $[\lambda]$. Entonces la k-ésima fila (o columna) del diagrama consiste en aquellos nodos cuya primera (respectivamente, segunda) coordenada es k.

Dibujaremos los diagramas como en el siguiente ejemplo:

Supongamos que $\lambda = (4,\ 2^2,\ 1)$, entonces el diagrama correspondiente a $[(4,\ 2^2,\ 1)]$ será

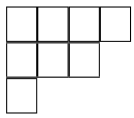


.

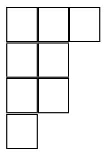
Es costumbre quitar los paréntesis cuando se denota un diagrama, por ejemplo $[\lambda] = [(4,\ 2^2,\ 1)] = [4,\ 2^2,\ 1]$.

Definición 18 *Decimos que una partición $\lambda^{'}$ es conjugada de una partición λ si se obtiene cambiando las filas por las columnas en el diagrama de $[\lambda]$.*

Por ejemplo, si $\lambda = (4,\ 3,\ 1)$ es una partición de 8, entonces

$[\lambda] =$  .

Si cambiamos filas por columnas obtenemos el diagrama

$[\lambda^{'}] =$  ,

siendo $\lambda^{'} = (3,\ 2^2,\ 1)$ la partición de 8 conjugada de $(4,\ 3,\ 1)$.

Definición 19 *Un* **tablero** *de λ es una de los $n!$ matrices obtenidas por la sustitución de cada nodo en $[\lambda]$ por uno de los enteros $1, ..., n$, sin repetición.*

Por ejemplo, los siguientes son tableros de $\lambda = (4,\ 3,\ 1)$

$$\begin{array}{|c|c|c|c|}\hline 1 & 2 & 4 & 5 \\ \hline 3 & 6 & 7 & \multicolumn{1}{c}{} \\ \cline{1-3} 8 & \multicolumn{3}{c}{} \\ \cline{1-1}\end{array} \quad , \qquad \begin{array}{|c|c|c|c|}\hline 4 & 5 & 7 & 3 \\ \hline 2 & 1 & 8 & \multicolumn{1}{c}{} \\ \cline{1-3} 6 & \multicolumn{3}{c}{} \\ \cline{1-1}\end{array} \quad .$$

El grupo simétrico $\mathbb{S}_n$ actúa sobre el conjunto de los tableros de λ en una forma natural permutando los coeficientes. Si consideramos el ejemplo anterior, la permutación $(1\ 4\ 7\ 8\ 6)(2\ 5\ 3)$ manda el primer tablero en el segundo. En particular, un tablero se puede definir como una biyección de $[\lambda]$ en el conjunto $\{1, ..., n\}$; por tanto, dado un tablero t y una permutación σ, la composición $\sigma_o t$ define un nuevo tablero que denominamos σt.

El siguiente resultado relaciona el orden parcial dado sobre las particiones y una propiedad de los tableros.

Lema 2.1 *Sean μ y λ particiones de n, y supongamos que t_1 es un tablero de λ y que t_2 es un tablero de μ. Si para todo i, los números de la i-ésima fila de t_2 pertenecen a distintas columnas de t_1, entonces $\lambda \geq \mu$.*

Demostración:
Tomemos la primera fila del tablero t_2, como cada elemento de esta fila se encuentra en diferente columna en el tablero t_1, debe ser que la cantidad de columnas en el tablero t_1 es mayor o igual a la del tablero t_2, es decir $\lambda_1 \geq \mu_1$. Como los elementos de la segunda fila de t_2 se encuentran en distintas columnas de t_1, tenemos que $\lambda_1 + \lambda_2 \geq \mu_1 + \mu_2$. Siguiendo así, se concluye que $\lambda \geq \mu$. $\square$

Definición 20 *Si t es un tablero, su estabilizador de filas R_t es el subgrupo de $\mathbb{S}_n$ cuyos elementos dejan invariantes cada fila de t. Es decir,*

$$R_t = \{\sigma \in \mathbb{S}_n : \forall\ i, \quad i \text{ y } \sigma(i) \text{ pertenecen a la misma fila}\}.$$

Análogamente se define al estabilizador de columnas C_t de t. Por ejemplo, si

$$t = \begin{array}{|c|c|c|c|}\hline 1 & 2 & 4 & 5 \\ \hline 3 & 6 & 7 & \multicolumn{1}{c}{} \\ \cline{1-3} 8 & \multicolumn{1}{c}{} & \multicolumn{1}{c}{} & \multicolumn{1}{c}{} \\ \cline{1-1} \end{array} \quad , \quad \text{entonces} \quad \begin{array}{l} R_t = \mathbb{S}_{\{1,\ 2,\ 4,\ 5\}} \times \mathbb{S}_{\{3,\ 6,\ 7\}} \times \mathbb{S}_{\{8\}}, \\ \\ C_t = \mathbb{S}_{\{1,\ 3,\ 8\}} \times \mathbb{S}_{\{2,\ 6\}} \times \mathbb{S}_{\{4,\ 7\}} \times \mathbb{S}_{\{5\}}. \end{array}$$

En particular, $|R_t| = 4!\ 3!\ 1!$, y $|C_t| = 3!\ 2!\ 2!\ 1!$.

Definición 21 *Se define sobre el conjunto de los tableros asociados a una partición, una relación de equivalencia dada por*

$$t_1 \sim t_2 \text{ si y sólo si } \quad \sigma(t_1) = t_2, \text{ para algún } \sigma \in R_{t_1}.$$

Esta relación divide al conjunto de tableros de una partición en un conjunto de clase de equivalencias. Llamaremos **tabloide** *$\{t\}$ a la clase de equivalencia de t.*

Generalmente, es útil pensar a los tabloides como tableros sin un orden entre los elementos de cada fila. Notaremos al tabloide $\{t\}$ eliminando las líneas verticales del tablero t, por ejemplo

$$\begin{array}{cccc}\hline 1 & 2 & 4 & 5 \\ 3 & 6 & 7 & \\ 8 & & & \end{array} = \begin{array}{cccc}\hline 4 & 5 & 1 & 2 \\ 7 & 6 & 3 & \\ 8 & & & \end{array},$$

son el mismo $(4,\ 3,\ 1)$-tabloide correspondiente a la clase de conjugación del tablero t.

El grupo simétrico actúa naturalmente sobre el conjunto de los tabloides de la partición λ por $\pi\{t\} = \{\pi t\}$. Veamos que esta acción resulta bien definida:

Supongamos que $\{t_1\} = \{t_2\}$, entonces por definición sabemos que existe $\sigma \in R_{t_1}$ tal que $\sigma(t_1) = t_2$. Como $R_{\pi t_1} = \pi R_{t_1} \pi^{-1}$, entonces $\pi\sigma\pi^{-1} \in R_{\pi t_1}$ y al ser $\pi t_2 = \pi\sigma\pi^{-1}\pi t_1$ se deduce que $\{\pi t_1\} = \{\pi t_2\}$; es decir, la acción está bien definida.

Los siguientes son tabloides de $(2,\ 1)$:

$$\begin{array}{cc}\hline 3 & 2 \\ 1 & \end{array}, \quad \begin{array}{cc}\hline 1 & 3 \\ 2 & \end{array}, \quad \begin{array}{cc}\hline 1 & 2 \\ 3 & \end{array}.$$

En el ejemplo anterior, los tabloides de $(2,\ 1)$ se dieron ordenados según el orden total:

Definición 22 *$\{t_1\} \prec \{t_2\}$ si y sólo si para algún i*

a) Si $j > i$, j está en la misma fila de $\{t_1\}$ y $\{t_2\}$,

b) La fila de $\{t_1\}$ que contiene a i es mayor que la fila de $\{t_2\}$ que contiene a i.

Sin embargo, como en las particiones, el orden más adecuado para nuestro propósito es un orden parcial y está dado por la siguiente definición:

Definición 23 *Dado un tablero t, denotemos por $m_{ir}(t)$ a la cantidad de coeficientes menores o iguales a i en las primeras r filas del tablero t. Entonces $\{t_1\} \leq \{t_2\}$ si y sólo si para todo i, r tenemos que $m_{ir}(t_1) \leq m_{ir}(t_2)$.*

La definición anterior permite ordenar tabloides de todo tipo y tamaño, sin embargo nosotros sólo compararemos tabloides asociados a la misma partición.

2.2.1. Ejemplos de orden parcial entre tabloides

a) Consideremos los siguientes tableros de $(3,\ 3,\ 1)$,

$$t_1 = \begin{array}{|c|c|c|}\hline 1 & 3 & 6 \\ \hline 2 & 5 & 7 \\ \hline 4 \\ \cline{1-1}\end{array}\ , \qquad \text{y} \qquad t_2 = \begin{array}{|c|c|c|}\hline 1 & 2 & 4 \\ \hline 3 & 5 & 6 \\ \hline 7 \\ \cline{1-1}\end{array}\ .$$

Luego, las matrices $(m_{ir}(t_1))_{ir}$ y $(m_{ir}(t_2))_{ir}$ son

$$(m_{ir}(t_1))_{ir} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 2 \\ 2 & 3 & 3 \\ 2 & 3 & 4 \\ 2 & 4 & 5 \\ 3 & 5 & 6 \\ 3 & 5 & 7 \end{pmatrix}, \quad (m_{ir}(t_2))_{ir} = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 2 & 2 \\ 2 & 3 & 3 \\ 3 & 4 & 4 \\ 3 & 5 & 5 \\ 3 & 6 & 6 \\ 3 & 6 & 7 \end{pmatrix}.$$

Comparando los coeficientes de las matrices, se tiene que $\{t_1\} \leq \{t_2\}$.

b) Supongamos que $w < x$ y que w está en la a-ésima fila y x en la b-ésima fila. Luego, por la definición de $m_{ir}(t)$ tenemos que

$$m_{ir}((w\ x)t) - m_{ir}(t) = \begin{cases} 1 & \text{si } b \leq r < a \text{ y } w \leq i < x \\ -1 & \text{si } a \leq r < b \text{ y } w \leq i < x \\ 0 & \text{en cualquier otro caso} \end{cases}$$

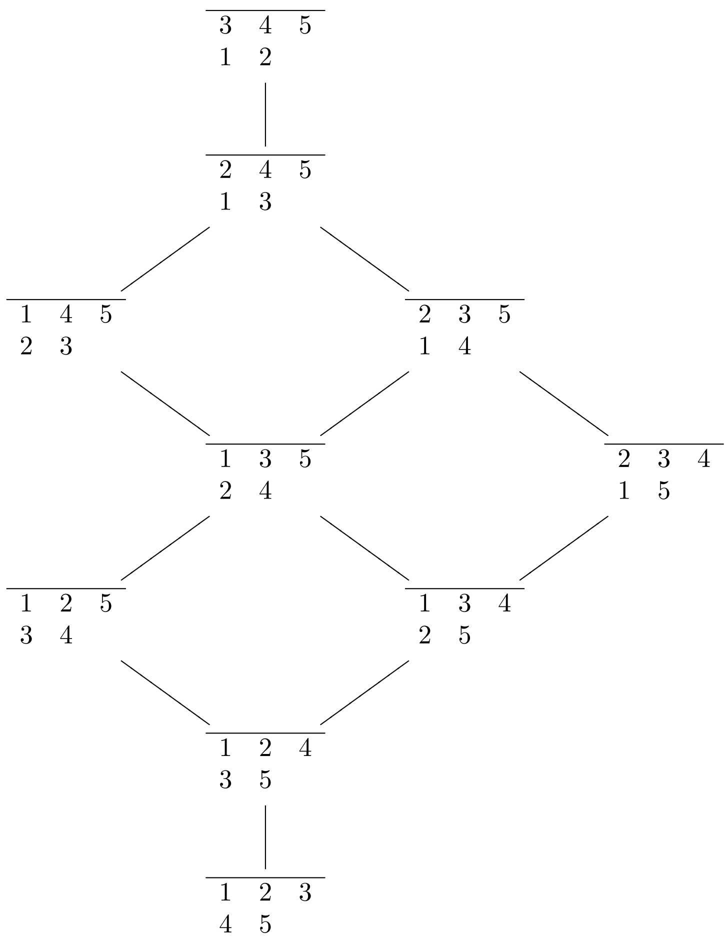
Por tanto, tenemos que

$$\{t\} \leq \{(w\ x)t\} \quad \text{si } w < x \text{ y } w \text{ está por debajo de la fila que contiene a } x. \tag{1}$$

Es fácil ver que los tabloides $\{t\}$ y $\{(x-1\ x)t\}$ son inmediatamente adyacentes en este orden (ver [J]), es decir:

Proposición 2.3 *Si $x-1$ está por debajo de la fila que contiene a x en el tablero t de la partición λ, entonces $\{t\} < \{(x-1\ x)t\}$ y además no existe un tablero de λ $\{t_1\}$ tal que $\{t\} < \{t_1\} < \{(x-1\ x)t\}$.*

c) El siguiente árbol muestra la relación de orden parcial $\leq$ entre los tabloides de $(3,\ 2)$:



2.3. Módulos de Specht

En esta sección encontraremos todos los $\mathbb{S}_n$-módulos irreducibles para cada natural n sobre un cuerpo de característica cero; es decir, se dará una parametrización de las representaciones irreducibles del grupo simétrico de n elementos a través de las particiones de n. Muchos de los teoremas y proposiciones valen sobre cuerpos de cualquier característica y serán usados en capítulos siguientes; por ello supondremos que el cuerpo es arbitrario y haremos hincapié en aquellos resultados donde sea necesario que la característica del cuerpo sea cero; en particular, notaremos S_K^μ y M_K^μ si queremos especificar sobre qué cuerpo se trabaja.

Definición 24 *A cada partición* $\mu = (\mu_1, \ldots, \mu_l)$ *de* n *le asociamos un* **Subgrupo de Young** $\mathbb{S}_\mu$ *de* $\mathbb{S}_n$ *tomando*

$$\mathbb{S}_\mu \quad = \mathbb{S}_{\{1,\ 2,\ldots,\ \mu_1\}} \times \mathbb{S}_{\{\mu_1+1,\ldots,\ \mu_1+\mu_2\}} \times \ldots \times \mathbb{S}_{\{\mu_1+\ldots+\mu_{l-1},\ldots,\ \mu_1+\ldots+\mu_l\}}.$$

Por ejemplo, si $\mu = (3,\ 2,\ 1)$ es una partición de 6, el subgrupo de Young $\mathbb{S}_{(3,\ 2,\ 1)}$ correspondiente está dado por

$$\mathbb{S}_{(3,\ 2,\ 1)} = \mathbb{S}_{\{1,\ 2,\ 3\}} \times \mathbb{S}_{\{4,\ 5\}} \times \ldots \times \mathbb{S}_{\{6\}}.$$

El estudio de las representaciones de $\mathbb{S}_n$ comienza con el estudio del módulo de permutación M^μ de $\mathbb{S}_n$ sobre $\mathbb{S}_\mu$. El módulo de Specht S^μ es un submódulo de M^μ, y cuando el cuerpo es de característica cero, los diferentes módulos de Specht dan todas las representaciones irreducibles de $\mathbb{S}_n$ a medida que varían las permutaciones de n.

Definición 25 *Sea K un cuerpo. Notaremos como M^μ al espacio vectorial sobre K de dimensión finita cuya base son los diferentes tabloides de μ.*

En la sección anterior definimos la acción de $\mathbb{S}_n$ sobre el conjunto de tabloides y vimos que estaba bien definida. Extendiendo linealmente esa acción sobre M^μ, obtenemos sobre M^μ una estructura de $K[\mathbb{S}_n]$-módulo.

Es claro que la acción del subgrupo de Young $\mathbb{S}_\mu$ de una partición μ sobre M^μ deja fijo uno de los tabloides. Supongamos que ese tabloide es $\{t\}$ y que W es el $K[\mathbb{S}_\mu]$ generado por ese tabloide. Es claro que el subgrupo de Young $\mathbb{S}_\mu$ actúa trivialmente sobre el módulo W, o sea, W es el módulo trivial de $\mathbb{S}_\mu$. Luego, como la acción de $\mathbb{S}_n$ sobre los tabloides es de permutación, es fácil ver que

$$M^\mu \quad = \bigoplus_{\sigma \in \mathbb{S}_n/\mathbb{S}_\mu} \sigma.W.$$

Es decir, M^μ es la representación inducida $Ind_{\mathbb{S}_\mu}^{\mathbb{S}_n} W$. En particular se tiene la siguiente proposición:

Proposición 2.4 *M^μ es un módulo de permutación de $\mathbb{S}_n$ sobre el subgrupo $\mathbb{S}_\mu$. M^μ es un $K[\mathbb{S}_n]$-módulo cíclico, generado por cualquier tabloide, y dim $M^\mu = n!/(\mu_1!\mu_2!....\mu_l!)$.*

Definición 26 *Sea t un tablero de μ. La* **suma signada por columnas** *κ_t es un elemento del álgebra de grupo $K[\mathbb{S}_n]$ obtenido mediante la suma de los elementos del estabilizador de columnas C_t de t, multiplicados por su signatura. Esto es,*

$$\kappa_t = \sum_{\sigma \in C_t} sg(\sigma)\sigma.$$

Un **politabloide** *e_t asociado a un tablero t está dado por $e_t = \kappa_t\{t\} \ \in M^\mu$.*

Observación: Notar que un politabloide no sólo depende del tabloide $\{t\}$ sino que también depende del tablero t.

Definición 27 *Un módulo de Specht S^μ para una partición μ de n el submódulo de M^μ generado por los politabloides.*

Por ejemplo, si

$$t = \begin{array}{|c|c|c|}\hline 2 & 5 & 1 \\ \hline 3 & 4 \\ \cline{1-2}\end{array}$$

entonces

$$\kappa_t = 1 - (2\ 3) - (4\ 5) + (2\ 3)(4\ 5) = (1 - (2\ 3))(1 - (4\ 5)).$$

Por tanto,

$$e_t = \begin{array}{ccc}\hline 2 & 5 & 1 \\ 3 & 4 & \end{array} - \begin{array}{ccc}\hline 3 & 5 & 1 \\ 2 & 4 & \end{array} - \begin{array}{ccc}\hline 2 & 4 & 1 \\ 3 & 5 & \end{array} + \begin{array}{ccc}\hline 3 & 4 & 1 \\ 2 & 5 & \end{array}.$$

Veamos como actúa $\mathbb{S}_n$ sobre el conjunto de los politabloides:

Sean $\pi \in \mathbb{S}_n$ y e_t un politabloide de t, luego

$$\begin{aligned} \pi e_t &= \pi\kappa_t\{t\} \\ &= \pi \sum_{\sigma \in\ C_t} sg(\sigma)\sigma\{t\} \\ &= \sum_{\sigma \in\ C_t} sg(\sigma)\pi\sigma\{t\}, \end{aligned}$$

recordando que $C_{\pi t} = \pi C_t \pi^{-1}$ se tiene entonces

$$\begin{aligned}\pi e_t &= \textstyle\sum_{\pi\sigma\in\ C_{\pi t}\pi} sg(\pi^{-1}\pi)sg(\sigma)\pi\sigma\{t\} \\ &= \textstyle\sum_{\mu\in\ C_{\pi t}} sg(\pi)sg(\mu)\mu\{\pi t\} \\ &= sg(\pi)e_{\pi t}.\end{aligned}$$

Por tanto, S^μ es un módulo cíclico, generado por cualquier politabloide.

Ejemplos

Sea $\mathbb{S}_n$ el grupo simétrico de n elementos. Veamos dos ejempos del $\mathbb{S}_n$-módulo cíclico S^μ para dos particiones distintas de n.

a) Si $\mu = (n)$, entonces $\mathbb{S}_\mu = \mathbb{S}_n$. Por tanto, M^μ es el $\mathbb{S}_n$-módulo trivial generado por el tabloide

$$\begin{array}{c}\hline 1 \quad 2... \quad ...n \\ \hline\end{array}$$
.

Luego, $M^\mu = S^\mu$ y S^μ es el módulo trivial de $K[\mathbb{S}_n]$.

b) Si $\mu = (1^n)$, entonces $\mathbb{S}_\mu = \mathbb{S}_{\{1\}} \times \mathbb{S}_{\{2\}} \times \ldots \times \mathbb{S}_{\{n\}} = Id$. Luego, M^μ resulta isomorfo al espacio de representación de la representación regular y S^μ es isomorfo al espacio de representación de la representación signo, puesto que $\pi e_t = sg(\pi)e_t,\ \forall\pi \in \mathbb{S}_n$.

Observación: Notar que en ambos ejemplos, los espacios de representación S^μ son de dimensión 1 y en consecuencia sus representaciones resultan irreducibles.

En lo que sigue demostraremos un lema y un corolario del mismo usando algunas propiedades combinatorias básicas que vimos al principio del capítulo. Estos serán de gran utilidad para demostrar que los $\mathbb{S}_n$-submódulos S^μ resultan irreducibles si la característica del cuerpo es cero.

Lema 2.2 *Sean λ y μ dos particiones de n. Supongamos que t es un tablero de λ, t^* es un tablero de μ y que $\kappa_t\{t^*\} \in M^\mu$ es no nulo. Entonces $\lambda \geq \mu$ y si $\lambda = \mu$ entonces $\kappa_t\{t^*\} = \pm\kappa_t\{t\} = \pm e_t$.*

Demostración:
Sean a y b dos números distintos que pertenecen a la misma fila de $\{t^*\}$. Luego,

$$(1 - (a\ b))\{t^*\} = \{t^*\} - \{(a\ b)t^*\} = 0.$$

Por tanto, a y b no pueden pertenecer a la misma columna en el tabloide $\{t\}$. En efecto, si fuera de otra manera, se podrían conseguir representantes $\sigma_1, \ldots, \sigma_k$ en el conjunto de estabilizadores con signo de columnas de $\{t\}$ que contengan a 1 y a $(a\ b)$ de modo que κ_t admita la escritura

$$\kappa_t = \quad (\sigma_1 + \ldots + \sigma_k)(1 - (a\ b)).$$

Luego, tendríamos que $\kappa_t\{t\} = (\sigma_1 + \cdots + \sigma_k)(1 - (a\ b))\{t\} = 0$ y esto contradice las hipótesis.

Tenemos entonces que para todo i, los número que pertenecen a la i-ésima fila de $\{t^*\}$ pertenecen a distintas columnas de $\{t\}$. Luego, el lema 2.1 nos dice que $\lambda \geq \mu$.

Por otra parte, si $\lambda = \mu$ entonces debe ser que $\{t^*\}$ es uno de los tabloides involucrados en $\kappa_t\{t\}$; en ese caso, $\sigma\{t\} = \{t^*\}$, para alguna permutación $\sigma \in C_t$. Por tanto, se tiene que

$$\kappa_t\{t^*\} = \kappa_t\sigma\{t\} = sg(\sigma)\kappa_t\{t\} =^{+}_{-} \kappa_t\{t\}.$$

□

Corolario 2.3 *Si u es un elemento de M^μ y t es un tablero de μ, entonces $\kappa_t u$ es un múltiplo de e_t.*

Demostración:
Si $u \in M^\mu$, entonces u es combinación lineal de tabloides $\{t^*\}$ de μ. Por el lema anterior tenemos que $\kappa_t\{t^*\}$ es un múltiplo de e_t, luego resulta que u es un múltiplo de e_t. □

Hemos definido el $\mathbb{S}_n$-módulo M^μ como el espacio vectorial generado por los tabloides; en particular se puede definir sobre él una forma bilineal simétrica dando solamente sus valores sobre los elementos de la base. Definimos entonces

$$< -, - >: M^\mu \to K, \quad \text{tal que } < \{t_i\}, \{t_j\} >= \begin{cases} 1 & \text{si } \{t_i\} = \{t_j\}, \\ 0 & \text{si } \{t_i\} \neq \{t_j\}. \end{cases}$$

Claramente esta forma bilineal sobre M^μ resulta no degenerada, simétrica y $\mathbb{S}_n$-invariante (si $\pi \in \mathbb{S}_n$ entonces $< \pi v, \pi w >=< v, w >$, $\forall\ v, w \in M^\mu$). En particular, si el cuerpo de base es $\mathbb{Q}$ entonces esta forma bilineal resulta un producto interno.

Teorema 2.1 *Teorema del submódulo (James).*

Si U es un submódulo de M^μ, entonces $U \supset S^\mu$ ó $U \subset S^{\mu\perp}$.

Demostración:
Sean $u \in U$ y t un tablero de μ. Por el corolario 2.3 sabemos que $\kappa_t u$ es un múltiplos de e_t.

Si este múltiplo es cero para todo $u \in U$ y t tablero de μ, entonces tenemos que

$$\begin{aligned} 0 =< \kappa_t u, \{t\} >= &< \textstyle\sum_{\sigma\in C_t} sg(\sigma)\sigma u,\ \{t\} > \\ &= \textstyle\sum_{\sigma\in C_t} < sg(\sigma)\sigma u,\ \{t\} > \\ &= \textstyle\sum_{\sigma\in C_t} < u,\ sg(\sigma)\sigma^{-1}\{t\} > \\ &=< u,\ \textstyle\sum_{\sigma\in C_t} sg(\sigma)\sigma^{-1}\{t\} > \\ &=< u,\ \kappa_t\{t\} > \\ &=< u,\ e_t > . \end{aligned}$$

Como S^μ es un $\mathbb{S}_n$-módulo que está generado por los politabloides e_t y $< u,\ e_t >= 0$, $\forall\ u, t$, se deduce que $U \subset S^{\mu\perp}$.

Supongamos ahora que podemos elegir u y t tal que $\kappa_t u = a.e_t$, $a \neq 0$. Se deduce entonces que $e_t \in U$. Al ser S^μ un módulo cíclico generado por cualquier politabloide , se tiene que $U \supset S^\mu$ como se quería probar. □

Definición 28 *Diremos que un $K[G]$-módulo V es* **absolutamente irreducible** *si para toda extensión $E \supseteq K$, la representación que se obtiene extendiendo escalares de K en E sigue siendo irreducible. A esta representación de $E[G]$ se la denota V^E.*

Proposición 2.5 *Sea V un $K[\mathbb{S}_n]$-módulo munido de una forma bilineal. La dimensión de $V/(V \cap V^{\perp})$ es igual al rango de la matriz de Gram respecto a una base dada de V.*

Demostración:
Consideremos la aplicación

$$\theta : V \to V^*,$$

$$v \mapsto \psi_v, \quad \text{donde } \psi_v(u) =< u,\ v >,\ \forall\, u \in V.$$

Supongamos que $e_1, ..., e_k$ es la base dada de V y que $\epsilon_1, ..., \epsilon_k$ es la base dual de V^*. Como $< e_i,\ e_j >= \psi_{e_j}(e_i)$ tenemos que

$$\psi_{e_j} =< e_1,\ e_j > \epsilon_1 + ...+ < e_k,\ e_j > \epsilon_k.$$

Si tomamos la matriz de Gram **A** para la base $e_1, ..., e_k$ de V, tenemos que $(a_{ij})_{ij} = (< e_i,\ e_j >)_{ij}$. Es claro que esta matriz coincide con la matriz de θ con respecto a las bases $e_1, ..., e_k$ de V y $\epsilon_1, ..., \epsilon_k$ de V^*.

Por definición de la aplicación de V en V^*, es fácil ver que $Ker\ \theta = (V \cap V^{\perp})$. Luego,

$$\dim V/(V \cap V^{\perp}) = \dim Im\ \theta = \text{ rango de la matriz de Gram.}$$

□

Teorema 2.2 *El $\mathbb{S}_n$-módulo $S^\mu/(S^\mu \cap S^{\mu\perp})$ es cero o es absolutamente irreducible. Más aún, si el cociente es no nulo, entonces $(S^\mu \cap S^{\mu\perp})$ es el único submódulo maximal de S^μ, y $S^\mu/(S^\mu \cap S^{\mu\perp})$ resulta isomorfo a su módulo dual.*

Demostración:
Por el teorema del submódulo, sabemos que cualquier $K[\mathbb{S}_n]$-submódulo de S^μ es el mismo $\mathbb{S}^\mu$ o está contenido en $(S^\mu \cap S^{\mu\perp})$; en particular, si V es un $K[\mathbb{S}_n]$-submódulo de S^μ tal que

$$(S^\mu \cap S^{\mu\perp}) \subseteq V \subseteq S^\mu,$$

entonces $V = S^\mu$ ó $V = (S^\mu \cap S^{\mu\perp})$.

Esto dice que, si el cociente es no nulo, $(S^\mu \cap S^{\mu\perp})$ es el único submódulo maximal de S^μ. Como los $[\mathbb{S}_n]$-submódulos del cociente corresponden biunívocamente a los $\mathbb{S}_n$-submódulos que contienen a $(S^\mu \cap S^{\mu\perp})$, se deduce que $S^\mu/(S^\mu \cap S^{\mu\perp})$ es un $\mathbb{S}_n$-módulo simple.

Se deduce fácilmente de los teoremas de isomorfismos de módulos y de que $V/U \cong$ al dual de $U^{\perp}/V^{\perp}$, siendo $0 \subseteq U \subseteq V$, que el cociente $S^\mu/(S^\mu \cap S^{\mu\perp})$ es isomorfo a su propio dual.

Para terminar la demostración debemos ver que $S^\mu/(S^\mu \cap S^{\mu\perp})$ se mantiene irreducible cuando extendemos el cuerpo de escalares. Tomemos una base $e_1, \ldots, e_k$ de politabloides de S^μ, por la proposición 2.5 sabemos que la dimensión de $S^\mu/(S^\mu \cap S^{\mu\perp})$ es igual al rango de la matriz de Gram con respecto a la base $e_1, \ldots, e_k$ de S^μ. Como los coeficientes de los tabloides involucrados en los elementos de la base son ± 1, tenemos que los coeficientes de la matriz de Gram pertenecen al subcuerpo primo de K. Entonces, el rango de la matriz de Gram es el mismo sobre K que sobre el subcuerpo primo, y por tanto la dimensión de $(S^\mu \cap S^{\mu\perp})$ no cambia si extendemos K; en particular si el cociente es no nulo sobre K entonces resulta no nulo sobre cualquier extensión. Al ser $S^\mu/(S^\mu \cap S^{\mu\perp})$ siempre irreducible, se deduce que es absolutamente irreducible. □

Corolario 2.4 *Si el cuerpo de base es de característica cero, entonces S^μ es irreducible.*

Demostración:
Podemos suponer que el cuerpo es $\mathbb{Q}$ ya que es el cuerpo primo de todo cuerpo K de característica cero. Para demostrar el corolario basta verificar que $(S^\mu \cap S^{\mu\perp}) = 0$. Pero si el cuerpo de base es $\mathbb{Q}$, la forma bilineal definida anteriormente resulta un producto interno; en particular esto implica que $(S^\mu \cap S^{\mu\perp}) = 0$.
□

De los teoremas anteriores se deduce que para cada partición μ de n existe una representación irreducible S^μ si el cuerpo de base es de característica cero. Veamos que si μ y λ son dos particiones distintas de n, entonces las representaciones irreducibles correspondientes resultan no isomorfas.

Lema 2.3 *Si θ es un morfismo de $\mathbb{S}_n$-módulos de M^λ en M^μ y S^λ no está incluido en $Ker\ \theta$, entonces $\lambda \geq \mu$. Si $\lambda = \mu$, entonces $\theta(S^\lambda) = S^\lambda$.*

Demostración:
Sea t un tablero de λ tal que $e_t \notin Ker\ \theta$. Tenemos entonces que

$$0 \neq \theta e_t = \theta \kappa_t \{t\} = \kappa_t \theta \{t\}.$$

Luego, al ser $\theta\{t\}$ una combinación lineal de tabloides de μ y $\kappa_t\theta\{t\} \neq 0$, por el lema 2.2 tenemos que $\lambda \geq \mu$. Si $\lambda = \mu$, entonces θe_t es un múltiplo de e_t. Como S^λ es un módulo cíclico generado por cualquier politabloide, se tiene que $\theta(S^\lambda) = S^\lambda$. □

Corolario 2.5 *Si la característica de K es cero, y $\theta \in Hom_{K[\mathbb{S}_n]}\ (S^\lambda,\ M^\mu)$ es no nulo, entonces $\lambda \geq \mu$. Si $\lambda = \mu$, entonces $\theta(S^\lambda) = S^\lambda$.*

Demostración:
Si $K = \mathbb{Q}$, entonces $< -, - >$ resulta un producto interno. El rango de la matriz de Gram con respecto a una base de S^λ es igual a la dimensión de S^λ para cualquier cuerpo de característica cero. Por tanto, si $car(K) = 0$,

$$(S^\lambda \cap S^{\lambda\perp}) = 0 \quad \text{y} \quad M^\lambda = S^\lambda \oplus S^{\lambda\perp},$$

Si S^λ no está incluido en $Ker\ \theta$, entonces por el teorema del submódulo tenemos que $Ker\ \theta \subseteq S^{\lambda\perp}$.

En particular, cualquier morfismo definido sobre S^λ se puede extender a un morfismo sobre M^λ definiéndolo nulo sobre $S^{\lambda\perp}$. Por tanto, el corolario se sigue del lema anterior. □

Teorema 2.3 *(Representaciones Irreducibles Ordinarias de $\mathbb{S}_n$).*

Sea K de característica cero. Los módulos de Specht sobre K son isomorfos a su módulo dual, son absolutamente irreducibles y dan todas las representaciones ordinarias de $\mathbb{S}_n$

Demostración:
Si $S^\lambda_{\mathbb{Q}} \cong S^\mu_{\mathbb{Q}}$, entonces por el corolario 2.5 $\lambda \geq \mu$, y análogamente, se tiene $\lambda \leq \mu$. Por tanto resulta $\lambda = \mu$.
□

Observación: Con lo hecho hasta aquí, hemos encontrado una representación irreducible S^μ de $\mathbb{S}_n$ para cada partición μ de n. Notar que aquí se hace explícita la relación entre las clases de conjugación de $\mathbb{S}_n$ y las representaciones irreducibles, tarea difícil de resolver cuando se trabaja con otros grupos.

Como M^λ completamente reducible cuando $car(K) = 0$, del corolario 2.5 también se deduce el siguiente

Teorema 2.4 *Si $car(K) = 0$, M^λ es completamente reducible y sus sumandos directos son S^λ, una sola vez, y algunos $\{S^\mu : \lambda < \mu\}$, posiblemente con repeticiones.*

Observación: Las representaciones irreducibles de $\mathbb{S}_n$ se pueden construir de manera intrínseca al álgebra de grupo $K[\mathbb{S}_n]$, correspondiendo a ideales generados por elementos del álgebra que se denominan *simetrizadores de Young* y se construyen de la siguiente manera:

Sean λ una partición de n y t un tablero de λ. Consideremos los subgrupos de $\mathbb{S}_n$ dados por C_t y R_t. En el álgebra de grupo, introducimos dos elementos que corresponden a estos dos subgrupos, a saber

$$a_\lambda = \sum_{\sigma\in\ R_t} \sigma, \quad \kappa_\lambda = \sum_{\sigma\in\ C_t} sg(\sigma)\sigma.$$

Para ver como actúan estos elementos, primero necesitamos algunas definiciones.

Definición 29 *Sea V un K espacio vectorial. Definimos las potencias exteriores $\bigwedge^n V$, a veces notadas como $Alt^n\ V$, como un espacio vectorial sobre K munido de una aplicación multilineal y alternada*

$$V \times \ldots \times V \to \bigwedge^n V,$$

$$v_1 \times \ldots \times v_n \mapsto v_1 \wedge \ldots \wedge v_n,$$

tal que cumple la siguiente propiedad universal: Para toda aplicación multilineal y alternada $\beta : V \times .... \times V \to U$, se tiene que existe una única función $\psi : \bigwedge^n V \to U$ tal que el siguiente diagrama conmuta

$$\begin{tikzcd} V \times .... \times V \arrow[r] \arrow[dr, "\beta"'] & \bigwedge^n V \arrow[d, dashed, "\exists! \psi"] \\ & U \end{tikzcd} \quad . \tag{2}$$

Una función multilineal β se dice *alternada* si $\beta(v_1, \ldots, v_n) = 0$ cada vez que dos de los vectores v_i son iguales. Esto implica que $\beta(v_1, \ldots, v_n)$ cambia de signo cuando dos vectores se intercambian, es decir

$$\beta(v_{\sigma(1)}, \ldots, v_{\sigma(n)}) = sg(\sigma)\beta(v_1, \ldots, v_n), \quad \forall\ \sigma \in \mathbb{S}_n.$$

Si $\{e_i\}_i$ es una base de V, entonces

$$\{e_{i_1} \wedge e_{i_2} \wedge \ldots \wedge e_{i_n} : i_1 < i_2 < .... < i_n\},$$

es una base para $\bigwedge^n V$. En particular, $\bigwedge^n V = 0$ si $n > dim\ V$.

Análogamente se definen las potencias simétricas:

Definición 30 *Sea V un espacio vectorial sobre K. Las potencias simétricas $Sym^n\ V$ son espacios vectoriales munidos con una aplicación multilineal simétrica universal*

$$V \times \ldots \times V \to Sym^n\ V,$$

$$v_1 \times \ldots \times v_n \mapsto v_1 \cdot \cdots \cdot v_n.$$

Una función multilineal $\beta : V \times \ldots \times V \to U$ se dice *simétrica* si no cambia su valor cuando se intercambian cualquier par de factores, esto es

$$\beta(v_{\sigma(1)}, \ldots, v_{\sigma(n)}) = \beta(v_1, \ldots, v_n), \quad \forall\, \sigma \in \mathbb{S}_n.$$

Si $\{e_i\}_i$ es una base de V, entonces

$$\{e_{i_1} \cdot e_{i_2} \cdot \cdots \cdot e_{i_n} : i_1 \leq i_2 \leq .... \leq i_n\},$$

es una base para $Sym^n\ V$.

Ahora bien, supongamos que V es un espacio vectorial y que $\mathbb{S}_n$ actúa sobre la n-ésima potencia tensorial $V^{\otimes n}$ permutando factores. La imagen del elemento a_t en $End(V^{\otimes n})$ es el subespacio

$$Im(a_\lambda) = Sym^{\lambda_1}\ V \otimes Sym^{\lambda_2}\ V \otimes \ldots \otimes Sym^{\lambda_k}\ V \quad \hookrightarrow V^{\otimes n},$$

donde la inclusión de la derecha se obtiene reagrupando los factores de $V^{\otimes n}$ de acuerdo con las filas del tablero de Young.

Análogamente, la imagen de κ_λ sobre la potencia tensorial viene dada por

$$Im(\kappa_\lambda) = \bigwedge^{\mu_1}\ V \otimes \bigwedge^{\mu_2}\ V \otimes \ldots \otimes \bigwedge^{\mu_k}\ V \quad \hookrightarrow V^{\otimes n},$$

donde la partición μ es la conjugada de la partición λ.

Finalmente, tomamos

$$c_\lambda = a_\lambda.\kappa_\lambda \quad \in \mathbb{S}_n.$$

Este elemento del álgebra de grupo se denomina **simetrizador de Young**.

Por ejemplo, cuando $\lambda = (n)$ tenemos que

$$c_{(n)} = a_{(n)} = \textstyle\sum_{\sigma \in \mathbb{S}_n} \sigma,$$

y la imagen de $c_{(n)}$ en $V^{\otimes n}$ es $Sym^n\ V$. Cuando $\lambda = (1^n)$ tenemos que

$$c_{(1^n)} = b_{(1^n)} = \kappa_(1^n) = \textstyle\sum_{\sigma \in \mathbb{S}_n} sg(\sigma)\sigma$$

y la imagen de $c_{(1^n)}$ en $V^{\otimes n}$ es $\bigwedge^n\ V$.

Veamos cómo se relaciona con la construcción de los módulos de Specht dados anteriormente. Sea t un tablero de una partición λ de n y consideremos la siguiente aplicación definida sobre el ideal a derecha $\mathcal{I} = a_\lambda K[\mathbb{S}_n]$ de $K[\mathbb{S}_n]$ generado por a_λ

$$\theta : \mathcal{I} \to M^\lambda,$$

$$a_\lambda \pi \mapsto \pi\{t\}, \quad \pi \in \mathbb{S}_n.$$

Claramente θ es un $K[\mathbb{S}_n]$ isomorfismo bien definido del ideal $\mathcal{I}$ en M^λ. La buena definición se deduce de lo siguiente:

$$a_\lambda \pi = a_\lambda \Leftrightarrow \pi \in\ R_t \Leftrightarrow \pi\{t\} = \{t\}.$$

Si restringimos θ al ideal a derecha $a_\lambda \kappa_\lambda K[\mathbb{S}_n]$ se obtiene un isomorfismo de $a_\lambda \kappa_\lambda K[\mathbb{S}_n]$ en S^λ. Usando este isomorfismo, cada resultado puede ser interpretado en términos del álgebra de grupo.

2.3.1. Ejemplos

a) Consideremos la partición $(n-1,\ 1)$ de n y su correspondiente módulo de permutación $M^{(n-1,\ 1)}$. Luego, sabemos que en su descomposición encontramos una vez a $S^{(n-1,\ 1)}$ y algunos $\{S^{\mu} : (n-1,\ 1) < \mu\}$, posiblemente más de una vez. Como existe sólo una partición μ de n tal que $(n-1,\ 1) < \mu$ y ésa es (n), si *car* $K = 0$, tenemos que

$$M^{(n-1,\ 1)} = S^{(n-1,\ 1)} \oplus a.S^{(n)}.$$

Sabemos que $M^{(n-1,\ 1)}$ tiene dimensión n, ya que hay n tabloides distintos para esta partición. Sea $\{\overline{1}, \overline{2}, ..., \overline{n}\}$ una base de $M^{(n-1,\ 1)}$. Luego, podemos definir $S^{(n-1,\ 1)}$ de la siguiente manera

$$S^{(n-1,\ 1)} = K[\mathbb{S}_n](e_2 - e_1) = \{\textstyle\sum_i a_i.\overline{i} : a_1 + ... + a_n = 0\}.$$

Por tanto, se deduce que la dimensión de $S^{(n-1,\ 1)}$ es $n-1$; y como $dim(S^{(n)}) = 1$, debe ser que $a = 1$, entonces

$$M^{(n-1,\ 1)} = S^{(n-1,\ 1)} \oplus S^{(n)}.$$

Claramente, $S^{(n-1,\ 1)^{\perp}} = K[\mathbb{S}_n](\overline{1} + \overline{2} + ... + \overline{n})$. Luego, si la característica de K no divide a n, entonces

$$M^{(n-1,\ 1)} = S^{(n-1,\ 1)} \oplus S^{(n-1,\ 1)^{\perp}}.$$

Notar que en todos los casos, tenemos que $S^{(n-1,\ 1)^{\perp}} \cong S^{(n)}$ y que la dimensión de $S^{(n-1,\ 1)}$ es $n-1$.

b) Sea $n = 3$ y descompongamos $M^{(2,\ 1)}$ como en el ejemplo *a)*

$$M^{(2,\ 1)} = S^{(2,\ 1)} \oplus S^{(3)},$$

siendo $dim(S^{(2,\ 1)}) = 2$ y $dim(S^{(3)}) = 1$. Esto concuerda con los ejemplos que vimos en el capítulo 1 donde encontramos las representaciones irreducibles de $\mathbb{S}_3$. Supongamos que $K = \mathbb{C}$, entonces $M^{(2,\ 1)}$ resulta isomorfo a $\mathbb{C}^3$, $S^{(3)}$ a la representación trivial U y $S^{(2,\ 1)}$ a la representación estándar V. En conclusión, recordando que la tercera representación irreducible de $\mathbb{S}_3$ viene dada por la representación signo $U^{'}$, tenemos que

$$M^{(2,\ 1)} \cong \mathbb{C}^3, \quad S^{(3)} \cong U,$$

$$S^{(2,\ 1)} \cong V, \qquad S^{(1^3)} \cong U^{'}.$$

En particular, tenemos la siguiente tabla de caracteres

	1	3	2
$\mathbb{S}_3$	id	$(1\ 2)$	$(1\ 2\ 3)$
$S^{(3)}$	1	1	1
$S^{(2,\ 1)}$	2	0	-1
$S^{(1,\ 1,\ 1)}$	1	-1	1

.

Observación: Notar que se ha cambiado el orden de las filas y la notación de las representaciones irreducibles. El orden de las filas está dado por el orden total definido sobre el conjunto de particiones de 3.

2.4. Base estándar de los módulos de Specht

En esta sección se dará una base para cada módulo de Specht; en particular se dará a conocer la dimensión de cada uno que resulta de gran utilidad cuando se calculan tablas de caracteres.

Definición 31 *Sea λ una partición de n. Un tablero t de λ se dice un* **tablero estándar** *si los coeficientes aumentan a lo largo de las filas y hacia abajo en las columnas de t.*

Un tabloide $\{t\}$ de λ se dice **tabloide estándar** *si existe un tablero estándar en la clase de equivalencia de $\{t\}$. Un politabloide e_t se dice estándar si t es estándar.*

Por ejemplo, los siguientes son tableros estándar de la partición $(3,\ 2)$ de 5:

$$t_1 = \begin{array}{|c|c|c|}\hline 1 & 3 & 5 \\ \hline 2 & 4 \\ \cline{1-2}\end{array}\ , \quad t_2 = \begin{array}{|c|c|c|}\hline 1 & 2 & 5 \\ \hline 3 & 4 \\ \cline{1-2}\end{array}\ , \quad t_3 = \begin{array}{|c|c|c|}\hline 1 & 3 & 4 \\ \hline 2 & 5 \\ \cline{1-2}\end{array}\ ,$$

$$t_4 = \begin{array}{|c|c|c|}\hline 1 & 2 & 4 \\ \hline 3 & 5 \\ \cline{1-2}\end{array}\ , \quad t_5 = \begin{array}{|c|c|c|}\hline 1 & 2 & 3 \\ \hline 4 & 5 \\ \cline{1-2}\end{array}\ .$$

Observación: Un tabloide estándar contiene sólo un tablero estándar, dado que los coeficientes deben aumentar a lo largo de las filas de un tablero estándar. Sin embargo, un politabloide puede contener más de un tabloide estándar, como por ejemplo e_{t_5} que contiene a $\{t_1\}$ y a $\{t_5\}$:

$$e_{t_5} = \begin{array}{ccc}\hline 1 & 2 & 3 \\ 4 & 5 \end{array} - \begin{array}{ccc}\hline 2 & 3 & 4 \\ 1 & 5 \end{array} - \begin{array}{ccc}\hline 1 & 3 & 5 \\ 2 & 4 \end{array} + \begin{array}{ccc}\hline 3 & 4 & 5 \\ 1 & 2 \end{array}.$$

Veremos que los politabloides estándar forman una base para los módulos de Specht, definidos sobre *cualquier* cuerpo.

En las secciones anteriores hemos dado un orden total para los tabloides de una partición μ dada. La independencia lineal de los politabloides se deduce del siguiente lema:

Lema 2.4 *Sean $v_1, v_2, \ldots, v_m$ elementos de M^μ y supongamos que $\{t_i\}$ es el mayor tabloide involucrado en v_i respecto al orden total $\prec$. Si los tabloides $\{t_i\}$ son todos diferentes, entonces $v_1, v_2, \ldots, v_m$ son linealmente independientes.*

Demostración:
Podemos suponer que $\{t_1\} < \{t_2\} < \ldots < \{t_m\}$. Si

$$a_1v_1 + a_2v_2 + \cdots + a_mv_m = 0, \quad a_i \in\ K \quad \text{y} \quad a_{j+1} = \ldots = a_m = 0,$$

entonces a_j debe ser cero ya que $\{t_j\}$ está involucrado en v_j y no lo está en $v_k,$ con $k < j$. Por tanto, tenemos que $a_1 = a_2 = \ldots = a_m = 0$, es decir, los vectores son linealmente independientes. □

Es claro que $\{t\}$ es el mayor tablero involucrado en e_t cuando t es estándar. De este hecho se deduce que los politabloides estándar son linealmente independientes, ya que los tabloides estándar involucrados en cada politabloide son distintos. Sin embargo, damos a continuación un resultado más fuerte donde se usa sólo el orden parcial sobre los tabloides.

Lema 2.5 *Si t tiene los coeficientes que aumentan hacia abajo en las columnas, entonces todos los tabloides $\{t^{'}\}$ involucrados en e_t satisfacen que $\{t^{'}\} < \{t\}$.*

Demostración:
Si $t^{'} = \pi t$, tal que π es un elemento distinto de la identidad en el estabilizador de columnas de t, entonces en alguna columna de $t^{'}$ existen coeficientes $w < x$ tal que w está en alguna fila abajo de x. Luego, por (1) tenemos que $\{t^{'}\} < \{(w\ x)t^{'}\}$. Como $(w\ x)$ está involucrado en e_t, aplicando un argumento inductivo se tiene que $\{(w\ x)t^{'}\} \leq \{t\}$, entonces $\{t^{'}\} < \{t\}$. $\square$

Para demostrar que los politabloides estándar generan el módulo de Specht, debemos primero encontrar elementos del álgebra de grupo $K[\mathbb{S}_n]$ que anulen a un politabloide e_t dado.

Fijemos un tablero t de una partición μ de n. Sean X un subconjunto de la i-ésima columna de t, e Y un subconjunto de la $(i+1)$-ésima columna de t. Sean $\sigma_1, \sigma_2, \ldots, \sigma_k$ representantes de las coclases para el cociente $\mathbb{S}_{X\cup Y}/(\mathbb{S}_X \times \mathbb{S}_Y)$, y sea

$$G_{X,Y} = \sum_{j=1}^{k} sg(\sigma_j)\sigma_j.$$

$G_{X,Y}$ se denomina el *elemento de Garnir*. De aquí en adelante, X se tomará al final de la i-ésima columna de t e Y se tomará al principio de la $(i+1)$-ésima columna. Claramente, las permutaciones $\sigma_1, \sigma_2, \ldots, \sigma_k$ no son únicas; sin embargo, para fines prácticos, podemos tomar $\sigma_1, \sigma_2, \ldots, \sigma_k$ tal que $\sigma_1(t), \sigma_2(t), \ldots, \sigma_k(t)$ sean tableros que coinciden con el tablero t excepto en las posiciones ocupadas por $X \cup Y$, cuyos coeficientes aumentan verticalmente hacia abajo en las posiciones ocupadas por $X \cup Y$.

Por ejemplo, si

$$t = \begin{array}{|c|c|}\hline 1 & 2 \\ \hline 4 & 3 \\ \hline 5 & \multicolumn{1}{c}{} \\ \cline{1-1}\end{array} \qquad X = \{4,\ 5\} \quad \text{e} \quad Y = \{2,\ 3\},$$

entonces se pueden tomar $\sigma_1(t),\ \sigma_2(t), \ldots, \sigma_k(t)$ como

$$\begin{array}{c} t = t_1 = \begin{array}{|c|c|}\hline 1 & 2 \\ \hline 4 & 3 \\ \hline 5 & \multicolumn{1}{c}{} \\ \cline{1-1}\end{array}\ , \quad t_2 = \begin{array}{|c|c|}\hline 1 & 2 \\ \hline 3 & 4 \\ \hline 5 & \multicolumn{1}{c}{} \\ \cline{1-1}\end{array}\ , \quad t_3 = \begin{array}{|c|c|}\hline 1 & 2 \\ \hline 3 & 5 \\ \hline 4 & \multicolumn{1}{c}{} \\ \cline{1-1}\end{array}\ , \\ \\ t_4 = \begin{array}{|c|c|}\hline 1 & 3 \\ \hline 2 & 4 \\ \hline 5 & \multicolumn{1}{c}{} \\ \cline{1-1}\end{array}\ , \quad t_5 = \begin{array}{|c|c|}\hline 1 & 3 \\ \hline 2 & 5 \\ \hline 4 & \multicolumn{1}{c}{} \\ \cline{1-1}\end{array}\ , \quad t_6 = \begin{array}{|c|c|}\hline 1 & 4 \\ \hline 2 & 5 \\ \hline 3 & \multicolumn{1}{c}{} \\ \cline{1-1}\end{array}\ , \end{array} \tag{3}$$

donde

$$sg(\sigma_i) = \begin{cases} 1 & \text{para } i = 1,\ 3,\ 4,\ 6 \\ \\ -1 & \text{para } i = 2,\ 5 \end{cases},$$

entonces $G_{X,Y} = 1 - (3\ 4) + (3\ 4\ 5) + (2\ 3\ 4) - (2\ 3\ 4\ 5) + (2\ 4)(3\ 5)$.

Daremos a continuación un teorema que muestra el elemento que anula a un politabloide dado. Su demostración se puede encontrar en [P].

Teorema 2.5 *Sean $\mu = (\mu_1, \ldots, \mu_l)$ una partición de n y $\mu^{'} = (\mu^{'}_1, \ldots, \mu^{'}_s)$ la partición conjugada de μ. Si $|X \cup Y| > \mu^{'}_i$ entonces $G_{X,Y}e_t = 0$ sobre cualquier cuerpo.*

Para el ejemplo anterior, del teorema se deduce que

$$0 = G_{X,Y}e_t = e_{t_1} - e_{t_2} + e_{t_3} + e_{t_4} - e_{t_5} + e_{t_6},$$

entonces se tiene que

$$e_t = e_{t_2} - e_{t_3} - e_{t_4} + e_{t_5} - e_{t_6}.$$

Ahora estamos en condiciones de probar que los politabloides estándar generan los módulos de Specht.

Teorema 2.6 *El conjunto $\{e_t : t$ es un tablero estándar de $\mu\}$ es una base de S^μ.*

Demostración:
Se ha probado que los politabloides estándar son linealmente independientes, ahora usaremos las relaciones de Garnir para probar que cualquier politabloide se puede escribir como combinación lineal de politabloides estándar.

Notaremos por $[t]$ a la clase de equivalencia de t por C_t; esto es,

$$[t] = \{t^{'}; t^{'} = \pi t, \text{ para algún } \pi \in C_t\}.$$

Esta clase de equivalencia está totalmente ordenada de manera similar al orden sobre las clases de equivalencia por filas (22).

Supongamos que t no es un tablero estándar, demostraremos que e_t se puede escribir como combinación lineal de politabloides estándar por inducción sobre el orden; es decir, supondremos que es cierto para $e_{t'}$ cuando $[t^{'}] < [t]$ y probaremos el resultado para e_t. Es fácil ver que se cumple para el primer elemento, ya que el politabloide que lo contiene es estándar.

Como $\pi e_t = sg(\pi)e_t$, si $\pi \in C_t$, podemos suponer que los coeficientes de t están en orden creciente hacia abajo en las columnas. Si el tablero t no es estándar, entonces deben existir dos columnas, digamos la j y $(j+1)$-ésima columnas, tal que sus coeficientes son $a_1 < a_2 < \ldots < a_r$ y $b_1 < b_2 < \ldots < b_s$ y que $a_q > b_q$ para algún q.

Sean $X = \{a_q, \ldots, a_r\}$ e $Y = \{b_1, \ldots, b_q\}$ y consideremos el elemento de Garnir correspondiente $G_{X,Y} = \sum sg(\sigma)\sigma$. Por el teorema 2.5, tenemos que

$$0 = G_{X,Y}e_t = \sum sg(\sigma)\sigma e_t = \sum sg(\sigma)e_{\sigma t}. \tag{4}$$

Por construcción de X e Y tenemos que $b_1 < \ldots < b_q < a_q < \ldots < a_r$. Luego, para cualquier σ en la sumatoria del elemento de Garnir, se tiene que $[\sigma t] < [t]$.

Por hipótesis inductiva, tenemos que para todo σ involucrado en el elemento de Garnir se cumple que $e_{\sigma t}$ es una combinación lineal de politabloides estándar. Por tanto, la demostración del teorema se sigue del hecho que $e_{t_1} = e_t$ y de la igualdad (4). □

De aquíse deduce inmediatamente el siguiente corolario, que afirma que la dimensión de los módulos de Specht no varía cuando se cambia el cuerpo de base.

Corolario 2.6 *La dimensión de los módulos de Specht S^μ es independiente del cuerpo de base y es igual al número de tableros estándar.*

De la demostración del teorema anterior se deduce otro corolario. Este permite reducir representaciones de $\mathbb{S}_n$ sobre $\mathbb{Q}$ a representaciones sobre un cuerpo finito.

Corolario 2.7 *En $S^\mu_{\mathbb{Q}}$ cualquier politabloide se puede escribir como una combinación lineal con coeficientes enteros de los politabloides estándar.*

Diremos que una base de S^μ es **estándar** si todos sus elementos son politabloides estándar. Entonces, del corolario anterior se deduce lo siguiente:

Corolario 2.8 *Las matrices de representación de $\mathbb{S}_n$ sobre $\mathbb{Q}$ con respecto a una base estándar de $S^\mu_{\mathbb{Q}}$ tienen todos los coeficientes enteros.*

Demostración:
Se deduce inmediatamente del hecho que $\pi e_t = e_{\pi t}, \ \forall \ \pi \in \mathbb{S}_n$, que vale en particular para la base de politabloides estándar, y del corolario anterior. $\square$

Daremos ahora un corolario que nos será de gran utilidad más adelante, cuando estudiemos las representaciones de $\mathbb{S}_n$ sobre cuerpos de característica positiva.

Corolario 2.9 *Sea v un elemento no nulo de S^μ y ordenemos los tabloides de v, según el orden parcial, en cadenas crecientes. Entonces todo tabloide involucrado en v que resulte el último de una cadena ascendente (el mayor entre los elementos de la cadena), es estándar.*

Demostración:
Como v es un elemento de S^μ, sabemos que es una combinación lineal de los politabloides estándar. Por otro lado, por el lema 2.5 tenemos que todos los tabloides $\{t^{'}\}$ involucrados en el politabloide estándar e_{t_i} verifican $\{t_i^{'}\} < \{t_i\}$, siendo t_i un tablero estándar. Por tanto, los tabloides que resultan los mayores son estándar. $\square$

El orden parcial nos permite parametrizar la base de los módulos de Specht por los politabloides estándar, lo cual resulta muy útil para cálculos numéricos.

Corolario 2.10 *Existe una base de S^μ cuyos elementos contienen un único tabloide estándar.*

Demostración:
Sean $\{t_1\} < \{t_2\} < \ldots < \{t_k\}$ los tabloides estándar de μ. Por el lema 2.5 sabemos que $\{t_1\}$ es el único tabloide estándar involucrado en e_{t_1}. Sin embargo, e_{t_2} puede contener a $\{t_1\}$. Supongamos que el coeficiente de $\{t_1\}$ en e_{t_2} es a, entonces reemplacemos e_{t_2} por $f_{t_2} = e_{t_2} - a.e_{t_1}$. Luego, $\{t_2\}$ es el único tabloide estándar involucrado en f_{t_2}. Continuando de esta manera, se construye la base deseada. $\square$

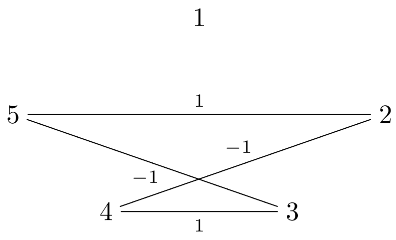
Ejemplo

Examinemos $M^{(3,\ 2)}$ en detalle, a través de una descripción geométrica.

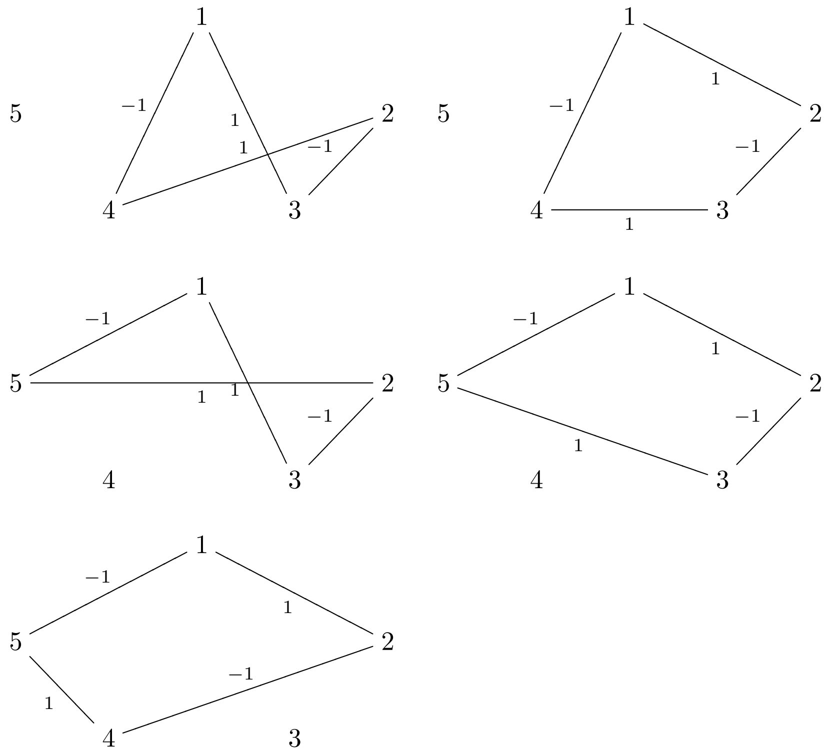
Un tabloide de la partición (3, 2) está determinado por el par de números $\overline{ij}$ que forman su segunda fila. Por tanto, podemos representar cada tabloide de $S^{(3,\ 2)}$ por su correspondiente par de números $\overline{ij}$. Para obtener una descripción geométrica de $M^{(3,\ 2)}$, consideremos el conjunto de grafos con 5 nodos, sin lazos, tales que a cada arista se le permite tener un *peso* determinado por un coeficiente en el cuerpo de base. Identificando $\overline{ij}$ con la arista que une los nodos i y j, obtenemos una costrucción isomorfa de $M^{(3,\ 2)}$. Por ejemplo, el elemento

$$\overline{\begin{matrix} 2 & 5 & 1 \\ 3 & 4 & \end{matrix}} - \overline{\begin{matrix} 3 & 5 & 1 \\ 2 & 4 & \end{matrix}} - \overline{\begin{matrix} 2 & 4 & 1 \\ 3 & 5 & \end{matrix}} + \overline{\begin{matrix} 3 & 4 & 1 \\ 2 & 5 & \end{matrix}},$$

corresponde a la figura



Sabemos que el módulo de Specht $S^{(3,\ 2)}$ está generado por los politabloides estándar e_{t_i}; más aún, existe una base cuyos elementos involucran solamente un tabloide estándar. Estos se deducen de la construcción de los tableros estándar dados en (2.4) y corresponden a los siguientes grafos:



respectivamente.

Las diez aristas están ordenadas por 22 de la siguiente manera:

$$\overline{1\ 2} < \overline{1\ 3} < \overline{2\ 3} < \overline{1\ 4} < \overline{2\ 4} < \overline{3\ 4} < \overline{1\ 5} < \overline{2\ 5} < \overline{3\ 5} < \overline{4\ 5},$$

donde los últimas aristas involucradas en $e_{t_1}, e_{t_2}, e_{t_3}, e_{t_4}, e_{t_5}$ son

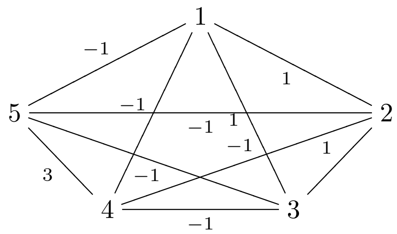
$$\overline{2\ 4} < \overline{3\ 4} < \overline{2\ 5} < \overline{3\ 5} < \overline{4\ 5};$$

los cuales corresponden a los tabloides $\{t_1\}, \{t_2\}, \{t_3\}, \{t_4\}$ y $\{t_5\}$.

Por lo dicho anteriormente, estos politabloides son linealmente independientes ya que sus últimos tabloides son todas diferentes, y generan el módulo de Specht $S^{(3\ 2)}$; en particular se tiene que $dim(S^{(3\ 2)}) = 5$.

Como e_{t_5} contiene dos tabloides estándar, a saber $\overline{2\ 4}$ y el $\overline{4\ 5}$, reemplazemos e_{t_5} por $f_{t_5} = e_{t_1} + e_{t_5}$ para obtener una base que cada elemento contenga a solo un tabloide estándar. Luego, $e_1, e_2, e_3, e_4, f_{t_5}$ contiene a $\overline{2\ 4}, \overline{3\ 4}, \overline{2\ 5}, \overline{3\ 5}, \overline{4\ 5}$ respectivamente, con coeficiente 1.

Por tanto, si $v \in S^{(3\ 2)}$ es de la forma



,

tenemos que v involucra a $-\overline{2\ 4}, -\overline{3\ 4}, -\overline{2\ 5}, -\overline{3\ 5}, 3.\overline{4\ 5}$,. Luego, debe ser que

$$\begin{aligned} v &= -e_{t_1} - e_{t_2} - e_{t_3} - e_{t_4} + 3.f_{t_5} \\ &= 2.e_{t_1} - e_{t_2} - e_{t_3} - e_{t_4} + 3.e_{t_5}. \end{aligned}$$

□

Recordemos que la partición $\lambda^{'}$ conjugada de una partición λ se obtiene cambiando las filas por las columnas en el diagrama de $[\lambda]$.

Como los coeficientes de los tabloides involucrados en los politabloides están en el anillo de los enteros, podemos analizar las representaciones irreducibles de $\mathbb{S}_n$ sobre un cuerpo de característica cero, directamente sobre el cuerpo $\mathbb{Q}$ de los enteros racionales.

Teorema 2.7 *Si λ es una partición de n, entonces la representación dada por $S^{\lambda}_{\mathbb{Q}} \otimes S^{(1^n)}_{\mathbb{Q}}$ es isomorfa al dual de la representación dada por $S^{\lambda^{'}}_{\mathbb{Q}}$.*

Nota: Por el teorema 2.2, si *car* $K = 0$ entonces $S^{\lambda^{'}}_{\mathbb{Q}}$ es isomorfo a su dual. Por tanto, en la demostración del teorema se omitirán las palabras “el dual de”. Cabe remarcar que si el cuerpo es de característica positiva, esta distinción debe ser hecha, ya que $S^{\lambda^{'}}_{\mathbb{Q}}$ y su dual no resultan isomorfos, en general.

Demostración:
Sea t un tablero de λ y $t^{'}$ el correspondiente tablero de la partición conjugada $\lambda^{'}$. Por ejemplo, si

$$t = \begin{array}{|c|c|c|} \hline 1 & 2 & 3 \\ \hline 4 & 5 \\ \cline{1-2} \end{array} \qquad \text{entonces } t^{'} = \begin{array}{|c|c|} \hline 1 & 4 \\ \hline 2 & 5 \\ \hline 3 \\ \cline{1-1} \end{array} .$$

Consideremos los siguientes elementos del álgebra de grupo:

$$\rho_{t'} = \textstyle\sum_{\{\pi \in\ R_{t'}\}} \pi \text{ y } \kappa_{t'} = \sum_{\{\pi \in\ C_{t'}\}} sg(\pi)\pi.$$

Sea u un generador del módulo cíclico $S^{(1^n)}$, tal que $\pi u = sg(\pi)u, \pi \in \mathbb{S}_n$. Es fácil ver que se puede definir un epimorfismo θ sobre $\mathbb{Q}[\mathbb{S}_n]$ tal que

$$\theta : M^{\lambda^{'}}_{\mathbb{Q}} \to S^{\lambda}_{\mathbb{Q}} \otimes S^{(1^n)}_{\mathbb{Q}},$$

$$\{t^{'}\} \mapsto \rho_{t'}(\{t\} \otimes u).$$

En efecto, si $\{t^{'}\} = \{t^{'}_1\}$, entonces existe $\sigma \in\ R_{t'}$ tal que $t^{'}_1 = \sigma t^{'}$. Luego,

$$\theta(\{t^{'}_1\}) = \theta(\{\sigma t^{'}\}) = \rho_{\sigma t'}(\{t\} \otimes u) = \rho_{t'}(\{t\} \otimes u) = \theta(\{t^{'}\}).$$

Como $\{\{\sigma t^{'}\} : \sigma \in \mathbb{S}_n\}$ es una base del módulo cíclico $M_{\mathbb{Q}}^{\lambda^{'}}$, θ queda definido por

$$\begin{aligned} \theta(\{\sigma t^{'}\}) &= \sigma\rho_{t^{'}}(\{t\} \otimes u) = \sigma(\rho_{t^{'}}\{t\} \otimes \rho_{t^{'}} u) \\ &= \sigma(\kappa_t\{t\} \otimes u) = (\sigma\kappa_t\{t\} \otimes \sigma u) \\ &= (\kappa_{\sigma t}\{\sigma t\} \otimes sg(\sigma)u) = sg(\sigma)(\kappa_{\sigma t}\{\sigma t\} \otimes u). \end{aligned}$$

Luego,

$$\theta(\kappa_{t^{'}}\{t^{'}\}) = \kappa_{t^{'}}\rho_{t^{'}}(\{t\} \otimes u) = \rho_t\kappa_t\{t\} \otimes u.$$

Por otra parte,

$$< \rho_t\kappa_t\{t\}, \{t\} >=< \kappa_t\{t\}, \rho_t\{t\} >=< \kappa_t\{t\}, |R_t|\{t\} >= |R_t|.$$

Como $|R_t|$ es un escalar no nulo sobre $\mathbb{Q}$, tenemos que $\theta(\kappa_{t^{'}}\{t^{'}\}) \neq 0$. Por tanto, $Ker\ \theta \not\supseteq S_{\mathbb{Q}}^{\lambda^{'}}$, y por el teorema del submódulo se tiene que $Ker\ \theta \subseteq (S_{\mathbb{Q}}^{\lambda^{'}})^{\perp}$. Entonces

$$dim(S_{\mathbb{Q}}^{\lambda}) = dim(\ Im\ \theta) = dim(M_{\mathbb{Q}}^{\lambda^{'}}/Ker\ \theta) \geq dim(M_{\mathbb{Q}}^{\lambda^{'}}/(S_{\mathbb{Q}}^{\lambda^{'}})^{\perp})) = dim(S_{\mathbb{Q}}^{\lambda^{'}}).$$

De manera análoga, se tiene que

$$dim(S_{\mathbb{Q}}^{\lambda^{'}}) \geq dim(S_{\mathbb{Q}}^{\lambda^{''}}) = dim(S_{\mathbb{Q}}^{\lambda}).$$

Por tanto, en (2.4) tenemos una igualdad; en particular resulta que $Ker\ \theta = (S_{\mathbb{Q}}^{\lambda^{'}})^{\perp}$ y esto implica que

$$M_{\mathbb{Q}}^{\lambda^{'}}/(S_{\mathbb{Q}}^{\lambda^{'}})^{\perp} \cong S_{\mathbb{Q}}^{\lambda} \otimes S_{\mathbb{Q}}^{(1^n)},$$

como se quería probar, siendo $M_{\mathbb{Q}}^{\lambda^{'}}/(S_{\mathbb{Q}}^{\lambda^{'}})^{\perp} \cong$ al dual de $S_{\mathbb{Q}}^{\lambda^{'}}$. □

2.5. Tabla de Caracteres

Para finalizar el capítulo daremos en esta sección una fórmula, debida a Frobenius, para calcular la tabla de caracteres de $\mathbb{S}_n$. En particular, se facilita el cálculo de la dimensión de estos módulos irreducibles.

Sin embargo, la mejor forma para calcular la tabla de caracteres de $\mathbb{S}_n$ para n chico, es deducir los caracteres que no se conocen de los triviales a través de las relaciones de ortogonalidad.

Por tanto, primero expondremos aquellos caracteres cuyo cálculo resulta trivial, debido a los teoremas anteriores, y luego mostraremos un ejemplo de cómo hallar los restantes cuando n es chico. Posteriormente daremos la fórmula de Frobenius para el cálculo de la tabla de caracteres y una fórmula para calcular la dimensión de los módulos de Specht.

Para que la notación no sea tan engorrosa, a partir de este momento los caracteres de los módulos de Specht $S_{\mathbb{Q}}^{\mu}$, correspondientes a una partición μ de n, se escribirán como

$$\chi_{S_{\mathbb{Q}}^{\mu}} \ = \ \chi^{\mu}.$$

Lema 2.6 *El valor del carácter $\chi^{(n-1,\ 1)}$ correspondiente a la representación irreducible $S_{\mathbb{Q}}^{(n-1,\ 1)}$ sobre una permutación $\sigma \in \mathbb{S}_n$ es uno menos a la cantidad de elementos que deja fijo σ.*

Demostración:
Es claro que la cantidad de elementos que deja fijo σ es exactamente la traza del endomorfismo que define sobre $M_{\mathbb{Q}}^{(n-1,\ 1)}$ (recordar que este espacio es el generado por $\overline{1}, \ldots \overline{n}$).

Por otro lado, sabemos que el carácter $\chi^{(n)}$ es el carácter de la representación trivial y vale 1 para toda permutación $\sigma \in \mathbb{S}_n$. Como $M_{\mathbb{Q}}^{(n-1,\ 1)} = S^{(n)} \oplus S_{\mathbb{Q}}^{(n-1,\ 1)}$, el resultado es inmediato. □

Ejemplo: Consideremos el grupo de permutaciones de 4 elementos y hallemos la tabla de caracteres del mismo.

Las clases de conjugación de $\mathbb{S}_4$ son 5 y cada una corresponde a una partición de 4. Las notaremos como las clases de equivalencia de un elemento, es decir $[1\ 2\ 3\ 4]$, $[1\ 2\ 3]$, $[(1\ 2)(3\ 4)]$, $[1\ 2]$, $[id]$, que corresponden a las particiones (4), $(3,\ 1)$, $(2,\ 2)$, $(2,\ 1^2)$ y (1^4) respectivamente.

Por el lema anterior, sabemos que $M_{\mathbb{Q}}^{(3,\ 1)} = S^{(4)} \oplus S_{\mathbb{Q}}^{(3,\ 1)}$. Luego, el carácter $\chi^{(3,\ 1)}$ se deduce de la igualdad

$$\chi_{M_{\mathbb{Q}}^{(3,\ 1)}} = \chi^{(4)} + \chi^{(3,\ 1)},$$

y toma los valores $-1,\ 0,\ -1,\ 1,\ 3$ sobre las clases de conjugación de $\mathbb{S}_4$ dadas en orden decreciente, respectivamente. En particular, la dimensión de $S_{\mathbb{Q}}^{(3,\ 1)}$ es 3. Como los caracteres de $S_{\mathbb{Q}}^{(4)}$, $S_{\mathbb{Q}}^{(1^4)}$ y $S_{\mathbb{Q}}^{(3,\ 1)}$ son conocidos, debemos encontrar los caracteres de las representaciones que faltan, a saber $S_{\mathbb{Q}}^{(2,\ 2)}$ y $S_{\mathbb{Q}}^{(2,\ 1^2)}$. Es claro que la partición conjugada de $S_{\mathbb{Q}}^{(3,\ 1)}$ es $S_{\mathbb{Q}}^{(2,\ 1^2)}$, entonces

$$S_{\mathbb{Q}}^{(2,\ 1^2)} \cong S_{\mathbb{Q}}^{(1^4)} \otimes S_{\mathbb{Q}}^{(3,\ 1)},$$

y su carácter viene dado por

$$\chi^{(2,\ 1^2)} = \chi^{(1^4)} \cdot \chi^{(3,\ 1)}.$$

Por tanto, sólo falta encontrar el carácter de la representación $S_{\mathbb{Q}}^{(2,\ 2)}$, pero éste se deduce fácilmente de las relaciones de ortogonalidad. En conclusión, la tabla de caracteres de $\mathbb{S}_4$ sobre $\mathbb{Q}$ es la siguiente:

	6	8	3	6	1
$\mathbb{S}_4$	$[1\ 2\ 3\ 4]$	$[1\ 2\ 3]$	$[(1\ 2)(3\ 4)]$	$[1\ 2]$	$[id]$
$S^{(4)}$	1	1	1	1	1
$S^{(3,\ 1)}$	-1	0	-1	1	3
$S^{(2,\ 2)}$	0	-1	2	0	2
$S^{(2,\ 1^2)}$	1	0	-1	-1	3
$S^{(1^4)}$	-1	1	1	-1	1

.

Expondremos a continuación la fórmula de Frobenius para el cálculo del carácter del módulo de Specht S^λ, siendo λ una partición de n; su demostración se puede encontrar en [F-H].

Denotemos por C_i las clases de conjugación en $\mathbb{S}_n$ donde i está determinada por la sucesión

$$i = (i_1,\ i_2, \ldots,\ i_n) \quad \text{tal que} \quad n = \sum \alpha i_\alpha.$$

Es decir, C_i consiste en aquellas permutaciones que tienen i_1 ciclos de longitud 1, i_2 ciclos de longitud 2, $\ldots$, e i_n ciclos de longitud n.

Definición 32 *Sean $x_1, \dots, x_k$ variables independientes tal que k es mayor o igual a la cantidad de filas en el diagrama de Young de λ. Definimos la suma de potencias $P_j(x), 1 \leq j \leq n$ y el discriminante $\Delta(x)$ por*

$$P_j(x) = x_1^j + x_2^j + \cdots + x_k^j,$$

$$\Delta(x) = \prod_{i<j}(x_i - x_j).$$

Definición 33 *Sean $f(x) = f(x_1, \cdots, x_k)$ una serie formal de potencias y $(l_1,\ l_2, \dots,\ l_k)$ una k- tupla de enteros no negativos. Definimos entonces*

$$[f(x)]_{(l_1,\ l_2,\dots,\ l_k)} = \text{ coeficiente de } x_1^{l_1} \cdot x_2^{l_2} \cdots x_n^{l_k} \text{ en } f.$$

Dada una partición λ de n tal que $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k \geq 0$, consideremos la siguiente sucesión estrictamente decreciente de k enteros no negativos

$$l_1 = \lambda_1 + k - 1, \qquad l_2 = \lambda_2 + k - 2, \dots l_k = \lambda_k.$$

Luego, el carácter de S^λ viene dado por la siguiente

Fórmula de Frobenius

$$\chi^\lambda(C_i) = [\Delta(x) \cdot \prod_j P_j(x)^{i_j}]_{(l_1,\ l_2,\dots,\ l_k)}.$$

Por ejemplo, si $n = 5, \lambda = (3,\ 2)$, y C_i es la clase de conjugación de $(1\ 2)(3\ 4\ 5)$, es decir $i_1 = 0, i_2 = 1, i_3 = 1$, entonces

$$\chi^{(3,\ 2)}(C_i) = [(x_1 - x_2)(x_1^2 + x_2^2)(x_1^3 + x_2^3)]_{(4,\ 2)}.$$

Se puede ver fácilmente que los coeficientes dados en las tablas de caracteres de $\mathbb{S}_3$ y $\mathbb{S}_4$ verifican esta fórmula. Por ejemplo, sabemos que

$$\chi^{(2,\ 2)}((1\ 2\ 3)) = -1,$$

veamos que se verifica la fórmula:

Tenemos entonces que $C_i = [1\ 2\ 3],\ i_1 = 1,\ i_2 = 0$ e $i_3 = 1$. Como $\lambda = (2,\ 2)$, tomamos $k = 2$ y según la fórmula de Frobenius se tiene que

$$\begin{aligned}
\chi^{(2,\ 2)} &= [(x_1 - x_2)(x_1 + x_2)(x_1^3 + x_2^3)]_{(3,\ 2)} \\
&= [(x_1^2 - x_2^2)(x_1^3 + x_2^3)]_{(3,\ 2)} \\
&= [x_1^5 - x_1^3x_2^2 + x_1^2x_2^3 - x_2^5]_{(3,\ 2)} \\
&= -1.
\end{aligned}$$

Usemos la fórmula de Frobenius para calcular la dimensión del módulo de Specht S^λ. Sabemos que ésta viene dada por $\chi^\lambda(C_i)$, siendo C_i la clase de conjugación de la identidad que corresponde a $i = (n)$. Luego,

$$dim(S^\lambda) = \chi^\lambda(C_{(n)}) = [\Delta(x)(x_1 + x_2 + \cdots + x_k)^n]_{(l_1,\ l_2,\dots,\ l_k)}.$$

Ahora bien, es claro que $\Delta(x)$ es el determinante de la matriz de *Vandermonde*:

$$\begin{vmatrix} 1 & x_k & \dots & x_k^{k-1} \\ \vdots & \vdots & & \vdots \\ 1 & x_1 & \dots & x_1^{k-1} \end{vmatrix} = \sum_{\sigma \in \mathbb{S}_n} sg(\sigma) x_k^{\sigma(1)-1} \cdots x_k^{\sigma(k)-1},$$

y que el otro término se puede escribir de la siguiente manera:

$$(x_1 + x_2 + \cdots + x_k)^n \quad = \sum \tfrac{n!}{r_1! \cdot \ldots r_k!} x_1^{r_1} \cdot x_2^{r_2} \cdots x_k^{r_k},$$

donde la suma se realiza sobre todas las k-tuplas $(r_1,\ r_2, \ldots,\ r_k)$ que suman n. Para obtener el coeficiente correspondiente a $x_1^{l_1} \cdot x_2^{l_2} \cdots x_k^{l_k}$ redistribuimos los terminos en ambas sumas y obtenemos que dicho coeficiente es

$$\sum sg(\sigma) \tfrac{n!}{(l_1 - \sigma(k)+1)! \cdot \ldots (l_k - \sigma(1)+1)!},$$

donde la suma se realiza sobre $\sigma \in \mathbb{S}_k$ tal que

$$l_{k-i+1} - \sigma(i) + 1 \geq 0, \quad \forall\ 1 \leq i \leq k.$$

En particular, esta suma se puede escribir como

$$\tfrac{n!}{l_1! \cdots l_k!} \sum_{\sigma \in \mathbb{S}_k} sg(\sigma) \prod_{j=1}^{k} l_j(l_j - 1) \cdots (l_j - \sigma(k-j+1) + 2),$$

y ésto, por definición de determinante, es igual a

$$\frac{n!}{l_1! \cdots l_k!} \begin{vmatrix} 1 & l_k & l_k(l_k-1) & \cdots \\ \vdots & \vdots & \vdots & \vdots \\ 1 & l_1 & l_1(l_1-1) & \cdots \end{vmatrix}.$$

Operando sobre las columnas, el determinante anterior se reduce a un determinante de Vandermonde, por tanto se obtiene la siguiente fórmula para la dimensión de los módulos de Specht S^λ

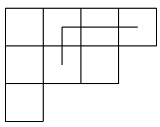
$$dim(S^\lambda) = \tfrac{n!}{l_1! \cdots l_k!} \prod_{i<j} (l_i - l_j),$$

recordando que $l_i = \lambda_i + k - i$.

Existe otra forma de expresar la dimensión de S^λ. Dicha forma está directamente ligada al diagrama $[\lambda]$.

Definición 34 *Un* **gancho** *en $(i,\ j)$ sobre el diagrama de $[\lambda]$ consiste en el nodo $(i,\ j)$ junto con los $\lambda_i - j$ nodos a la derecha de él y los $\lambda_j^{'} - i$ nodos debajo de él, los cuales se denominan el* **brazo** *y la* **pierna** *del gancho, respectivamente.*

Aquí mostramos un gancho en el nodo $(1,\ 2)$ sobre el diagrama $[4,\ 3,\ 1]$ de una partición de 8:



La **longitud** de un gancho en un nodo $(i,\ j)$, correspondiente a un diagrama de Young $[\lambda]$, es el número de nodos involucrados en el gancho. Claramente este número viene dado por

$$h_{ij} = \lambda_i + \lambda_j^{'} + 1 - i - j.$$

Si reemplazamos el nodo $(i,\ j)$ de $[\lambda]$ por la longitud h_{ij} del gancho que determina, obtenemos un grafo semejante a un tablero. En el caso anterior, dicho grafo sería:

6	4	3	1
4	2	1	
1			

Con esta nueva definición, la dimensión de los módulos de Specht se puede expresar de la siguiente manera:

$$dim(S^\lambda) = \frac{n!}{\prod_{i,j} h_{ij}},$$

donde el producto se hace sobre todos los ganchos posibles en el diagrama de $[\lambda]$.

Demostración:
Mostraremos a través de un razonamiento inductivo que el resultado es cierto cuando λ tiene sólo tres coeficientes no nulos; es decir, $\lambda = (\lambda_1,\ \lambda_2,\ \lambda_3)$ tal que $\lambda_i \neq 0\ \forall\ i$. Claramente la demostración funciona para el caso general, pero una prueba completa de este resultado resultaría demasiado engorrosa y ocultaría la simplicidad de las ideas que ella involucra.

Hasta aquí, la fórmula de la dimensión de los módulos Specht involucra a $l_i = \lambda_i + k - i$ y no se hace mención de la longitud de los ganchos. Sin embargo, es claro que la longitud de los ganchos correspondientes a la primera columna coinciden con los números l_i, esto es

$$h_{i1} = \lambda_i + \lambda_1^{'} - i - 1 + 1 = \lambda_i + k - i = l_i.$$

En particular, tenemos la siguiente igualdad:

$$\frac{dim(S^\lambda)}{n!} = \frac{\prod_{i<j}(h_{i1} - h_{j1})}{h_{11}! \cdots h_{k1}!}.$$

Entonces, recordando el determinante de Vandermonde tenemos que

$$\begin{aligned} \frac{dim(S^\lambda)}{n!} &= \frac{1}{h_{11}!}\frac{1}{h_{21}!}\frac{1}{h_{31}!} \cdot \begin{vmatrix} h_{11}(h_{11}-1) & h_{11} & 1 \\ h_{21}(h_{21}-1) & h_{21} & 1 \\ h_{31}(h_{31}-1 & h_{31} & 1 \end{vmatrix} \\ &= \begin{vmatrix} \frac{1}{(h_{11}-2)!} & \frac{1}{(h_{11}-1)!} & \frac{1}{h_{11}!} \\ \frac{1}{(h_{21}-2)!} & \frac{1}{(h_{21}-1)!} & \frac{1}{h_{21}!} \\ \frac{1}{(h_{31}-2)!} & \frac{1}{(h_{31}-1)!} & \frac{1}{h_{31}!} \end{vmatrix}. \end{aligned}$$

Utilizando algunas propiedades de determinantes obtenemos

$$\frac{dim(S^\lambda)}{n!} = \frac{1}{h_{11}h_{21}h_{31}} \cdot \begin{vmatrix} \frac{1}{(h_{11}-3)!} & \frac{1}{(h_{11}-2)!} & \frac{1}{(h_{11}-1)!} \\ \frac{1}{(h_{21}-3)!} & \frac{1}{(h_{21}-2)!} & \frac{1}{(h_{21}-1)!} \\ \frac{1}{(h_{31}-3)!} & \frac{1}{(h_{31}-2)!} & \frac{1}{(h_{31}-1)!} \end{vmatrix}.$$

Aplicando la hipótesis inductiva al diagrama $[\lambda^*] = [\lambda_1 - 1,\ \lambda_2 - 1,\ \lambda_3 - 1]$ que se obtiene del diagrama $[\lambda]$ quitándole la primera columna, tenemos que

$$\begin{aligned} \frac{dim(S^\lambda)}{n!} &= \frac{1}{h_{11}h_{21}h_{31}} \cdot \frac{1}{\prod \text{longitud de los ganchos en } [\lambda^*]} \\ &= \frac{1}{\prod_{i,j} h_{ij}}, \end{aligned}$$

como se quería probar. $\square$

Capítulo 3

Introducción a las representaciones modulares

Este capítulo contiene una introducción a la teoría de Brauer de representaciones modulares. Sea G un grupo finito y p un número primo que divide al orden de G. La estructura $p-local$ de G es la familia de p-subgrupos de G, juntos con sus normalizadores. Las estructuras p-locales de G, para varios primos p, determinan la estructura de G y juegan un papel preponderante en el problema de clasificación de los grupos finitos simples.

El objetivo principal de la teoría de Brauer ha sido relacionar la teoría de caracteres G sobre el cuerpo de los números complejos con las estructuras p-locales de G para primos que dividen al orden de G. Comienza con un trabajo de Brauer en representaciones de un grupo finito G sobre un cuerpo modular k de característica p. En su forma actual, es el estudio de la teoría de representaciones de G sobre tres anillos R, K y k, y las relaciones que hay entre ellos. Aquí, el anillo k es un cuerpo de característica p y el anillo K es un cuerpo, generalmente de característica cero. Sin embargo, no haremos suposición alguna sobre la característica de K, salvo que se mencione lo contrario. La situación más importante es aquella en la que el cuerpo K es un cuerpo de descomposición de G (cuya definición se verá más adelante). Podremos entonces relacionar los KG-módulos y sus caracteres con los kG-módulos y la estructura p-local de G.

Por otro lado, como los kG-módulos pueden no ser semisimples, la maquinaria de anillos y módulos semisimples no se puede aplicar directamente al estudio de los kG-módulos. Por tanto, se usará la teoría de anillos artinianos con radical y los resultados se darán en términos de Grupos de Grothendieck y de caracteres de Brauer.

Comenzaremos con algunas definiciones y terminología que usaremos a través de todo el capítulo. De aquí en adelante, todos los módulos se supondrán finitamente generados, salvo que se especifique lo contrario.

3.1. Definiciones

Definición 35 *Sea $\mathbb{R}^+$ el conjunto de los número reales positivos. Una* **valuación** *sobre un cuerpo K es una aplicación $\varphi : K \to \mathbb{R}^+$ tal que para todo $a,\ b\ \in K$ se tiene que*

$$\begin{cases} \varphi(a) = 0 \quad \textit{si solo si } a = 0 \\ \varphi(ab) = \varphi(a)\varphi(b) \\ \varphi(a+b) \leq \varphi(a) + \varphi(b) \end{cases}$$

Una valuación *no-arquimedeana* es aquella que satisface

$$\varphi(a+b) \leq max(\varphi(a),\ \varphi(b)).$$

Una valuación se dice *discreta* si su grupo de valores $\{\varphi(a) : a \in K,\ a \neq 0\}$ es un grupo cíclico e infinito. Se puede ver que una valuación discreta es también no-arquimedeana.

Cada valuación induce una métrica sobre K tomando los entornos para cada $a \in K$ como las esferas abiertas de radio $\epsilon \in \mathbb{R}^+$,

$$\{x\ \in K : \varphi(x-a) < \epsilon\}.$$

Los axiomas de métrica se deducen trivialmente de la definición de valuación y del hecho de que $\varphi(1) = \varphi(-1) = 1$ para toda valuación. Dos valuaciones se dicen equivalentes si definen la misma topología sobre K.

Dada una valuación no-arquimedeana sobre K definimos los siguientes subconjuntos de K:

$$R = \{a\ \in K : \varphi(a) \leq 1\}, \quad \wp = \{a\ \in K : \varphi(a) < 1\}.$$

Luego, R resulta un anillo, que se denomina **anillo de valuación** de φ y $\wp$ es el único ideal maximal de R; en particular, R resulta ser un anillo local. Se verifica fácilmente que R es un anillo y que $\wp$ es un ideal, veamos entonces que éste ideal es maximal y que es el único:

Supongamos que J es un ideal no nulo de R tal que $\wp \subset J \subset R$. Luego, existe un elemento $x \in J$ tal que $\varphi(x) = 1$. Como $1 = \varphi(1) = \varphi(x \cdot x^{-1}) = \varphi(x)\varphi(x^{-1})$, tenemos que $x^{-1} \in R$ y al ser J un ideal de R, debe ser que $x^{-1} \cdot x \in J$; lo cual implica que $J = R$. Por tanto, $\wp$ es un ideal maximal.

Si Q es otro ideal maximal de R distinto de $\wp$, entonces existe un elemento b de Q tal que $\varphi(b) = 1$. Siguiendo el razonamiento anterior se deduce que $Q = R$. Si para todo elemento b de Q se tiene $\varphi(b) < 1$, entonces $Q \subset \wp$, lo cual es una contradicción. Luego, $\wp$ es el único ideal maximal de R. $\square$

Más aún, si φ es una valuación discreta, entonces $\wp = R\pi$ es un ideal principal, generado por cualquier elemento $\pi\ \in \wp$ tal que $\varphi(\pi)$ genera el grupo de valores de φ. En este caso, el anillo R se denomina un **anillo de valuación discreto**, cuyo nombre abreviaremos por **d.v.r**. Análogamente, se tiene que todo ideal no nulo de R es de la forma $\pi^k R$, para algún $k \geq 0$; en particular, resulta que el anillo de valuación discreto es un dominio principal.

Por ser $\wp$ un ideal maximal de R, el cociente $R/\wp$ es un cuerpo que se denomina el **cuerpo de residuos** de φ.

Un ejemplo de valuación es el siguiente:

Sea $\mathbb{Q}$ el cuerpo de los números racionales y sea p un número entero primo. Para cada $a \in \mathbb{Q}$ sea $\nu_p(a)$ el número que resulta de restar el exponente de p que aparece en la factorización del numerador por el exponente de p que aparece en la factorización del denominador; por ejemplo $\nu_p(p) = 1$ y $\nu_p(\frac{1}{p}) = -1$. Tomemos $\nu_p(0) = +\infty$ y sea κ un número real mayor a 1. Definimos entonces

$$\varphi_p(a) = \kappa^{-\nu_p(a)}, \quad \forall\ a\ \in \mathbb{Q}.$$

Esta valuación φ_p es una valuación discreta no-aquimedeana sobre $\mathbb{Q}$ que se denomina la valuación p-ádica de $\mathbb{Q}$. Observar que cambiar el valor de κ no cambia la clase de equivalencia de la valuación.

El anillo de valuación de φ_p es precisamente

$$\begin{aligned} R_p &= \{a \in \mathbb{Q} : \varphi_p(a) \leq 1\} \\ &= \{a \in \mathbb{Q} : \nu_p(a) \geq 0\} \\ &= \{\tfrac{x}{s} \in K : x \in \mathbb{Z},\ s \in \mathbb{Z} - p \cdot \mathbb{Z}\}. \end{aligned}$$

Esto es, la localización de $\mathbb{Z}$ en p. Análogamente, su ideal maximal será

$$\begin{aligned} \wp &= \{a \in \mathbb{Q} : \varphi_p(a) < 1\} \\ &= \{a \in \mathbb{Q} : \nu_p(a) > 0\} \\ &= \{\tfrac{x}{s} \in K : x \in p \cdot \mathbb{Z},\ s \in \mathbb{Z} - p \cdot \mathbb{Z}\}. \end{aligned}$$

Por tanto, el cuerpo de residuos $R_p/\wp$ resulta isomorfo al cociente $\mathbb{Z}/p \cdot \mathbb{Z}$, esto es

$$R_p/\wp \cong \mathbb{Z}_p.$$

Hemos visto que una valuación sobre un cuerpo le da a éste una estructura de espacio métrico. Podemos entonces completar dicho espacio métrico para que resulte completo. Este proceso se realiza de la manera usual; es decir, se toman los elementos de $\hat{K}$ la completación de K como las clases de equivalencia de las sucesiones de Cauchy de K. Luego, $\hat{K}$ resulta un cuerpo, que se denomina *la completación φ-ádica* de K. La valuación φ se extiende únicamente a una valuación $\hat{\varphi}$ de $\hat{K}$, y $\hat{K}$ resulta completo con respecto a la métrica definida por $\hat{\varphi}$. Si φ es una valuación no-arquimedeana, entonces $\hat{\varphi}$ también es no-arquimedeana y el grupo de valores es el mismo. Por tanto, si φ es una valuación discreta, también lo es $\hat{\varphi}$. Su anillo de valuación y su ideal maximal son los siguientes:

$$\hat{R} = \{a \in K : \hat{\varphi}(a) \leq 1\}, \quad \hat{\wp} = \{a \in K : \widehat{\varphi(a)} < 1\}.$$

Se puede demostrar que hay un isomorfismo de cuerpos $R/\wp \cong \hat{R}/\hat{wp}$. Más aún, se tiene que

$$\hat{\wp} = \wp \cdot \hat{R}, \quad \wp = \hat{\wp} \cap R.$$

Recordaremos ahora la definición de módulos proyectivos y sus equivalencias que necesitaremos a lo largo de todo el capítulo.

Definición 36 *Sea A un anillo. Un A-módulo se dice* **proyectivo** *si es un sumando directo de un A-módulo libre.*

Definición 37 *Sea A un anillo arbitrario, y sea $\mathcal{C}$ una categoría de A-módulos a izquierda. Una sucesión exacta corta (s.e.s.) es una sucesión de A-módulos tal que*

$$0 \longrightarrow L \xrightarrow{\psi} M \xrightarrow{\theta} N \longrightarrow 0, \tag{1}$$

donde $Ker\ \theta = Im\ \psi$, θ es un epimorfismo y es ψ un monomorfismo.

Proposición 3.1 *Sea P un A-módulo. Las siguientes condiciones son equivalentes:*

i) P es proyectivo.

ii) Toda sucesión exacta $0 \to X \to Y \to P \to 0$ de A-módulos se parte. Es decir, $Y \cong X \oplus P$.

iii) Para cada diagrama con la última fila exacta

$$\begin{tikzcd} & P \arrow[dl, dashed, "h"'] \arrow[d, "f"] & \\ X \arrow[r, "g"'] & Y \arrow[r] & 0 \end{tikzcd}$$

existe un morfismo de A-módulos h tal que $f = gh$.

iv) Para cada morfismo suryectivo $g : X \to Y$, la aplicación inducida

$$g_* : Hom_A(P, X) \to Hom_A(P, Y),$$

es también suryectiva.

v) El funtor $Hom_A(P, -)$ es exacto.

Definición 38 *Sea A un anillo. La torsión de un A-módulo M está definido por*

$$t(M) = \{m \ \in M : r \cdot m = 0, \ \textit{para algún } r \in A, \ r \neq 0\}.$$

Supongamos que A es un dominio íntegro y sea K el cuerpo de cocientes de A. Es claro que $t(M)$ es el núcleo del morfismo natural

$$M \xrightarrow{\psi} K \otimes_A M\,.$$

Decimos que M es **libre de torsión** si $t(M) = 0$. En este caso, ψ es inyectivo y M está inmerso en $K \otimes_A M$. De aquí en adelante, si M es libre de torsión, identificaremos a M con su imagen por ψ, $1 \otimes_A M$ en $K \otimes_A M$. Además,

$$K \otimes_A M = K(1 \otimes_A M) = KM,$$

siendo KM el conjunto de combinaciones lineales sobre K de elementos de M. Es claro que para todo elemento $v \ \in KM$, existe $r \ \in A$ no nulo tal que $r \cdot v \ \in M$.

Definición 39 *Sea R un anillo conmutativo arbitrario. Un* **R-retículo** *es un R-módulo proyectivo finitamente generado.*

Si G es un grupo finito, un RG-retículo es un RG-módulo tal que el R-módulo subyacente es un R-retículo.

Supongamos que R es un anillo de valuación discreto; luego, es un dominio principal. Por tanto, todo R-módulo proyectivo finitamente generado es un R-módulo libre con base finita. En particular, los RG-retículos son RG-módulos libres con una base finita sobre R. Dado un RG-retículo M, podemos formar el KG-módulo $KM = K \otimes_R M$, y el kG-módulo $\overline{M} = M/\wp \cdot M$, cuya construcción se verá en detalle más adelante. En este capítulo, estudiaremos la conexión entre M, KM y kM a través del mapa de descomposición y el triángulo de Brauer-Cartan.

Definición 40 *Sea p un número primo. Un* **sistema p-modular** *(K, R, k) consiste de un anillo de valuación discreta R con cuerpo de cocientes K, ideal maximal $\wp = \pi R$, y cuerpo residual $k = R/\wp$ de característica p.*

Recordemos que el anillo R es un anillo local, que $\wp$ es su único ideal maximal y $\wp = R\cdot\pi$, siendo π cualquier elemento de $\wp$ que genere el grupo de valores de la valuación. Los sistemas modulares se pueden encontrar en un cuerpo K de números algebraicos, tomando una valuación φ no-arquimedeana p-ádica sobre K, R como el anillo de valuación de φ y k como el cuerpo de residuos $R/\wp$. En el ejemplo anterior vimos que el cuerpo residual tenía característica p y era isomorfo a $\mathbb{Z}_p$. En ese caso, el sistema p-modular sería $(\mathbb{Q},\ R_p,\ \mathbb{Z}_p)$, siendo R_p la localización de $\mathbb{Z}$ en p. También se puede tomar K como la completación p-ádica de un cuerpo algebraico de números; de esta forma, el anillo de valuación R resulta completo con la topología p-ádica. Sea $\bar{a}$ la imagen de un elemento $a\ \in R$ por la aplicación natural $R \to R/\wp = k$. Sea M un RG-retículo en un KG-módulo V. Entonces $\overline{M} = M/\wp \cdot M$ es un RG-módulo que es anulado por $\wp$, por tanto, puede adquirir una estructura de kG-módulo, donde la acción de kG está dada por

$$(\sum_{x\in G} \bar{a}_x x)\cdot \bar{m} = \sum_{x\in G} \overline{a_x x \cdot m}, \quad a_x \in R,\ m \in M,$$

siendo $\bar{m}$ la imagen en $\overline{M}$ del elemento $m \in M$ por la aplicación natural.

Denotamos por $\overline{M}$ al kG-módulo que se obtiene de M por reducción módulo $\wp$.

Definición 41 *Un elemento $x\ \in G$ se dice* **p-regular** *si su orden es un número coprimo con p. Diremos que $x\ \in G$ es un* **p-elemento** *si el orden de x es una potencia de p.*

La identidad 1_G de G es el único elemento que es p-regular y es un p-elemento. Se puede ver que todo elemento $x\ \in G$ se escribe de manera única como $x = s\cdot u$, siendo s un elemento p-regular, u un p -elemento y $s\cdot u = u\cdot s$. Esto se deduce fácilmente debido a que u y s resultan ser potencias de x. Diremos entonces que s es la parte p-regular de x, y que u es la p-parte de x. De esta forma, definimos

$$G_{p'} = \{\text{elementos } p\text{-regulares de } G\}.$$

3.2. Grupos de Grothendieck

Sean A un anillo arbitrario y $\mathcal{C}$ una subcategoría plena de la categoría de A-módulos a izquierda. Consideremos la siguiente sucesión exacta corta de A-módulos:

$$0 \longrightarrow L \xrightarrow{\psi} M \xrightarrow{\theta} N \longrightarrow 0. \tag{2}$$

Si cada módulo de la sucesión exacta anterior pertence a $\mathcal{C}$, decimos que (2) es una s.e.s. de $\mathcal{C}$. Supondremos siempre que $0\ \in \mathcal{C}$, y que si $M,\ N\ \in \mathcal{C}$ entonces $M \oplus N\ \in \mathcal{C}$. Asumiremos también que la colección de clases de isomorfismos de módulos en $\mathcal{C}$ forman un conjunto. Por ejemplo, $\mathcal{C}$ se puede elegir como una de estas tres categorías:

$_A\mathcal{M}$ = categoría de todos los A-módulos a izquierda,

$_A mod$ = categoría de todos los A-módulos a izquierda finitamente generados,

$\mathcal{P}(A)$ = categoría de todos los A-módulos proyectivos a izquierda finitamente generados.

Considerando invariantes de módulos, usualmente se busca construir una aplicación $h : \mathcal{C} \to T$, que asigna a cada módulo $M\ \in \mathcal{C}$ un elemento $h(M)$ en algún grupo abeliano fijo T. Se desea que el mapa sea aditivo en sucesiones exactas cortas de $\mathcal{C}$, esto es,

$$h(M) = h(L) + h(N),$$

para toda s.e.s. (1) en $\mathcal{C}$. Esto implica en particular que la imagen de cada módulo sólo depende de la clase de isomorfismo del mismo. Por ejemplo, sea $\mathcal{C}$ la categoría de todos los $\mathbb{C}G$-módulos a izquierda de dimensión finita, y para cada $M \in \mathcal{C}$, sea $h(M) = \chi_M$ el carácter de M. Luego, la aplicación h va de $\mathcal{C}$ al grupo aditivo $ch\ \mathbb{C}G$ de los caracteres virtuales de G, definido en (9). Por lo visto en el primer capítulo, sabemos que h es aditiva sobre s.e.s. en $\mathcal{C}$ ya que toda sucesión exacta se parte por ser el anillo $\mathbb{C}G$ un anillo semisimple.

Definición 42 *Sea $\mathcal{C}$ una categoría de A-módulos. Sea F el grupo abeliano libre generado por los símbolos (M), uno por cada clase de isomorfismo de módulos en $\mathcal{C}$. Sea F_0 el subgrupo de F generado por todas las expresiones*

$$(M) - (L) - (N),$$

provenientes de todas las s.e.s. (1) en $\mathcal{C}$. El **grupo de Grothendieck** $\mathcal{K}_0(\mathcal{C})$ *de la categoría $\mathcal{C}$ está definido como el grupo abeliano aditivo construido a través del cociente*

$$\mathcal{K}_0(\mathcal{C}) = F/F_0.$$

Para la construcción de un grupo abeliano libre se puede consultar [L].

Si $M \in \mathcal{C}$, escribiremos $[M]$ para denotar la imagen de M en $\mathcal{K}_0(\mathcal{C})$. De la definición del grupo de Grothendieck se deduce inmediatamente la siguiente

Proposición 3.2 *Sean T un grupo abeliano fijo y $h : \mathcal{C} \to T$ una aplicación que es aditiva sobre s.e.s. en $\mathcal{C}$. Entonces existe un único morfismo aditivo*

$$g : \mathcal{K}_0(\mathcal{C}) \to T,$$

que extiende h, y está dado por la fórmula

$$g([M]) = h(M), \quad \forall\ M \in \mathcal{C}.$$

Si la categoría en cuestión es la categoría ${}_Amod$ de los A-módulos a izquierda finitamente generados, su grupo de Grothendieck se notará

$$G_0(A) = \mathcal{K}_0({}_Amod).$$

Por otra parte, el **grupo de clases proyectivas** $\mathcal{K}_0(A)$ de un anillo A está definido por

$$\mathcal{K}_0(A) = \mathcal{K}_0(\mathcal{P}(A)).$$

Luego, $\mathcal{K}_0(A)$ está generado por las expresiones $[P]$, una para cada clase de isomorfismo (P) de A-módulos proyectivos finitamente generados, con relaciones

$$[P \oplus P'] = [P] + [P'], \quad \forall\ P,\ P' \in \mathcal{P}(A).$$

Notar que para este grupo, las relaciones se puede expresar de manera más simple debido a que toda s.e.s. en la categoría de A-módulos proyectivos f.g. se parte.

Dados un sistema modular $(K,\ R,\ k)$ y un grupo finito G, estudiaremos principalmente los grupos de Grothendieck $G_0(KG)$, $G_0(kG)$ y los grupos de clases proyectivas $\mathcal{K}_0(KG)$ y $\mathcal{K}_0(kG)$.

Más adelante mostraremos que si la característica de K es cero, entonces $G_0(KG) = ch\ (KG)$, el anillo de caracteres virtuales de los KG-módulos. Como un primer paso, tenemos la siguiente proposición:

Proposición 3.3 *Sean A un anillo artiniano y $\{V_1, \ldots, V_s\}$ un conjunto de representantes de clases de isomorfismo de A-módulos simples a izquierda. Entonces*

$$G_0(A) = \bigoplus_{i=1}^{s} \mathbb{Z}\ [V_i];$$

es decir, el grupo de Grothendieck $G_0(A)$ es un grupo abeliano libre con base $\{[V_1], \ldots, [V_s]\}$.

Demostración:
Cada A-módulo U finitamente generado tiene una cadena de composición

$$U = U_0 \supset U_1 \supset \cdots \supset U_{t+1} = 0,$$

y factores de composición (U_i/U_{i+1}), que son A-módulos simples por ser A artiniano. Como la sucesión

$$0 \longrightarrow U_{i+1} \longrightarrow U_i \longrightarrow (U_i/U_{i+1}) \longrightarrow 0,$$

es exacta para cada i, se sigue de la definición de $G_0(A)$ que

$$[U] = \sum_{i=0}^{t} [U_i/U_{i+1}], \quad \text{en } G_0(A).$$

Luego, como $\{V_1, \ldots, V_s\}$ es un conjunto base de A-módulos simples, tenemos que

$$[U] = \sum_{i=0}^{t} r_i(U)[V_i], \quad \text{en } G_0(A),$$

donde para cada i, $r_i(U)$ es la multiplicidad de V_i como factor de composición de U. Por el teorema de Jordan-Hölder, se tiene que $r_i(U)$ está bien definido y claramente r_i es aditivo en s.e.s. de A-módulos. Luego, por la propopsición anterior, tenemos que existe un morfismo aditivo

$$g : G_0(A) \to \mathbb{Z}^s,$$

definido por $g[U] = (r_1(U), \ldots,\ r_s(U))$; siendo claramente un morfismo suryectivo.

Por otra parte, existe un morfismo $f : \mathbb{Z}^s \to G_0(A)$, definido por

$$f(r_1, \ldots,\ r_s) = \sum_{i=0}^{t} r_i(U)[V_i], \quad r_i\ \in \mathbb{Z}.$$

Es claro que $gf = id$ y que $fg = id$; por tanto, f y g son isomorfismos, siendo uno inversa del otro. Luego, $[V_1], \ldots,\ [V_s]$ forma una base libre sobre $\mathbb{Z}$ de $G_0(A)$. $\square$

Daremos a continuación, sin demostración aunque los argumentos son muy similares a los utilizados en la demostración anterior, un teorema que describe la estructura aditiva de $\mathcal{K}_0(A)$ para el caso que A sea un **anillo semiperfecto**, es decir, un anillo que cumple las siguientes condiciones:

i) $A/rad\ A$ es un anillo artiniano semisimple.

ii) Todo idempotente en $A/rad\ A$ se puede levantar a un idempotente en A.

Los anillo semiperfectos que estudiaremos son RG y kG, donde $(K,\ R,\ k)$ es un sistema modular. Se puede probar que RG es un anillo semiperfecto siempre que R sea completo con la topología $\wp$-ádica; esto es, la topología que tiene como base de entornos abiertos de $a \in RG$ a los conjuntos

$$\{a + \wp^k : k = 0,\ 1,\ 2, \ldots\}.$$

En general, dado un anillo A y un ideal bilátero N contenido en $rad\ A$, se define la topología N-ádica, como la topología cuya base de entornos abiertos de $a \in A$ son los conjuntos

$$\{a + N^k : k = 0,\ 1,\ 2, \ldots\}.$$

Decimos que A es completo con la topología N-ádica si toda sucesión de Cauchy de A, converge (en la topología N-ádica) a un único elemento de A. Si R es un anillo de valuación discreto completo con la topología inducida por la valuacíon discreta φ, entonces R es completo con la topología $\wp$-ádica. Más aún, es fácil ver que la topología $\wp$-ádica es equivalente a la topología φ-ádica.

Por otro lado, kG es semiperfecto para cualquier cuerpo arbitrario k. (Ver [C-R] para las demostraciones de estos hechos y para la demostración de la proposición).

Proposición 3.4 *Sean A un anillo semiperfecto y $\{P_1, \ldots,\ P_r\}$ un conjunto de representantes de clases de isomorfismo de A-módulos a izquierda, proyectivos, indescomponibles y finitamente generados. Es decir, todo A-módulo a izquierda, finitamente generado, proyectivo e indescomponible es isomorfo a exactamente uno de los $\{P_i\}$. Entonces*

$$\mathcal{K}_0(A) = \bigoplus_{i=1}^{r} \mathbb{Z}\ [P_i].$$

Es decir, el grupo de clases proyectivas es un grupo abeliano libre con base $\{[P_1], \ldots,\ [P_r]\}$.

Sean K un cuerpo arbitrario y G un grupo finito. Mostraremos en lo que sigue que el grupo de Grothendieck $G_0(KG)$ se puede transformar en un anillo conmutativo, con la multiplicación correspondiendo al producto tensorial de KG-módulos. $M,\ N$ un par de KG-módulos finitamente generados, y $M \otimes_K N$ el producto tensorial usual, que también tiene una estructura de KG-módulo. Intentamos definir la multiplicación en $G_0(KG)$ a partir de la siguiente fórmula:

$$[M][N] = [M \otimes_K N],$$

y extenderla a todo el grupo por linealidad. Sin embargo, este proceso tiene una dificultad extra que es la de demostrar que la multiplicación está bien definida. Por tanto, lo haremos de la siguiente manera:Recordando la costrucción del grupo de Grothendieck, sabemos que $G_0(KG) = F/F_0$, donde F es un grupo abeliano libre generado por las clases de isomorfismos (M) de KG-módulos a izquierda finitamente generados. Por tanto, podemos definir sobre F la multiplicación sin ambigüedad, esto es

$$(M)(N) = (M \otimes_K N),$$

para cada par de KG-módulos $M,\ N$. Por tanto, F resulta un anillo conmutativo y asociativo con unidad. Para ver que esta multiplicación se puede llevar a cabo en $G_0(KG)$, basta ver que F_0 es un ideal de F. Consideremos una s.e.s. de KG-módulos como en (1), y sea X cualquier KG-módulo. Entonces, la sucesión de KG-módulos

$$0 \longrightarrow X \otimes_K L \longrightarrow X \otimes_K M \longrightarrow X \otimes_K N \longrightarrow 0,$$

es exacta. Por tanto, tenemos que

$$(X)((M) - (L) - (N)) = (X \otimes_K M) - (X \otimes_K L) - (X \otimes_K N) \text{ en } F.$$

Luego, F_0 es un ideal en F; lo que implica que la multiplicación pase al cociente y le de a $G_0(KG)$ una estructura de anillo conmutativo con unidad. Observar que luego de esta construcción, la fórmula (3.2) es válida.

Estableceremos ahora la relación entre el grupo de Grothendieck $G_0(KG)$ y el anillo de caracteres virtuales $ch\ KG$ definido en el capítulo 1.

Proposición 3.5 *Sean K un cuerpo de característica cero y G un grupo finito. Existe un isomorfismo de anillos*

$$G_0(KG) \cong ch\ KG,$$

dado por la aplicación que a cada KG-módulo M le asigna su carácter.

Demostración:
Sea $\psi : G_0(KG) \to ch\ KG$, definida por $\psi(M) = \chi_M$. Como los caracteres son aditivos sobre s.e.s. de KG-módulos, se tiene que la aplicación ψ está bien definida sobre $G_0(KG)$. Por definición, sabemos que $ch\ KG$ es $\mathbb{Z}$ libre sobre los caracteres irreducibles de G; y por la proposición 3.3 se tiene que $G_0(KG)$ es $\mathbb{Z}$ libre sobre los KG-módulos simples. Al ser K de característica cero, es claro que ψ es un isomorfismo de grupos aditivos. Más aún, si N es un KG-módulo de carácter χ_N, entonces por lo visto en el capítulo 1 sabemos que el carácter de $M \otimes_K N$ está dado por $\chi_M \cdot \chi_N$. Esto implica que el isomorfismo es de anillos, como se quería probar. □

Para un sistema modular (K, R, k) y un grupo finito G, esperamos que el grupo de Grothendieck $G_0(kG)$ sirva como objeto de estudio; ya que, al no ser kG un anillo semisimple, un kG-módulo nunca está unívocamente determinado por su carácter, es por eso que no se considera el anillo de caracteres virtuales $ch\ kG$.

3.3. El mapa de descomposición

A través de esta sección, (K, R, k) será un sistema modular y G un grupo finito. Obtendremos aquí las primeras conexiones entre los KG-módulos, los RG-modulos y los kG-módulos. Recordemos que los RG-retículos son RG-módulos que tiene una base finita sobre R. Como R es un dominio principal, los submódulos de RG-retículos son necesariamente subretículos.

Definición 43 *Sea V un KG-módulo a izquierda finitamente generado. Un* RG**-retículo completo** *M en V es un RG-retículo M contenido en V tal que $KM = V$.*

Observemos que para cada RG-retículo M en V tenemos que

$$K \otimes_R M \cong KM,$$

como KG-módulos. A saber, la suryección $K \otimes_R M \to KM$, es un morfismo sobre KG; y como M es un R-módulo libre de torsión, dicha suryección es un isomorfismo.

Mostraremos ahora que todo KG-módulo contiene un RG-retículo completo M. Luego, se considerará el kG-módulo $\overline{M} = M/\wp \cdot M$, que se obtiene a partir de M por reducción módulo $\wp$. Para un KG-módulo fijo V puede haber muchos RG-retículos completos M en V, más aún, los kG-módulos $\overline{M}$, que se obtienen por reducción módulo $\wp$, en general no resultan ser isomorfos. Sin embargo, veremos que si son iguales en el grupo de Grothendieck $G_0(kG)$. Esta observación es el punto de partida de la teoría de representaciones modulares.

Veamos ahora un lema, cuya demostración es trivial, que nos muestra dos condiciones sobre un RG-módulo de V para que sea un RG-retículo completo en V.

Lema 3.1 *Sea V un KG-módulo a izquierda finitamente generado. Un RG-submódulo M de V es un RG-retículo completo en V si y sólo si se cumplen las condiciones:*

i) M tiene una base finita sobre R,

ii) $KM = V$.

En particular, si M es un RG-retículo completo en V, entonces para cada base $\{m_1, \ldots, m_d\}$ sobre R de M, el conjunto $\{1 \otimes m_1, \ldots, 1 \otimes m_d\}$ es una base sobre K para el KG-módulo $K \otimes_R M$. Identificando M con $1 \otimes M$ tenemos el siguiente

Corolario 3.1 *Si M es un RG-retículo completo en V, entonces toda base de M sobre R, es también una base de V sobre K.*

Recordemos del primer capítulo que las equivalencias de representaciones de G sobre K de un KG-módulo provienen de cambios de bases sobre K. En consecuencia, tenemos el siguiente resultado:

Corolario 3.2 *Toda representación de G sobre K cuyo módulo admite un RG-retículo completo, es equivalente sobre K a una representación de G sobre R, esto es, una representación por matrices con coeficientes en R.*

Veamos ahora el problema de existencia de RG-retículos completos en KG-módulos.

Proposición 3.6 *Todo KG-módulo a izquierda finitamente generado V contiene RG-retículos completos.*

Demostración:
Sea $\{v_i\}$ una base sobre K de V. Luego, tenemos que $V = \sum_{i=1}^{d} K \cdot v_i$. Definimos entonces

$$M = \sum_{i=1}^{d} RG \cdot v_i.$$

Entonces, M es un RG-módulo finitamente generado sobre R y es libre de torsión, por tanto es un RG-retículo en V. Claramente, $KM = V$, es decir que M es un RG-retículo completo en V. $\square$

Hemos visto la construcción de un kG-módulo a partir de un RG-retículo a través de la reducción módulo $\wp$ en la sección anterior. Esta construcción puede ser reformulada de varias maneras, y aquí expondremos algunas de ellas que nos serán de utilidad para más adelante.

Por el corolario 3.2, sabemos que toda representación de G sobre K es equivalente a una representación de G sobre R. Sea $T : G \to GL_d(R)$ una representación matricial de G sobre R, dada por

$$T(x) = (a_{ij}(x)), \quad a_{ij}(x) \in R, \ x \in G.$$

Luego, definimos $\bar{T} : G \to GL_d(k)$ una representación matricial de G sobre k por

$$\bar{T}(x) = (\overline{a_{ij}(x)}), \quad x \in G.$$

Por tanto, si T es una representación lineal de G sobre R dada por un RG- retículo completo M en V, con respecto a una base $\{m_1, \ldots, m_d\}$ de M, entonces $\{\bar{m_1}, \ldots, \bar{m_d}\}$ es una base de $\overline{M}$ sobre k, y $\bar{T}$ es una representación matricial de G sobre k dada por $\overline{M}$ con respecto a la base $\{\bar{m_1}, \ldots, \bar{m_d}\}$.

Una segunda interpretación de $\overline{M}$ está dada por el isomorfismo

$$\overline{M} \cong k \otimes_R M.$$

Verifiquemos dicho isomorfismo. Consideremos la sucesión exacta corta

$$0 \longrightarrow \wp \longrightarrow R \longrightarrow k \longrightarrow 0,$$

y apliquemos $(-) \otimes_R M$ para obtener la sucesión

$$0 \longrightarrow \wp \otimes_R M \longrightarrow R \otimes_R M \longrightarrow k \otimes_R M \longrightarrow 0,$$

que es exacta pues M es libre. Identificando $R \otimes_R M$ con M, tenemos que la imagen de $\wp \otimes_R M$ se identifica con $\wp \cdot M$, y por tanto, $M/\wp \cdot M \cong k \otimes_R M$ como se quería probar. □

Veremos ahora una proposición que nos da una cierta unicidad de RG-retículos completos en el grupo de Grothendieck.

Proposición 3.7 *Sean M y N un par de RG-retículos completos en un KG-módulo V. Entonces $[\overline{M}] = [\bar{N}]$ en $G_0(kG)$, o equivalentemente, los kG-módulos $\overline{M}$ y $\overline{N}$ tienen los mismos factores de composición.*

Demostración:
(Idea) Por el Lema 3.1, la suma $M + N$ es un RG-retículo completo que contiene a M y a N. Por tanto, basta con demostrar la proposición para RG-retículos L y M tal que $L \subset M$. Como RG es un anillo noetheriano, tenemos que M es un RG-módulo noetheriano, luego se puede suponer que L es un submódulo maximal de M. Más aún, se puede demostrar, usando el lema de Nakayama, que $\wp \cdot M \subseteq L$. Por tanto, se tiene que

$$\wp \cdot L \subseteq \wp \cdot M \subseteq L \subseteq M.$$

Entonces, debemos demostrar que $\overline{L}$ y $\overline{M}$ tienen los mismos factores de composición. Pero como estos kG-módulos tienen los factores de composición de $L/\wp \cdot M$ en común, la demostración se termina demostrando que M/L y $\wp \cdot M/\wp \cdot L$ tienen los mismos factores de composición. Para ver la demostración completa ver [C-R]. □

Proposición 3.8 *Existe un morfismo de grupos abelianos*

$$d : G_0(KG) \to G_0(kG),$$

tal que para cada KG-módulo a izquierda finitamente generado V, la aplicación le asigna a $[V] \in G_0(KG)$, el elemento $[\overline{M}] \in G_0(kG)$, siendo M un RG-retículo completo en V.

Demostración:
Por la proposición anterior, la imagen $[\overline{M}]$ es independiente del RG-retículo que se elija en V, por tanto d está bien definida si es aditiva sobre s.e.s. Dada una s.e.s de KG-módulos

$$0 \longrightarrow V_1 \longrightarrow V_2 \xrightarrow{\psi} V_3 \longrightarrow 0,$$

sea M_2 un RG-retículo competo en V_2, y pongamos $M_3 = \psi(M_2)$. Luego, M_3 es un RG-retículo en V_3, y como ψ es un morfismo de KG-módulos, se tiene que

$$KM_3 = K\psi(M_2) = \psi(KM_2) = \psi(V_2) = V_3.$$

Es decir, M_3 es un RG-retículo completo en V_3. Supongamos que la aplicación $V_1 \to V_2$ es la inclusión y pongamos $M_1 = M_2 \cap V_1$. Claramente M_1 es un RG-retículo, y obtenemos entonces la s.e.s.

$$0 \longrightarrow M_1 \longrightarrow M_2 \xrightarrow{\psi} M_3 \longrightarrow 0. \tag{3}$$

Luego, $0 \longrightarrow KM_1 \longrightarrow KM_2 \longrightarrow KM_3 \longrightarrow 0$, es exacta; en particular, $KM_1 = V_1$, siendo M_1 un RG-retículo completo en V_1. Como M_3 es un R-módulo proyectivo, la sucesión (3) se parte. Por tanto, tensorizar por k sobre R mantiene la exactitud. Como $k \otimes_R M_i \cong \bar{M}_i$, tenemos entonces una s.e.s. de kG-módulos

$$0 \longrightarrow \bar{M}_1 \longrightarrow \bar{M}_2 \longrightarrow \bar{M}_3 \longrightarrow 0.$$

Por tanto, $[\bar{M}_2] = [\bar{M}_1] + [\bar{M}_3]$ en $G_0(kG)$, esto es

$$d[V_2] = d[V_1] + d[V_3].$$

Es decir que d es aditiva para s.e.s. como se quería probar. □

Como los anillos KG y kG son artinianos, se puede aplicar la proposición 3.3. Sea entonces $\{[Z_1], \dots, [Z_s]\}$ una $\mathbb{Z}$-base libre de $G_0(KG)$ de KG-módulos simples y sea $\{[F_1], \dots, [F_r]\}$ una $\mathbb{Z}$-base libre de $G_0(kG)$ de kG-módulos simples. Entonces

$$d[Z_i] = \sum_{j=0}^{r} d_{ij}[F_j], \quad 1 \leq \ i \leq,$$

siendo d_{ij} la multiplicidad de F_j como factor de composición del kG-módulo que se obtiene por reducción módulo $\wp$ de un RG-retículo completo en Z_i.

Definición 44 *El morfismo de grupos abelianos*

$$d : G_0(KG) \to G_0(kG),$$

se denomina el **mapa de descomposición** *o morfismo de descomposición asociado al sistema p-modular $(K,\ R,\ k)$ y el grupo finito G. La matriz $\mathbf{D} = (\mathbf{d_{ij}})$ definida en (3.3) se denomina la* **matriz de descomposición**.

3.3.1. Ejemplos

a) Supongamos que $G = \mathbb{S}_3,\ p = 2$, y que el sistema p-modular es $(\mathbb{Q}_2,\ R,\ k)$; siendo $\mathbb{Q}_2$ el cuerpo que resulta de completar $\mathbb{Q}$ con respecto a la topología 2-ádica, R el anillo de los enteros 2-ádicos correspondiente a la valuación 2-ádica sobre $\mathbb{Q}$, $\wp = 2 \cdot R$, y $k = R/2 \cdot R = \mathbb{Z}_2$. Por lo visto en los primeros capítulos, sabemos que hay tres representaciones irreducibles de $\mathbb{S}_3$ sobre $\mathbb{Q}$, las cuales son la estándar, la representación signo y la representación trivial, cada una asociada a una partición de 3. Como las representaciones sobre $\mathbb{Q}_2$ son las mismas que sobre $\mathbb{Q}$, la tabla de caracteres es la siguiente:

$\mathbb{Q}_2\mathbb{S}_3$	1	3	2
$\mathbb{S}_3$	id	$(1\ 2)$	$(1\ 2\ 3)$
la trivial $S^{(3)}$	1	1	1
la estándar $S^{(2,\ 1)}$	2	0	-1
signo $S^{(1,\ 1,\ 1)}$	1	-1	1

En el capítulo 2 vimos que estas representaciones se realizan sobre $\mathbb{Z}$; luego, reduciendo módulo 2 las tres representaciones irreducibles, obtenemos dos representaciones de $\mathbb{Z}_2\mathbb{S}_3$, una de dimensión 1 y otra de dimensión 2. La primera es la imagen de la representación trivial y de la representación signo, que claramente es la misma, y la segunda es la reducción de la estándar. A través de un simple cálculo, es fácil ver que dicha reducción resulta una representación irreducible de $\mathbb{S}_3$ sobre $\mathbb{Z}_2$. Si no lo fuera, debería tener un subrepresentación propia, que por cuestión de dimensiones, debe estar generada por un vector que sería autovector de todos los endomorfismos definidos por la representación. Pero, ningún vector de $S^{(2,\ 1)}$ genera un subespacio estable por la acción de $\mathbb{S}_3$ sobre $\mathbb{Z}_2$. Luego, su matriz de descomposición es

$$\mathbf{D} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Para el ejemplo *ii)* necesitamos una proposición, cuya demostración se puede encontrar en [C-R].

Proposición 3.9 *Sean D un p-subgrupo normal de G, y $(K,\ R,\ k)$ un sistema modular arbitrario. Entonces*

i) D actúa trivialmente sobre todos los kG-módulos simples V, y por tanto, los kG-módulos simples coinciden con los $k(G/D)$-módulos simples.

ii) La suryección natural $\tau : RG \to R(G/D)$ tiene la propiedad de que ker τ es nilpotente módulo $\wp \cdot G$, y por tanto ker $\tau \subset$ rad RG.

□

b) Sean $G = \mathbb{S}_4$, $p = 2$, y $(\mathbb{Q}_2,\ R,\ k)$ el sistema 2-modular definido en el ejemplo anterior. Sabemos que hay 5 representaciones irreducibles de $\mathbb{S}_4$ sobre $\mathbb{Q}$, de dimensiones 1, 3, 2, 3, 1. Ellas son $S^{(4)}$, $S^{(3,\ 1)}$, $S^{(2,\ 2)}$, $S^{(2,\ 1,\ 1)}$ y $S^{(1,\ 1,\ 1,\ 1)}$, respectivamente. La primera es la representación trivial, la segunda la representación estándar, la última la representación signo y la cuarta la representación que se obtiene tensorizando sobre $\mathbb{Q}$ la representación signo con la estándar.

Sea H el 2-subgrupo abeliano normal generado por producto de dos trasposiciones que conmutan, esto es

$$H = \{id,\ (1\ 2),\ (3\ 4),\ (1\ 2)(3\ 4)\}.$$

Luego, el orden de H es 4. Consideremos el cociente de $\mathbb{S}_4$ con este subgrupo normal, su orden será $|\mathbb{S}_4/H| = 6$. Claramente, el cociente no es un grupo abeliano, por tanto debe ser que $\mathbb{S}_4/H \cong \mathbb{S}_3$. Por la proposición anterior, el 2-subgrupo H actúa trivialmente sobre cada $\mathbb{Z}_2\mathbb{S}_4$-módulo simple y los $\mathbb{Z}_2\mathbb{S}_4$-módulos simples coinciden con los $\mathbb{Z}_2\mathbb{S}_3$-módulos simples. Por tanto, tenemos dos $\mathbb{Z}_2\mathbb{S}_4$-módulos simples $F_1,\ F_2$, ver el ejemplo *a)*.

Claramente, $S^{(4)}$ y $S^{(1,\ 1,\ 1,\ 1)}$ tienen la misma imagen, así también como los módulos $S^{(3,\ 1)}$ y $S^{(2,\ 1,\ 1)} \cong S^{(3,\ 1)} \otimes S^{(1,\ 1,\ 1,\ 1)}$. La representación de dimensión dos tiene la misma imagen que la representación estándar de $\mathbb{S}_3$, ya que es la única de dimensión 2 y resulta ser una representación irreducible sobre $\mathbb{Z}_2$, por los mismos argumentos expuestos en el ejemplo anterior. Por tanto, la matriz de descomposición es la siguiente:

$$\mathbf{D} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \\ 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

Recordemos que ordenamos la base de los $\mathbb{Q}\mathbb{S}_n$-módulos simples según el orden establecido en el capítulo 2. Cabe destacar que la reducción de los módulos simples $S^{(3,\ 1)}$ y $S^{(2,\ 1,\ 1)}$ dejó de ser simple para ser una combinación lineal de $\mathbb{Z}_2\mathbb{S}_4$-módulos simples.

3.3.2. Extensiones de cuerpos de base y grupos de Grothendieck

Durante el transcurso de esta sección seguiremos con la intención de no hacer tantas demostraciones para poder dar una idea general de la teoría. Las demostraciones de las proposiciones que aquí expondremos se pueden ver en [C-R].

Sean $(K,\ R,\ k)$ un sistema p-modular, donde la característica de K es cero, y sea $K^{'}$ una extensión finita de cuerpos de K. Se intenta encontrar un sistema p-modular $(K^{'},\ R^{'},\ k^{'})$ que extienda al sistema original. Esto siempre se puede lograr debido a la siguiente proposición:

Proposición 3.10 *Sea $(K,\ R,\ k)$ un sistema p-modular y denotemos por ν a la valuación sobre K cuyo anillo de valuación es R. Para cada cuerpo $K^{'}$ que es una extensión finita de K, la valuación ν se puede extender a una valuación discreta $\nu^{'}$ sobre $K^{'}$. Sean $R^{'}$ el anillo de valuación de $\nu^{'}$, $\wp^{'}$ el ideal maximal de $R^{'}$, y $k^{'} = R^{'}/\wp^{'}$ el cuerpo residual. Entonces*

$$R^{'} \cap K = R, \quad \wp^{'} \cap K = \wp,$$

y $k^{'}$ es una extensión finita del cuerpo k.

Demostración:
(Idea). Expondremos, sin demostración, algunos hechos relevantes para la prueba de esta proposición. El d.v.r. R es el anillo asociado a alguna valuación discreta ν sobre K, por tanto

$$R = \{a\ \in K : \nu(a) \geq 0\}, \quad \wp = \{a\ \in K : \nu(a) > 0\}.$$

Sea $\hat{K}$ la completación p-ádica de K, luego la valuación ν se extiende a una valuación discreta $\hat{\nu}$ sobre $\hat{K}$: Sea Ω alguna clausura algebraica de $\hat{K}$. Entonces $\hat{\nu}$ se extiende a una valuación ω sobre Ω, definida por

$$\omega(x) = \frac{1}{n}\ \hat{\nu}(Nx), \quad n = dim_{\hat{K}}\ \hat{K}(x), \quad x \in \Omega,$$

siendo Nx la norma de x que proviene de la extensión finita $\hat{K}(x)$ de $\hat{K}$. Ahora, sea Ω es un cuerpo algebraicamente cerrado que contiene a K. Sean $\theta_i : K^{'} \to \Omega,\ 1 \leq i \leq m$, las distintas inclusiones de $K^{'}$ en Ω. Entonces, la valuación discreta ν tiene exactamente m extensiones distintas $\nu_1,\ \nu_2, \ldots,\ \nu_m$ en $K^{'}$, dadas por la fórmula

$$\nu_i(a) = \omega(\theta_i a), \quad a \in K^{'},\ 1 \leq i \leq m.$$

Dejando i fijo, la valuación que se obtiene es una valuación discreta sobre $K^{'}$, con anillo de valuación $R^{'}$ e ideal maximal $\wp^{'}$, donde

$$R^{'} = \{a\ \in K^{'} : \nu_i(a) \geq 0\}, \quad \wp = \{a\ \in K^{'} : \nu_i(a) > 0\}.$$

La aplicación $R \to R' \to k'$, tiene núcleo $R \cap \wp'$. Esta intersección es justamente $\wp$, por tanto obtenemos una inyección natural de k en k'. $\square$

Por conveniencia, al sistema p-modular (K', R', k') lo llamaremos una extensión finita del sistema p-modular (K, R, k). Estudiaremos ahora el comportamiento de los grupos $G_0(KG)$, $\mathcal{K}_0(kG)$ y $G_0(kG)$ cuando se extiende el cuerpo de base.

Proposición 3.11 *Sea (K', R', k') una extensión finita del sistema p-modular (K, R, k). Entonces, existen morfismos aditivos*

$$G_0(KG) \to G_0(K'G), \quad \mathcal{K}_0(kG) \to \mathcal{K}_0(k'G), \quad G_0(kG) \to G_0(k'G),$$

definidos mediante la tensorización por K', k' y k' respectivamente. Las tres aplicaciones son inyectivas. Más aún, las aplicaciones

$$\mathcal{K}_0(kG) \to \mathcal{K}_0(k'G), \quad G_0(kG) \to G_0(k'G),$$

son inyecciones que identifican a $\mathcal{K}_0(kG)$ y $G_0(kG)$ como sumando directos sobre $\mathbb{Z}$ de $\mathcal{K}_0(k'G)$ y $G_0(k'G)$, respectivamente.

$\square$

Existen ejemplos que muestran que la inyección $G_0(KG) \to G_0(K'G)$ no identifica a $G_0(KG)$ como sumando directo sobre $\mathbb{Z}$ de $G_0(K'G)$. Por ejemplo, sean G el grupo de los cuaterniones de orden 8 y K una extensión finita de $\mathbb{Q}$ que contiene las 8-ésimas raíces de la unidad. Sea $M = \mathbb{Q} \oplus \mathbb{Q} \cdot i \oplus \mathbb{Q} \cdot j \oplus \mathbb{Q} \cdot k$ el $\mathbb{Q}G$-módulo simple de los cuaterniones sobre $\mathbb{Q}$. Es fácil ver que

$$[K \oplus_{\mathbb{Q}} M] = 2[W] \quad \text{en } G_0(KG),$$

donde W es un KG-módulo simple de dimensión 2 sobre K. De aquí se deduce que la imagen de $G_0(\mathbb{Q}G)$ en $G_0(KG)$ no es un sumando directo sobre $\mathbb{Z}$ de $G_0(KG)$.

Proposición 3.12 *Sea (K', R', k') una extensión finita del sistema p-modular (K, R, k). Entonces existe un diagrama conmutativo*

$$\begin{tikzcd} G_0(KG) \arrow[r] \arrow[d, "d"'] & G_0(K'G) \arrow[d, "d"'] \\ G_0(kG) \arrow[r] & G_0(k'G), \end{tikzcd}$$

donde las aplicaciones verticales son los morfismos de descomposición, y las aplicaciones horizontales son las inyecciones definidas en la proposición anterior.

$\square$

3.4. Caracteres de Brauer

En esta sección, interpretaremos el mapa de descomposición en término de caracteres. Como ya nos es habitual, daremos algunas definiciones antes de desarrollar la teoría.

3.4.1. Cuerpos de descomposición

Definición 45 *Sea G un grupo finito de exponente m, es decir, el máximo común múltiplo de los órdenes de los elementos en G. Diremos que un cuerpo E es* **suficientemente grande** *con respecto a G, si contiene a todas las raíces m-ésimas de la unidad.*

Si la característica de E es 0, entonces E es suficientemente grande con respecto a G si y sólo si E contiene al cuerpo ciclotómico de las raíces m-ésimas de la unidad. Por otra parte, si $car\ E = p > 0$, y $m = p^a \cdot m^{'}$, donde p no divide a $m^{'}$, entonces en $E[X]$ tenemos la siguiente igualdad:

$$X^m - 1 = (X^{m^{'}} - 1)^{p^a},$$

y por tanto, E contiene a las raíces m-ésimas de la unidad si y sólo si E contiene a las raíces $m^{'}$-ésimas de la unidad. Más aún, el polinomio $X^{m^{'}} - 1$ es separable sobre E, y todas sus raíces forman un grupo cíclico de orden $m^{'}$ generado por cualquier raíz $m^{'}$-ésima primitiva de la unidad.

Sean A una K-álgebra de dimensión finita, M un A-módulo a izquierda y E una extensión de cuerpos de K. Entonces la E-álgebra $A^E = E \otimes_K A$, que se obtiene extendiendo escalares, es de dimensión finita y $M^E = E \otimes_K M$ tiene una estructura de A^E-módulo a izquierda inducida por la acción

$$(e \otimes_K a) \cdot (e^{'} \otimes_K m) = ee^{'} \otimes_K a \cdot m, \quad e,\ e^{'} \in E,\ a \in A,\ m \in M.$$

Definición 46 *Sean A una K-álgebra de dimensión finita y M un A-módulo a izquierda. Decimos que M es* **absolutamente simple** *si para toda extensión de cuerpos E de K, el A^E-módulo M^E es simple.*

Traduciendo esta definición al lenguaje de representaciones sobre G, y recordando la definición 28 del capítulo 2, un espacio de representación M se dice absolutamente irreducible si para toda extensión de cuerpos E de K, la representación que se obtiene extendiendo escalares de K en E sigue siendo irreducible. A esta representación de $E[G] = EG$ la denotábamos M^E.

No todos los módulos simples resultan absolutamente simples. Consideremos, por ejemplo, $G = \mathbb{Z}_4$ el grupo cíclico aditivo de orden 4. El anillo $\mathbb{R}[\mathbb{Z}_4]$ es un anillo semisimple, siendo

$$\mathbb{R}[\mathbb{Z}_4] = \mathbb{R}_{tr} \oplus \mathbb{R}_{sg} \oplus V;$$

donde $(\mathbb{R}_{tr},\ tr)$ es la representación trivial de dimensión 1 sobre $\mathbb{R}$, $(\mathbb{R}_{sg},\ sg)$ es la representación signo de dimensión 1, y $(V,\ \rho)$ es la representación de dimensión 2 de $\mathbb{Z}_4$ dada por

$$\rho(u) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \in \mathbb{R}^{2\times 2},$$

siendo u un generador de $\mathbb{Z}_4$. Claramente, V es una representación irreducible de $\mathbb{Z}_4$ sobre $\mathbb{R}$. Sin embargo, al extender escalares al cuerpo de los números complejos, deja de ser simple. A saber,

$$\mathbb{C} \otimes_{\mathbb{R}} V = \mathbb{C}_i \oplus \mathbb{C}_{-i},$$

donde $\mathbb{C}_i$ es el espacio generado por el autovector asociado al autovalor i y $\mathbb{C}_{-i}$ es el espacio generado por el autovector asociado al autovalor $-i$.

Definición 47 *Sea A una K-álgebra de dimensión finita sobre K y sea E una extensión de cuerpos de K. Decimos que E es un* **cuerpo de descomposición** *de A sobre K, si todo A^E-módulo a izquierda simple es absolutamente simple.*

La siguiente proposición se sigue inmediatamente de la definición anterior:

Proposición 3.13 *Si E es un cuerpo de descomposición de A sobre K, entonces toda extensión de cuerpos F de E también es un cuerpo de descomposición.*

$\square$

Las siguientes proposiciones no son tan inmediatas, para sus demostraciones ver [C-R].

Proposición 3.14 *Para toda K-álgebra A, cualquier cuerpo algebraicamente cerrado que contenga a K es un cuerpo de descomposición de A.*

$\square$

Proposición 3.15 *Toda K-álgebra A de dimensión finita admite un cuerpo de descomposición E tal que la extensión E/K es finita.*

$\square$

Teorema 3.1 *Si E es suficientemente grande con respecto a G, entonces E es un cuerpo de descomposición de G, y de todos sus subgrupos.*

$\square$

Observación: En el caso particular que $A = KG$, es claro que este teorema implica la proposición anterior. En efecto, basta adjuntar a K todas las raìces primitivas de orden $m = exp\ G$.

Corolario 3.3 *Sea $(K,\ R,\ k)$ un sistema p-modular tal que car $K = 0$. Si K es suficientemente grande con respecto a G, entonces k también es suficientemente grande, y ambos son cuerpos de descomposición de G y de todos sus subgrupos.*

Demostración:
Sean m el exponente de G, $m = p^a \cdot m^{'}$, donde p no divide a $m^{'}$, y ω una raíz m-ésima primitiva de la unidad en K. Como K es el cuerpo de cocientes del anillo de valuación R y ω cumple que $\omega^m - 1 = 0$, entonces $\omega \in K$ es raíz de un polinomio con coeficientes en $\mathbb{Z}$; esto implica que $\omega \in R$. Tenemos entonces que

$$X^m - 1 = \prod_{i=0}^{m-1} (X - \omega^i), \quad \text{en } R[X].$$

Pasando esta igualdad al cuerpo residual tenemos que

$$(X^{m^{'}} - \bar{1})^{p^a} = X^m - 1 = \prod_{i=0}^{m-1} (X - \bar{\omega}^i), \quad \text{en } k[X].$$

Por tanto, las potencias $\bar{\omega}^i,\ 1 \leq i \leq m-1$, dan todas las raíces $m^{'}$-ésimas de la unidad, cada una con multiplicidad p^a. Cada $\bar{\omega}^i \in k$, puesto que $\omega^i \in R$. Luego, k contiene las raíces $m^{'}$-ésimas de la unidad, y por consiguiente las m-ésimas. Esto implica que k es suficientemente grande con respecto a G. Lo que sigue de la demostración se deduce inmediatamente del teorema anterior. $\square$

Para finalizar esta sección, daremos un resultado de Dedekind que nos será muy útil en la siguiente.

Teorema 3.2 *Sean E un cuerpo arbitrario y G un grupo finito. Los caracteres dados por el conjunto base de EG-módulos simples son linealmente independientes sobre E.*

□

3.4.2. Caracteres de Brauer

En esta sección desarrollaremos una idea fundamental en la teoría, debida a Brauer. A lo largo de esta exposición, $(K,\ R,\ k)$ será un sistema p-modular, tal que $car\ K = 0$, y K es suficientemente grande con respecto a un grupo finito G dado. Por m denotaremos al exponente de ese grupo finito, donde $m = p^a \cdot m^{'}$ tal que p no divide a $m^{'}$, y por $\omega \in K$ a una raíz $m^{'}$-ésima primitiva de la unidad. Veremos que los caracteres de las representaciones irreducibles de G sobre k son linealmente independientes sobre k. Sin embargo, hay ejemplos donde dos kG-módulos tiene el mismo carácter sobre k sin ser isomorfos, ni tener los mismos factores de composición. La gran utilidad de los caracteres sobre cuerpos de característica cero motivó la búsqueda de manejar los caracteres de los kG-módulos sin perder mucha información. Brauer encontró una manera ingeniosa de hacer esto asociando a cada kG-módulo $\overline{M}$ una función a valores en K, definida sobre el conjunto $G_{p'}$ de los elementos p-regulares de G.

Por el corolario 3.3, si K es suficientemente grande, entonces k es suficientemente grande con respecto a G, siendo además K y k cuerpos de descomposición de G y de todos sus subgrupos. Más aún, siguiendo la demostración de ese corolario, la imagen de ω por el morfismo natural $f : R \to k, \quad f(\omega) = \bar{\omega}$, es una raíz $m^{'}$-ésima primitiva de la unidad en k. Por tanto,

$$f :< \omega > \to < \bar{\omega} >,$$

es un isomorfismo entre los grupos cíclicos de raíces $m^{'}$-ésimas de la unidad en K y k, respectivamente.

Sea L un kG-módulo a izquierda. Para cada elemento p-regular de G, $x \in G_{p'}$, los autovalores $\{\xi_1, \ldots,\ \xi_d\}$ asociados al endomorfismo de L que define x son raíces $m^{'}$-ésimas de la unidad. Luego, se pueden expresar como potencias de $\bar{\omega}$, digamos $\{\bar{\omega}^{i_1}, \ldots,\ \bar{\omega}^{i_d}\}$, siendo $d = dim_k\ L$. Definimos entonces una función a valores en K por la fórmula

$$\lambda_L(x) = \omega^{i_1} + \cdots + \omega^{i_d}. \tag{4}$$

Utilizando el isomorfismo f, la definición anterior en término de los autovalores $\{\xi_i\}$ del endomorfismo de L determinado por x es

$$\lambda_L(x) = \sum_{i=1}^{d} f^{-1}(\xi_i).$$

Es claro que una vez fijado el sistema p-modular $(K,\ R,\ k)$, no hay ambigüedad en la definición de λ, ya que el isomorfismo $f :< \omega > \to < \bar{\omega} >$ queda determinado por la aplicación natural $R \to R/\wp$.

Definición 48 *Sea L un kG-módulo a izquierda. La función a valores en K*

$$\lambda : G_{p'} \to K,$$

definida en (4) se denomina el **carácter de Brauer** *de G inducido por L.*

La función traza $x \mapsto Tr(x,\ L),\ x \in G$ a valores en k, se denomina el k-**carácter** de L. En su trabajo, Brauer solía llamar a estas funciones a valores en K caracteres modulares.

Proposición 3.16 *i) El carácter de Brauer λ_L, L un kG-módulo a izquierda de dimensión finita, es una función de clases sobre los elementos p-regulares de G.*

ii) El carácter de Brauer λ_L toma valores en R, y además

$$\overline{\lambda_L(x)} = Tr(x,\ L),\ x \in G_{p'}.$$

iii) Consideremos un kG-módulo L_0 y un kG-submódulo L_1 no nulo. Sean χ el carácter de Brauer inducido por L_0/L_1, χ_1 el carácter de Brauer inducido por L_1 y χ_0 el carácter de Brauer inducido por L_0. Entonces $\chi_0 = \chi + \chi_1$.

iv) Sea V un KG-módulo con carácter sobre K χ_V. Entonces para cada RG-retículo completo M en V, la imagen de la restricción $\chi_V|_{G_{p'}}$ de χ_V a $G_{p'}$ es el carácter de Brauer del kG-módulo $\overline{M}$.

Demostración:
i) Sean $x,\ y \in G_{p'}$, y supongamos que existe $z \in G$ tal que $x = z^{-1}yz$. Entonces los polinomios característicos de los endomorfismos de L que inducen x e y son el mismo. Luego, sus autovalores son los mismos, y por tanto, también lo deben ser sus caracteres de Brauer.

ii) Por lo visto en la sección anterior, si K es suficientemente grande, las raíces $m^{'}$-ésimas de la unidad pertenecen a R. Luego, el carácter de Brauer toma valores en R. Como el morfismo $R \to k$ es un isomorfismo cuando se restringe al grupo cíclico de raíces $m^{'}$-ésimas de la unidad, tenemos que la reducción del carácter de Brauer λ debe ser el k-carácter de L.

iv) Sea $\mathbf{M}$ la matriz de representación de G inducida por V, con respecto a una base sobre R de un RG-retículo completo M en V. Para cada $x \in G_{p'}$, los autovalores $\{\xi_i\}_{1 \leq i \leq d}$ de $\mathbf{M}(x)$ pertenecen a R, y

$$\chi_V(x) = \xi_1 + \cdots + \xi_d.$$

Como $\overline{\mathbf{M}}$ es la matriz de la representación de G dada por el kG-módulo $\overline{M}$, bastaría ver que $\{\bar{\xi}_i\}_{1 \leq i \leq d}$ son los autovalores de $\overline{\mathbf{M}}(x)$. La matriz $\mathbf{M}(x)$ tiene coeficientes en R, por tanto su polinomio característico $P_{\mathbf{M}(x)} \in R[X]$, y

$$P_{\mathbf{M}(x)} = \prod_{i=1}^{d}(X - \xi_i), \quad \text{en } R[X].$$

El polinomio que se obtiene reduciendo los coeficientes de $P_{\mathbf{M}}$ módulo $\wp$ es el polinomio característico de $\overline{\mathbf{M}}(x)$. Por tanto,

$$P_{\overline{\mathbf{M}}(x)} = \prod_{i=1}^{d}(X - \overline{\xi_i}), \quad \text{en } k[X].$$

Luego, $\{\bar{\xi}_i\}_{1 \leq i \leq d}$ son los autovalores de $\overline{\mathbf{M}}(x)$, como se quería probar.

iii) Es consecuencia inmediata de *iv)* y de que la igualdad vale para carácteres inducidos por representaciones sobre K. $\square$

Sean $\{F_1, \dots,\ F_r\}$ un conjunto base de kG-módulos simples y $\{\varphi^1, \dots, \varphi^r\}$ los caracteres de Brauer inducidos por los kG-módulos simples, a los cuales llamaremos **caracteres de Brauer irreducibles**. Sea Z_i un KG-módulo simple con carácter ξ^i. Entonces por la proposición anterior, más especificamente por el ítem *iii)*, el mapa de descomposición está dado en términos de caracteres por

$$\xi^i(x) = \sum_{j=1}^{r} d_{ij}\varphi^j(x), \quad \forall\ x \in G_{p'},$$

siendo $\mathbf{D} = (\mathbf{d_{ij}})$ la matriz de descomposición.

Sabemos por el teorema 3.2 que los k-caracteres inducidos por los módulos $\{F_1, \ldots,\ F_r\}$ son linealmente independientes sobre k. En lo que sigue, veremos que los caracteres de Brauer $\{\varphi^i\}$ son linealmente independientes sobre K. Sin embargo, necesitamos primero demostrar el siguiente lema.

Lema 3.2 *Sea* $\mathbf{M} : G \to GL_n(k)$ *una representación matricial de* G *sobre* k*. Sea* $x \in G$*, tal que su descomposición en partes p-regular* s *y en p-parte* u *está dada por* $x = s \cdot u$*. Entonces las matrices* $\mathbf{M}(x)$ *y* $\mathbf{M}(s)$ *tienen los mismos autovalores, contados con multiplicidad.*

Demostración:
Por definición, tenemos que $\mathbf{M}(x) = \mathbf{M}(s)\mathbf{M}(u)$, donde las matrices $\mathbf{M}(s)$ y $\mathbf{M}(u)$ conmutan. Luego, se diagonalizan en la misma base y, por consiguiente, el conjunto de autovalores de $\mathbf{M}(x)$ está dado por producto de a pares entre autovalores de $\mathbf{M}(s)$ y autovalores de $\mathbf{M}(u)$. Como u es un elemento cuyo orden es potencia de p, debe ser que $\mathbf{M}(u)^{p^k} = I$, para cierto $k \in \mathbb{N}$. Como *car* $k = p$, se tiene que todos los autovalores de $\mathbf{M}(u)$ deben ser igual a 1. En particular, esto implica que los autovalores de $\mathbf{M}(x)$ y los autovalores de $\mathbf{M}(s)$ son iguales, contados con multiplicidad. $\square$

Teorema 3.3 *Los caracteres de Brauer irreducibles* $\{\varphi^1, \ldots,\ \varphi^r\}$ *forman una base sobre* K *del espacio de funciones de clases sobre* $G_{p'}$ *a valores en* K*.*

Al espacio de funciones de clases sobre $G_{p'}$ a valores en K lo notaremos como $cf_K(G_{p'})$.

Demostración:
Veamos primero que el conjunto $\{\varphi^1, \ldots,\ \varphi^r\}$ es linealmente independiente sobre K. Supongamos que no, y consideremos una combinación lineal de dependencia lineal no trivial con coeficientes en K. Como K es el cuerpo de cocientes de R, limpiando denominadores obtenemos una relación con coeficientes en R. Por lo visto anteriormente, toda no unidad de R es divisible por una potencia de π, siendo π un elemento de $\wp$ que genera el grupo de valores de la valuación. Luego, dividiendo por una potencia apropiada de π, tenemos la siguiente relación

$$\sum_{i=1}^{r} a_i \varphi^i(s) = 0, \quad \forall\ s \in G_{p'},$$

donde $a_i \in R$, y algún $a_{i_0} \notin \wp$. Reduciendo módulo $\wp$ obtenemos

$$\sum_{i=1}^{r} \bar{a}_i \overline{\varphi^i(s)} = 0, \quad \forall\ s \in G_{p'},$$

donde por lo menos un coeficiente $a_{i_0} \neq 0$ en k. Por (3.16.*ii*), podemos escribir la relación anterior como

$$\sum_{i=1}^{r} \bar{a}_i Tr(s,\ F_i) = 0, \quad \forall\ s \in G_{p'}.$$

Por la proposición anterior, tenemos que $Tr(s,\ F_i) = Tr(x,\ F_i)$, si s es la parte p-regular de x, ya que $Tr(x,\ F_i)$ es la suma de los autovalores del endomorfismo de F_i que determina x. Se sigue entonces que

$$\sum_{i=1}^{r} \bar{a}_i Tr(x,\ F_i) = 0, \quad \forall\ x \in G.$$

Como $a_{i_0} \neq 0$ en k, tenemos una relación de dependencia lineal sobre k de los k-caracteres correspondientes a los kG-módulos simples $\{F_i\}$. Esto contradice (3.2). Por tanto, $\{\varphi^1, \ldots, \varphi^r\}$ es linealmente independiente sobre K.

Veamos ahora que generan $cf_K(G_{p'})$. Sea $\xi \in cf_K(G_{p'})$ una función de clases a valores en K sobre $G_{p'}$. Luego, ξ se puede extender a una función de clases $\tilde{\xi}$ sobre todo G, poniendo por ejemplo $\tilde{\xi}(x) = 0$ para $x \notin G_{p'}$. Al ser $car\ K = 0$ y K suficientemente grande, del primer capítulo sabemos que $\tilde{\xi}$ es combinación de los caracteres irreducibles $\{\xi^1, \ldots, \xi^s\}$ correspondientes a las representaciones irreducibles sobre K de G. Entonces

$$\tilde{\xi}(x) = \sum_{j=1}^{s} \alpha_j \xi^j, \quad \forall\ x \in G,$$

para cierto coeficientes $\alpha_j \in K$. Restringiendo la igualdad anterior al subgrupo de elementos p-regulares de G tenemos

$$\xi = \sum_{j=1}^{s} \alpha_j \xi^j|_{G_{p'}},$$

Pero $\xi^j|_{G_{p'}}$ es una combinación lineal sobre K de los caracteres de Brauer irreducibles $\{\varphi^1, \ldots, \varphi^r\}$, por tanto también lo es ξ. $\square$

Dado que dos representaciones de G sobre k no isomorfas pueden tener el mismo carácter de Brauer, cabe preguntarse cómo se relacionan. El siguiente corolario nos dice que al menos determinan el mismo elemento en el grupo de Grothendieck $G_0(kG)$, es decir, tienen los mismos factores de composición.

Corolario 3.4 *Sean L, M dos kG-módulos. Si $\lambda_L = \lambda_M$, entonces L y M tienen el mismo conjunto de factores de composición, y por tanto $[L] = [M]$, en $G_0(kG)$.*

Demostración:
Supongamos que L y M tienen series de composición tales que los kG-módulos simples F_i aparecen a_i veces en L y b_i veces en M. Por (3.16.*iii*), se sigue que

$$\lambda_L = \sum_{i=1}^{r} a_i \varphi^i, \quad \lambda_M = \sum_{i=1}^{r} b_i \varphi^i.$$

Por el teorema anterior, si $\lambda_L = \lambda_M$, entonces $a_i = b_i,\ 1 \leq i \leq r$. Por tanto, L y M tienen el mismo conjunto de factores de composición. $\square$

El siguiente corolario es de suma importancia porque determina la cantidad de kG-módulos simples en un conjunto base.

Corolario 3.5 *Sea E un cuerpo de descomposición de G de característica p. Entonces el número de clases de isomorfismo de EG-módulos absolutamente simples es igual al número de clases de conjugación de elementos p-regulares de G.*

Demostración:
Veamos primero que es suficiente probarlo para kG-módulos, donde k es parte del sistema p-modular $(K,\ R,\ k)$.

Recordemos que K y por tanto k son suficientemente grandes por hipótesis. A saber, existe un cuerpo de composición que es extensión de E y de k,

$$\begin{tikzcd}[column sep=small] & L = kE \arrow[dl, dash] \arrow[dr, dash] & \\ k \arrow[dr, dash] & & E \arrow[dl, dash] \\ & \mathbb{F}_p & \end{tikzcd} \quad .$$

Como E es un cuerpo de descomposición de G, los EG-módulos simples deben coincidir con los L-módulos simples. Análogamente, los kG-módulos simples deben coincidir con los L-módulos simples, por tanto, los EG-módulos simples deben coincidir con los kG-módulos simples.

Luego, debemos probar que el número de clases de isomorfismo de kG-módulos es igual al número de clases de conjugación de G contenidas en $G_{p'}$. Pero esto es inmediato, pues los caracteres de Brauer irreducibles $\{\varphi^1, \dots, \varphi^r\}$ forman una base sobre K de $cf_K(G_{p'})$. □

Interpretaremos ahora el mapa de descomposición en términos de los caracteres de Brauer.

Definición 49 *Un* **carácter virtual de Brauer** *sobre G es una combinación lineal sobre $\mathbb{Z}$ de caracteres de Brauer de kG-módulos. El conjunto de los caracteres virtuales de Brauer se denota por $Bch\ kG$.*

Lema 3.3 *Sean L y M dos kG-módulos. Entonces el carácter de Brauer dado por el kG-módulo $L \otimes_k M$ es $\lambda_L \lambda_M$.*

Demostración:
Sea $x \in G_{p'}$. Las transformaciones lineales que define sobre L y sobre M son diagonalizables. Tomando bases de autovectores sobre L y sobre M, podemos formar una base de $L \otimes_k M$ tomando el producto tensorial entre los elementos de ambas bases. Luego, los autovalores de x sobre $L \otimes_k M$ son el producto de los autovalores de x sobre L y los autovalores de x sobre M. Como los caracteres de Brauer están definidos en términos de autovalores, se deduce que el carácter de Brauer asociado a $L \otimes_k M$ debe ser $\lambda\mu$. □

Proposición 3.17 *El conjunto de caracteres virtuales de Brauer $Bch\ kG$ es un anillo cuyas operaciones son la suma y el producto de funciones. La aplicación que asigna a cada elemento $t \in G_0(kG)$ el carácter virtual de Brauer asociado a él, define un isomorfismo de $\mathbb{Z}$-álgebras, esto es*

$$G_0(kG) \cong Bch\ kG.$$

Demostración:
Dado un elemento $t \in G_0(kG)$, sabemos que es combinación lineal de $\{F_1, \dots, F_r\}$, con coeficientes en $\mathbb{Z}$,

$$t = \sum_{i=1}^{r} a_i [F_i], \quad a_i \in \mathbb{Z},$$

estando los coeficientes unívocamente determinados. El carácter virtual de Brauer τ asociado a t está definido por

$$\tau = \sum_{i=1}^{r} a_i \varphi^i, \quad a_i \in \mathbb{Z}.$$

Por el teorema anterior, sabemos que $\{\varphi^1, \ldots, \varphi^r\}$ forma una base sobre $\mathbb{Z}$ de $Bch\ kG$. Por tanto, la aplicación

$$t \mapsto \tau,$$

es un isomorfismo de $\mathbb{Z}$-módulos libres. Por el lema anterior, se deduce que este isomorfismo es de $\mathbb{Z}$-álgebras, como se quería probar. $\square$

Finalizaremos esta sección con la siguiente proposición:

Proposición 3.18 *El diagrama*

$$\begin{array}{ccc} G_0(KG) & \longrightarrow & ch\ KG \\ {\scriptstyle d}\downarrow & & \downarrow{\scriptstyle d'} \\ G_0(kG) & \longrightarrow & Bch\ kG \end{array},$$

es un diagrama conmutativo, donde las aplicaciones horizontales son los isomorfismos definidos en (3.5) y en (3.17). La aplicación vertical d es el mapa de descomposición, y d' es la restricción $\psi \mapsto \psi|_{G_{p'}}$ de los caracteres virtuales $\psi \in ch\ KG$ a $G_{p'}$.

Demostración:
Basta verificar que el diagrama conmuta en cada elemento de la base $\{[Z_j]\}$ de $G_0(KG)$ que corresponde al KG-módulo simple Z_j. Por lo visto anteriormente sabemos que

$$d[Z_j] = \sum_{i=1}^{r} r_i(Z_j)[F_i], \quad \text{en } G_0(kG).$$

Luego, el carácter virtual de Brauer asociado a $d[Z_i]$ está dado por

$$\tilde{\xi^j} = \sum_{i=1}^{r} r_i(Z_j)\varphi^i, \quad \text{sobre } G_{p'}.$$

Pero

$$\xi^j|_{G_{p'}} = \sum_{i=1}^{r} r_i(Z_j)\varphi^i, \quad \text{sobre } G_{p'}.$$

Por tanto, $\tilde{\xi^j} = \xi^j|_{G_{p'}}$, lo que implica que el diagrama conmuta para los elementos $[Z_i]$, como se quería probar. $\square$

Ejemplo

Sean p un primo impar y $G = Sl_2(p)$ el grupo de matrices de 2×2 con coeficientes en el cuerpo $\mathbb{F}_p$ y de determinante 1. Sea $|G| = p^a \cdot m'$, donde p no divide a m' y sea $(K,\ R,\ k)$ un sistema p-modular con $car\ K = 0$ y K suficientemente grande con respecto a G. Es fácil ver que las clases de conjugación de los elementos p-regulares de G están determinadas por su ecuación característica y que hay exactamente p clases de conjugación de elementos p-regulares. A saber, si dos elementos $a,\ b \in G$ son conjugados, entonces tienen el mismo polinomio característico $P_a(X)$ en $\mathbb{F}_p[X]$. Como las matrices son de 2×2, este polinomio tiene la forma

$$P_a(X) = X^2 - tr(a)X + 1, \quad \text{donde } tr(a) \in \mathbb{F}_p,$$

siendo $tr(a)$ la suma de los autovalores del endomorfismo que determina $a \in G$. Como $a \in G_{p'}$, éstos son raíces de la unidad, una conjugada de la otra. Como $p > 2$, se deduce que el polinomio es minimal y que si dos elementos p-regulares tienen el mismo polinomio característico, entonces son conjugados. Como la cantidad de polinomios característicos que dividen a $X^{m'} - 1$ es p, tenemos que la cantidad de clases de conjugación de elementos p-regulares es p. Luego, por (3.5) sabemos que hay exactamente p clases de isomorfismo de kG-módulos simples, cuya construcción es la siguiente:

Para cada d, $0 \leq d \leq p-1$, sea M_d el espacio sobre k de polinomios homogéneos de grado d en dos variables $X,\ Y$. El grupo G actúa sobre $k[X,Y]$ como un grupo de automorfismos por

$$gX = \alpha X + \beta Y, \quad gY = \gamma X + \delta Y,$$

siendo

$$g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in G.$$

Los subespacios $\{M_d\}_{0 \leq d \leq p-1}$ de $k[X,Y]$ son kG-módulos de dimensión $1,\ 2, \ldots,\ p$, respectivamente. Por la definición de la acción de G sobre M_d, es claro que los elementos

$$X^d,\ X^{d-1}Y, \ldots,\ XY^{d-1},\ Y^d,$$

generan subespacios no isomorfos de dimensión 1 que son estables por la acción de T, siendo $T \subset G$ el subgrupo de las matrices diagonales. En particular, dichos subespacios tiene una estructura de kT-módulos. Siguiendo este razonamiento, se puede ver que los espacios M_d son kG-módulos simples, con $1 \leq d \leq p-1$. Comparando la $dim_k\ M_d$ con $|G|$, se ve que las dimensiones de los kG-módulos simples no tienen por qué dividir al orden del grupo.

3.5. El triángulo de Cartan-Brauer.

En la sección anterior definimos el morfismo de descomposición para un sistema p-modular arbitrario $(K,\ R,\ k)$ y un grupo finito G. En esta sección supondremos que RG es un anillo semiperfecto. Mostraremos que existe un diagrama conmutativo entre $G_0(KG)$, $G_0(kG)$ y $\mathcal{K}_0(kG)$, que se denomina el triángulo de Cartan-Brauer. Las propiedades de dicho triángulo se deducen de suponer K suficientemente grande, y luego éstas se aplican para obtener relaciones de ortogonalidad para los caracteres de Brauer de los kG-módulos y de sus envolventes proyectivas.

La hipótesis de que RG sea un anillo semiperfecto se cumple cuando R es completo con la topología $\wp$-ádica. Esto ocurre cuando K es la completación de algún cuerpo algebraico con respecto a una valuación discreta, siendo R el anillo de valuación en K. Se puede ver que la condición se mantiene sobre cualquier cuerpo K que sea suficientemente grande con respecto a G y cuya característica no divida al orden del grupo. Por otro lado, kG es un anillo semiperfecto para cualquier cuerpo. En las siguientes subsecciones no supondremos que K sea suficientemente grande o de característica cero.

3.5.1. Envolventes Proyectivas

Sea A un anillo cualquiera. Comenzaremos con la definición y algunas propiedades de la envolvente proyectiva de un A-módulo cualquiera, y veremos bajo qué condiciones ésta existe.

Definición 50 *Sean A un anillo y M, N dos A-módulos a izquierda. Una aplicación $f \in Hom_A(M,N)$ se dice* **esencial** *si f es suryectiva, y para cada sucesión de A-módulos $X \xrightarrow{g} M \xrightarrow{f} N$ tal que fg es suryectiva, entonces la aplicación g es también suryectiva.*

En otras palabras, una aplicación suryectiva $f : M \to N$ es esencial si ningún submódulo propio de M tiene como imagen N.

Definición 51 *Una* **envolvente proyectiva** *de un módulo M es un diagrama*

$$P \xrightarrow{f} M,$$

donde P es un A-módulo proyectivo y f es esencial.

Proposición 3.19 *Las envolventes proyectivas son únicas salvo isomorfismos. Esto es, dadas dos envolventes proyectivas $P \xrightarrow{f} M$ y $P' \xrightarrow{f'} M$, existe un isomorfismo θ entre P y P' tal que $f = f'\theta$.*

Demostración:
Al ser P un A-módulo proyectivo y la aplicación f' suryectiva, existe un morfismo θ tal que el siguiente diagrama

$$\begin{tikzcd} & P \arrow[dl, dashed, "\theta"'] \arrow[d, "f"] \\ P' \arrow[r, "f'"'] & M \end{tikzcd},$$

resulta conmutativo, es decir que $f = f'\theta$. Luego, θ es suryectiva ya que $f'\theta$ es suryectiva y f' es esencial. Análogamente, al ser P' proyectivo, existe un morfismo $\varphi : P' \to P$, tal que $\theta\varphi = id_{P'}$. Entonces $f\varphi = f'\theta\varphi = f'$; en particular, resulta que φ es suryectiva ya que $f\varphi$ es suryectiva y f es esencial. Por tanto, φ y θ son isomorfismos.
□

Observación: Algunos módulos pueden no tener envolvente proyectiva. Por ejemplo, el $\mathbb{Z}$-módulo $\mathbb{Z}/2\cdot\mathbb{Z}$ no tiene ninguna. A saber, si $f : P \to \mathbb{Z}/2\cdot\mathbb{Z}$ es una envolvente proyectiva, con P proyectivo sobre $\mathbb{Z}$; entonces P es libre sobre $\mathbb{Z}$ por ser $\mathbb{Z}$ un dominio principal, y $3 \cdot P$ es un submódulo propio de P tal que $f(3 \cdot P) = \mathbb{Z}/2\cdot\mathbb{Z}$, lo cual es una contradicción porque suponíamos que f era esencial. El próximo resultado nos muestra cómo se pueden determinar envolventes proyectivas en algunos casos.

Lema 3.4 *Sea $f : X \to M$ una aplicación suryectiva de A-módulos a izquierda finitamente generados. Si*

$$ker\ f \subseteq (rad\ A)X,$$

entonces f es esencial.

Demostración:
Sea $Y \subseteq X$ un submódulo tal que $f(Y) = M$. Entonces

$$X = Y + ker\ f = Y + (rad\ A)X.$$

Luego, $X = Y$ por el lema de Nakayama; lo que prueba que f es esencial. $\square$

Corolario 3.6 *Sea P un A-módulo a izquierda proyectivo finitamente generado, y sea J un ideal bilátero contenido en rad A. Entonces la aplicación natural $P \to P/JP$ da una envolvente proyectiva del A-módulo P/JP.*

Demostración:
Se deduce inmediatamente del lema anterior debido a que $P \to P/JP$ resulta esencial. $\square$

Supongamos que A es un anillo semiperfecto y que $N = rad\ A$. Luego, el anillo $\bar{A} = A/N$ es un anillo semisimple; en particular se tiene una descomposición

$$\bar{A} = \bigoplus \bar{A}\bar{e}_i,$$

siendo $\bar{e}_i$ idempotentes primitivos centrales y $\bar{A}\bar{e}_i$ son $\bar{A}$-módulos a izquierda simples. Más aún, todo $\bar{A}$-módulo simple es isomorfo $\bar{A}\bar{e}_i$ para algún i. Usando esto se puede probar el siguiente teorema:

Teorema 3.4 *Sean A un anillo semiperfecto, $N = rad\ A$ y $\bar{A} = A/N$. Entonces todo A-módulo a izquierda finitamente generado X tiene una envolvente proyectiva. Esto es, existe un A-módulo a izquierda proyectivo finitamente generado P tal que $P/NP \cong X/NX$ como $\bar{A}$-módulos, y este isomorfismo se levanta a una aplicación suryectiva $P \to X$ dando una envolvente proyectiva de X.*

Demostración:
(Ver [C-R]) $\square$

Más aún, se puede ver que si todo A-módulo tiene una envolvente proyectiva, entonces A es semiperfecto. (Anderson-Fuller [73, th. 27.6, p. 304])

Considerando sólo A-módulos finitamente generados, tenemos el siguiente corolario:

Corolario 3.7 *Sean A un anillo semiperfecto y $N = rad\ A$.*

i) Sea $f : P \to X$ una aplicación suryectiva, con P proyectivo. Entonces f da una envolvente proyectiva si y sólo si $ker\ f \subseteq N \cdot P$.

ii) Para cada A-módulo X, los módulos X y X/NX tienen la misma envolvente proyectiva como A-módulos.

iii) Las envolventes proyectivas son aditivas; esto es, si $f_i : P_i \to X_i,\ 1 \leq i \leq k$, son envolventes proyectivas, entonces

$$\bigoplus_{i=1}^{k} f_i : \bigoplus_{i=1}^{k} P_i \to \bigoplus_{i=1}^{k} X_i,$$

es una envolvente proyectiva.

□

Para finalizar daremos, sin demostración, una proposición que se deriva del teorema de Krull-Schmidt-Azumaya y que es de gran interés para la siguiente sección.

Proposición 3.20 *Sean A un anillo semiperfecto, N un ideal bilátero contenido en rad A y $\bar{A} = A/N$. Para cada A-módulo X, sea $\bar{X} = X/N$ el correspondiente $\bar{A}$-módulo. Sea*

$$A = Ae_1 \oplus \cdots \oplus Ae_n,$$

una descomposición de A en ideales a izquierda indescomponibles, numerados de manera tal que los módulos $Ae_1, \ldots, Ae_m$ son representantes de clases de isomorfismos de módulos no isomorfos entre los $\{Ae_i\}$. Entonces

i) Para cada $P \in \mathcal{P}(A)$, existen enteros no negativos $\{r_i\}$ tal que

$$P \cong \bigoplus_{i=1}^{m} (Ae_i)^{(r_i)}.$$

ii) Si $\{r_i\}$ y $\{s_i\}$ son enteros no negativos, entonces

$$\bigoplus_{i=1}^{m} (Ae_i)^{(r_i)} \cong \bigoplus_{i=1}^{m} (Ae_i)^{(s_i)} \quad \textit{si y sólo si } r_i = s_i \textit{ para todo } i.$$

iii) Para cada $Y \in \mathcal{P}(\bar{A})$, existen enteros no negativos $\{r_i\}$ tal que

$$Y \cong \bigoplus_{i=1}^{m} (\bar{A}\bar{e_i})^{(r_i)},$$

donde las multiplicidades $\{r_i\}$ están unívocamente determinadas por las clases de isomorfismo de Y.

iv) Las clases de isomorfismo en $\mathcal{P}(A)$ corresponden biyectivamente a aquellas en $\mathcal{P}(\bar{A})$, donde la correspondencia está dada por la aplicación que a cada clase $P \in \mathcal{P}(A)$ le asigna la clase $\bar{P} \in \mathcal{P}(\bar{A})$.

3.5.2. La aplicación de Cartan y el triángulo de Cartan-Brauer.

Comenzaremos dando algunos resultados con respecto a la estructura de RG, kG y sus módulos. Como en las secciones anteriores, denotaremos $RG/\wp G$ por $\overline{RG}$ o por kG; denotando $a \mapsto \bar{a}$ tanto el morfismo de R a k, como el de RG a kG. Sean $N = rad\ RG$ y $\wp G = \wp \cdot (RG)$. Entonces $\wp G \subseteq N$ y $RG/N \cong kG/rad\ kG$. El último isomorfismo implica que los kG-módulos simples se pueden identificar con los RG-módulos simples.

Para ver que $\wp G \subseteq N$, veamos que $\wp GM = 0$ para todo RG-módulo simple M. Como $M = RG \cdot m$, para cada $m \in M$ no nulo, se tiene que M es finitamente generado como R-módulo. Ahora bien, $\wp M$ es un submódulo de M, por tanto debe ser M o 0. Por el lema de Nakayama, $\wp M \neq M$, puesto que en ese caso resultaría $M = 0$. Entonces $\wp M = 0$, y por tanto $\wp GM = 0$ para todo RG-módulo simple M. Ahora veamos que $RG/N \cong kG/rad\ kG$. Es claro que la aplicación suryectiva $\varphi : RG \to \overline{RG}$ se factoriza en una aplicación suryectiva

$$RG/N \to \overline{RG}/rad\ \overline{RG}.$$

Por otro lado, como $\wp G \subseteq N$, existe otra suryección

$$\psi : \overline{RG} \to A/N.$$

Al ser ψ una suryección, se tiene que $\psi(rad\ \overline{RG}) \subseteq rad(RG/N) = 0$, y por tanto, existe una suryección

$$\overline{RG}/rad\ \overline{RG} \rightarrow A/N.$$

Como RG/N y $\overline{RG}/rad\ \overline{RG}$ son álgebras de dimensión finita sobre el cuerpo k, y cada una tiene una suryección en la otra; debe ser que las suryecciones son isomorfismos, obteniendo

$$\overline{RG}/rad\ \overline{RG} \cong RG/N.$$

□

De la teoría de envolventes proyectivas y de la proposición 3.20, se deduce que todo módulo proyectivo finitamente generado sobre RG y kG, respectivamente, se descompone en suma directa de módulos proyectivos indescomponibles, los cuales son únicos salvo isomorfismos y orden de ocurrencia. Esto se deduce de lo siguiente: si $\wp G \subseteq N$, entonces Ae_i es una envolvente proyectiva de $\bar{A}\bar{e_i}$. Luego, por la unicidad de la envolvente proyectiva se tiene que

$$Ae_i \cong Ae_j \text{ si y sólo si } \bar{A}\bar{e_i} \cong \bar{A}\bar{e_j}.$$

De lo hecho hasta ahora se deduce gran parte de la siguiente proposición:

Proposición 3.21 *Sea $(K,\ R,\ k)$ un sistema p-modular tal que RG es un anillo semiperfecto.*

i) Sea $\{F_1, \ldots,\ F_r\}$ un conjunto base de kG-módulos simples. Cada módulo F_i tiene una envolvente proyectiva indescomponible U_i, la cual es isomorfa a un ideal a izquierda de kG generado por un idempotente primitivo. Cada módulo indescomponible proyectivo U_i tiene un único submódulo maximal rad U_i, y $U_i/rad\ U_i \cong F_i$.

ii) A través del isomorfismo $\overline{RG}/rad\ \overline{RG} \cong RG/N$, los módulos simples $\{F_1, \ldots, F_r\}$ se pueden identificar con un conjunto base de RG-módulos simples. Cada RG-módulo simple F_i tiene una envolvente proyectiva indescomponible $P_i \in \mathcal{P}(RG)$ tal que $\bar{P_i} \cong U_i,\ 1 \leq i \leq r$. El módulo P_i se puede tomar como el ideal a izquierda RGe_i, donde e_i es un idempotente primitivo en RG tal que $\bar{e_i}$ es primitivo en kG, y $kG\bar{e_i} \cong U_i$.

iii) Todo RG-módulo proyectivo finitamente generado. M se puede expresar como una suma directa

$$M \cong \bigoplus m_i P_i,$$

donde las multiplicidades $\{m_i\}$ están unívocamente determinadas. Dos módulos M y $M^{'} \in \mathcal{P}(RG)$ son isomorfos si y sólo si $\bar{M} \cong \bar{M}'$. Un módulo $M \in \mathcal{P}(RG)$ es indescomponible si y sólo si $\bar{M}$ es indescomponible.

iv) Cada módulo $M \in \mathcal{P}(RG)$ es la envolvente proyectiva de un módulo semisimple $M/rad\ M$. El módulo $M \in \mathcal{P}(RG)$ es indescomponible si y sólo si $M/rad\ M$ es simple, y en ese caso, rad M es el único submódulo maximal de M.

□

El hecho que $\bar{P_i} \cong U_i$ se sigue de que $\bar{P_i}$ es un módulo proyectivo, pues es sumando directo de RG, y de que ambos $\bar{P_i}$ y U_i son envolventes proyectivas de F_i, para $1 \leq i \leq r$.

Por (3.4) sabemos que los grupos de Grothendieck $\mathcal{K}_0(RG)$ y $\mathcal{K}_0(kG)$ son grupos abelianos libres con base $\{[P_1], \ldots,\ [P_r]\}$ y $\{[U_1], \ldots,\ [U_r]\}$ que corresponden a representantes de clases de isomorfismo de módulos proyectivos indescomponibles en $\mathcal{P}(RG)$ y $\mathcal{P}(kG)$, respectivamente. Por (3.21ii), estas bases se pueden elegir de manera tal que $[\bar{P_i}] = [U_i],$ para $1 \leq i \leq r$. Esto da el siguiente

Teorema 3.5 *La aplicación $[M] \rightarrow [\bar{M}],$ para $M \in \mathcal{P}(RG)$, define un isomorfismo de grupos abelianos:*

$$\mathcal{K}_0(RG) \cong \mathcal{K}_0(kG).$$

Demostración:
Por lo dicho en el parágrafo anterior, existe un isomorfismo de grupos abelianos entre $\mathcal{K}_0(RG)$ y $\mathcal{K}_0(kG)$ dado por

$$\sum_{i=1}^{r} a_i[P_i] \mapsto \sum_{i=1}^{r} a_i[\bar{P}_i], \quad a_i \in \mathbb{Z}.$$

Claramente esta aplicación es biyectiva; por tanto, solamente resta verificar que la aplicación manda $[M]$ en $[\bar{M}]$ para todo $M \in \mathcal{P}(RG)$. Por (3.21iii) sabemos que

$$M \cong \bigoplus_{i=1}^{r} m_i P_i,$$

para ciertos enteros no negativos $\{m_i\}$. Como las relaciones en $\mathcal{K}_0(RG)$ están dadas por descomposiciones en suma directa, tenemos que

$$[M] = \sum_{i=1}^{r} m_i [P_i].$$

Por otro lado, la descomposición de M da

$$\bar{M} \cong \bigoplus_{i=1}^{r} m_i \bar{P}_i,$$

por tanto, tenemos que

$$[\bar{M}] = \sum_{i=1}^{r} m_i [\bar{P}_i].$$

Luego, la imagen de $[M]$ por el isomorfismo es $[\bar{M}]$, como se quería probar. $\square$

Dado una s.e.s. de RG-módulos proyectivos, es claro que tensorizar por K mantiene la exactitud de la sucesión. Por tanto, la aplicación

$$P \mapsto K \otimes_R P, \quad P \in \mathcal{P}(RG),$$

define un morfismo de grupos abelianos entre $\mathcal{K}_0(RG)$ y $G_0(KG)$. Componiendo esta aplicación con el isomorfismo $\mathcal{K}_0(kG) \to \mathcal{K}_0(RG)$, dado por el teorema anterior, obtenemos un morfismo de grupos abelianos:

$$e : \mathcal{K}_0(kG) \to G_0(KG). \tag{5}$$

Sean $U \in \mathcal{P}(kG)$ y $c_i(U)$ la multiplicidad del módulo simple F_i como factor de composición de U. Este número está unívocamente determinado por el teorema de Jordan-Hölder. Luego, existe un morfismo de grupos aditivos

$$c : \mathcal{K}_0(kG) \to G_0(kG),$$

definido por

$$c[U] = [U] = \sum_{i=1}^{r} c_i(U)[F_i] \quad \text{para cada } U \in \mathcal{P}(kG).$$

Definición 52 *El morfismo*

$$c : \mathcal{K}_0(kG) \to G_0(kG),$$

definido anteriormente se denomina el **morfismo de Cartan**. *La* **matriz de Cartan** *de* $r \times r$, $\mathbf{C} = (\mathbf{c_{ij}})$ *de* kG *está definida por*

$$c[U_i] = \sum_{i=1}^{r} c_{ij}[F_j], \quad 1 \leq i \leq r.$$

Luego, la matriz de Cartan es la traspuesta de la matriz de c con respecto a las bases $\{[U_i]\}$ y $\{[F_j]\}$ de $\mathcal{K}_0(kG)$ y $xyG_0(kG)$, respectivamente.

Proposición 3.22 *El* **triángulo de Cartan-Brauer**

$$\begin{tikzcd} G_0(KG) \arrow[rr, "d"] & & G_0(kG) , \\ & \mathcal{K}_0(kG) \arrow[ul, "e"] \arrow[ur, "c"'] & \end{tikzcd}$$

es un diagrama conmutativo de grupos abelianos y morfismos aditivos; siendo d el mapa de descomposición, c el morfismo de Cartan, y e la aplicación definida en (5).

Demostración:
Debemos probar que $d(e[U]) = c[U]$, para cada $U \in \mathcal{P}(kG)$. De la proposición 3.21 se deduce que existe $P \in \mathcal{P}(RG)$ tal que $\bar{P} = U$. Entonces, por definición de e, tenemos que $e[U] = [K \otimes_R P]$. Claramente, P es un RG-retículo completo en $K \otimes_R P$, por tanto, la definición del mapa de descomposición nos dice que $d(K \otimes_R P] = [\bar{P}]$. Luego,

$$d(e[U]) = [\bar{P}] = [U], \quad \text{en } G_0(kG).$$

Por otra parte, el elemento $[U] \in G_0(kG)$ es la imagen $c[U]$ del elemento $[U] \in \mathcal{K}_0(kG)$. Por tanto, $d(e[U]) = c[U]$, como se quería probar. $\square$

3.5.3. Propiedades del triángulo de Cartan-Brauer

En esta sección, seguiremos pidiendo que $(K,\ R,\ k)$ sea un sistema p-modular tal que RG es un anillo semiperfecto. También supondremos que K es suficientemente grande,y que *car* $K = 0$. Como señalábamos antes, si K es la completación de un cuerpo con respecto a una valuación discreta, las hipótesis anteriores garantizan que el anillo RG sea semiperfecto. Más aún, vimos que K y k son cuerpos de descomposición de G y de todos sus subgrupos. Las propiedades del triángulo de Cartan-Brauer son fundamentales para el estudio de los caracteres de Brauer y generalmente, resultan equivalentes a propiedades de la matriz $\mathbf{C}$ de Cartan y la matriz $\mathbf{D}$ del mapa de descomposición.

Denotaremos por $\{Z_1, \ldots,\ Z_s\}$ al conjunto base de KG-módulos simples y por $\{\xi^1, \ldots,\ \xi^s\}$ a sus respectivos caracteres irreducibles. Recordamos la aplicación bilineal definida en el capítulo 1 por

$$(\xi,\ \xi') = \frac{1}{|G|} \sum_{x \in G} \xi(x)\xi'(x^{-1}), \tag{6}$$

para caracteres ξ y $\xi^{'}$ sobre K. Como K es un cuerpo de descomposición, los caracteres irreducibles $\{\xi^1, \ldots, \xi^s\}$ forman una base ortonormal de las funciones centrales sobre K, $cf_K(G)$, con respecto a la forma bilineal. Más aún, tenemos que

$$(\xi,\ \xi^{'}) = i(M,\ M^{'}), \tag{7}$$

para KG-módulos M y $M^{'}$ que inducen los caracteres ξ y $\xi^{'}$, respectivamente. Donde $i(M,\ M^{'})$ es el número entero definido por

$$i(M,\ M^{'}) = dim_K(Hom_{KG}(M,\ M^{'})).$$

Por (3.5), sabemos que $G_0(KG) \cong ch\ KG$ cuando $car\ K = 0$. Luego, podemos definir una aplicación bilineal sobre $\mathbb{Z}$

$$i_K : G_0(KG) \times G_0(KG) \to \mathbb{Z},$$

que corresponde a la forma bilineal sobre $ch\ KG$ definida en (6). Usando la igualdad (7), la formas bilineal i_K se define por

$$i_K([M],\ [M^{'}]) = i(M,\ M^{'}) = (\xi,\ \xi^{'}),$$

para KG-módulos M y $M^{'}$ cuyos caracteres son ξ y $\xi^{'}$, respectivamente. De las relaciones de ortogonalidad se tiene que

$$i_K([Z_i],\ [Z_j]) = \delta_{ij}, \quad 1 \leq i,\ j \leq s.$$

Esto da lugar a la siguiente proposición, que define una forma bilineal sobre el cuerpo de residuos k:

Proposición 3.23 *Sea k un cuerpo de descomposición de G. Existe una aplicación bilineal*

$$i_k : \mathcal{K}_0(kG) \times G_0(kG) \to \mathbb{Z},$$

tal que

$$i_k([U],\ [M]) = dim_k(Hom_{kG}(U,\ M)), \tag{8}$$

para todos los módulos $U \in \mathcal{P}(kG)$ y $M \in\ _{kG}mod$. Más aún, si $\{U_1, \ldots, U_r\}$ y $\{F_1, \ldots, F_r\}$ denotan las correspondientes bases de módulos proyectivos indescomponibles y de módulos simples de kG, respectivamente, tenemos que

$$i_k([U_i],\ [F_j]) = \delta_{ij}, \quad 1 \leq i,\ j \leq r.$$

Demostración:
Definamos primero la aplicación bilineal por (8) sobre la base y luego extendámosla por linealidad a una aplicación

$$i_k : \mathcal{K}_0(kG) \times G_0(kG) \to \mathbb{Z}.$$

Primero debemos probar que la aplicación i_k está bien definida, es decir, que es aditiva en sucesiones exactas cortas. Sean

$$0 \to M^{'} \to M \to M^{''} \to 0,$$

una s.e.s. de kG-módulos y $U \in \mathcal{P}(kG)$. Luego, como P es un kG-módulo proyectivo, tenemos que la sucesión

$$0 \to Hom_{kG}(P,\ M^{'}) \to Hom_{kG}(P,\ M) \to Hom_{kG}(P,\ M^{''}) \to 0,$$

es exacta. Por otro lado, si tenemos una sucesión exacta en $\mathcal{P}(kG)$ dada por

$$0 \to U^{'} \to U \to U^{''} \to 0,$$

entonces $U \cong U' \oplus U^{''}$, y esto implica que

$$Hom_{kG}(U,\ M) = Hom_{kG}(U^{'},\ M) \oplus Hom_{kG}(U^{''},\ M),$$

para todo kG-módulo finitamente generado M. De esto se sigue que i_k está bien definida y es lineal en ambas variables sobre los correspondientes grupos de Grothendieck.

Supongamos ahora que los conjuntos $\{U_i\}$ y $\{F_j\}$ se corresponden entre sí como en la proposición 3.21. Luego, $rad\ U_i$ es el único submódulo maximal de U_i, y $U_i/rad\ U_i$ es un kG-módulo simple que resulta isomorfo a F_i, para $1 \leq i \leq r$, por unicidad de la envolvente proyectiva. Al ser k un cuerpo de descomposición de G, se tiene que

$$dim_k(Hom_{kG}(U_i,\ F_j)) = \delta_{ij}, \quad 1 \leq i,\ j \leq r,$$

completando así la demostración de la proposición. □

Teorema 3.6 *El mapa de descomposición d y la aplicación $e : \mathcal{K}_0(kG) \to G_0(KG)$ definida anteriormente son traspuestas con respecto a las formas bilineales i_K e i_k. Esto es,*

$$i_k(u,\ d(z)) = i_K(e(u),\ z), \quad \forall u \in \mathcal{K}_0(kG),\ z \in G_0(KG).$$

Demostración:
Basta demostrar que el resultado es cierto para los conjuntos de generadores de $\mathcal{K}_0(kG)$ y de $G_0(KG)$. Supongamos que $u = [U]$ y que $z = [Z]$, para módulos $U \in \mathcal{P}(kG)$ y $Z \in\ _{KG}mod$. Como el anillo RG es semiperfecto, podemos aplicar el isomorfismo definido en (3.5) y encontrar un kG-módulo proyectivo $P \in \mathcal{P}(kG)$ tal que $\bar{P} = U$. Entonces $e[U] = K \otimes_R P$. Supongamos que L es un RG-retículo completo de Z, entonces $d[Z] = [\bar{L}]$ en $G_0(KG)$. Por otro lado, tenemos el siguiente isomorfismo

$$K \otimes_R Hom_{RG}(P,\ L) \cong Hom_{KG}(K \otimes_R P,\ K \otimes_R L),$$

donde $Hom_{RG}(RG,\ L) \cong L$ como RG-módulos. Por tanto,

$$\overline{Hom_{RG}(RG,\ L)} \cong \bar{L} \cong Hom_{kG}(kG,\ \bar{L}).$$

Al ser P un módulo proyectivo y Hom aditivo, de la última igualdad se deduce que

$$\overline{Hom_{RG}(P,\ L)} \cong Hom_{kG}(\bar{P},\ \bar{L}).$$

Combinando estos resultados, obtenemos

$$\begin{aligned} i_K(e[U],\ [Z]) &= dim_K(Hom_{KG}(K \otimes_R P,\ K \otimes_R Z)) \\ &= dim_K(K \otimes_R Hom_{RG}(P,\ Z)) \\ &= dim_R(Hom_{RG}(P,\ Z)) \\ &= dim_k(Hom_{kG}(\bar{P},\ \bar{L})) \\ &= dim_k(Hom_{kG}(U,\ \bar{L})) \\ &= i_k([U],\ d[Z]), \end{aligned}$$

como se quería probar. □

Corolario 3.8 *Sea* $\mathbf{C}$ *la matriz de Cartan y* $\mathbf{D}$ *la matriz de descomposición de* G*, para un sistema* p*-modular* $(K,\ R,\ k)$*. Entonces* $\mathbf{C}$ *es una matriz simétrica, siendo*

$$\mathbf{C} = \mathbf{D^t D}.$$

Demostración:
Sea $\mathbf{E^t}$ la matriz de $e : \mathcal{K}_0(kG) \to G_0(KG)$, con respecto a las bases $\{U_i\}_{1\le i\le r}$ y $\{Z_j\}_{1\le j\le s}$. Usando una de las formas bilineales anteriores, se tiene que

$$d_{ij} = i_k([F_j],\ d[Z_i]) = i_k([U_j],\ d[Z_i]),$$

siendo $\{F_j\}_{1\le j\le r}$ un conjunto base de módulos simples en $G_0(kG)$ cuyas envolventes proyectivas son $\{U_i\}_{1\le i\le r}$ tales que $i_k([U_i],\ [F_j]) = \delta_{ij}$. Por el teorema anterior, tenemos que

$$d_{ij} = i_K(e[U_j],\ [Z_i]) = e_{ji}.$$

Luego, resulta que $\mathbf{D^t} = \mathbf{E}$. Por otro lado, el triángulo de Cartan-Brauer nos dice que $c = d_\circ e$; usando las definiciones de las matrices $\mathbf{C}$ y $\mathbf{D}$ se obtiene

$$\mathbf{C} = \mathbf{ED} = \mathbf{D^t D}.$$

Por tanto, $\mathbf{C^t} = \mathbf{C}$, lo cual completa la demostración. □

En un ejemplo anterior hemos dado la matriz de descomposición para $G = \mathbb{S}_4$ y el sistema modular $(\mathbb{Q},\ R_2,\ \mathbb{Z}_2)$:

$$\mathbf{D} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \\ 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

Luego, la matriz de Cartan está dada por $\mathbf{C} = \mathbf{D^t D}$ y es la siguiente:

$$\mathbf{C} = \begin{pmatrix} 4 & 2 \\ 2 & 3 \end{pmatrix}.$$

Corolario 3.9 *Supongamos que* p *no divide al orden de* G*. Entonces* $G = G_{p'}$*,* $r = s$*,* $\mathbf{C}$ *es la matriz identidad, y* $\mathbf{D}$ *es una matriz de permutación. Cada carácter de Brauer de un* kG*-módulo coincide con un carácter sobre* K *correspondiente a un* KG*-módulo.*

Demostración:
Si p no divide al orden del grupo, entonces el anillo kG es semisimple, y por tanto la cantidad de kG-módulos simples coincide con la cantidad de órbitas de conjugación de G. Por tanto, la cantidad de kG-módulos simples coincide con la cantidad de KG-módulos simples. Los conjuntos bases $\{[F_i]\}$, $\{[Z_j]\}$ de módulos simples en $G_0(kG)$ y en $G_0(KG)$, son ortonormales con respecto a las formas bilineales $i_k,\ i_K$, respectivamente. Como los coeficientes de $\mathbf{D}$ son enteros no negativos, la matriz de descomposición es una matriz de permutación, es decir que $\mathbf{D^t D} = \mathbf{I}$. Luego, se deduce del corolario anterior que $\mathbf{C} = I$. □

El siguiente resultado, además de interés en sí mismo, nos será de gran utilidad para encontrar más propiedades del triángulo de Cartan-Brauer. Como es usual, su demostración se puede encontrar en [C-R].

Teorema 3.7 *Sea λ_L un carácter de Brauer correspondiente a un kG-módulo L. Extendemos λ_L a una función de clases $\hat{\lambda}$ sobre todo G, por*

$$\widehat{\lambda_L}(x) = \lambda(s), \quad x \in G,$$

donde s es la parte p-regular de x. Entonces $\widehat{\lambda_L}$ es un carácter virtual de G sobre K.

□

Definición 53 *El carácter virtual $\hat{\lambda}$ sobre K, asociado al carácter de Brauer λ de G, se denomina el* **levantamiento de Brauer** *de λ.*

Corolario 3.10 *El mapa de descomposición $d : G_0(KG) \to G_0(kG)$, es suryectivo.*

Demostración:
Por la proposición 3.18, es suficiente probar que todo carácter de Brauer λ es la restricción de un elemento de $chKG$. Por el teorema anterior, sabemos que λ es la restricción $\hat{\lambda}|_{G_{p'}}$ de su levantamiento de Brauer $\hat{\lambda}$, puesto que se deduce inmediatamente de su definición. Por tanto, el mapa de descomposición es suryectivo. □

Corolario 3.11 *La aplicación $e : \mathcal{K}_0(kG) \to G_0(KG)$ es inyectiva.*

Demostración:
Sea $u \in ker\ e$. Entonces $i_K(e(u),\ z) = 0,\ \forall z \in G_0(KG)$. Al ser d la traspuesta de e, se tiene que $i_k(u,\ d(z)) = 0,\ \forall z \in G_0(KG)$. Como el mapa de descomposición d es suryectivo, debe ser que

$$i_k(u,\ v) = 0,\ \forall v \in G_0(kG).$$

Por (3.23), $G_0(kG)$ y $\mathcal{K}_0(kG)$ admiten bases duales con respecto a la forma bilineal i_k; luego, se deduce que $u = 0$, probando de esta manera que e es inyectivo. □

Como consecuencia inmediata del corolario anterior tenemos el siguiente resultado:

Corolario 3.12 *Supongamos que $P,\ P^{'} \in \mathcal{P}(RG)$ tal que los KG-módulos correspondientes $K \otimes_R P$ y $K \otimes_R P^{'}$ son isomorfos. Entonces $P \cong P^{'}$, como RG-módulos.*

□

3.6. Relaciones de ortogonalidad de los caracteres de Brauer

Antes de continuar con las propiedades de los caracteres de Brauer, recordamos que $(K,\ R,\ k)$ es un sistema p-modular, tal que $car\ K = 0$, K es suficientemente grande con respecto a G y RG es un anillo semiperfecto.

De aquí en adelante supondremos que $\{F_1, \ldots,\ F_r\}$ son representantes de las clases de isomorfismo de kG-módulos simples y que $\{\varphi^1, \ldots, \varphi^r\}$ son los caracteres de Brauer inducidos por estos módulos simples. Más aún, supondremos que $\{U_1, \ldots,\ U_r\}$ son los representantes de las clases de isomorfismo de KG-módulos proyectivos indescomponibles tal que U_i es la envolvente proyectiva de F_i, $1 \le i \le r$, y cuyos caracteres de Brauer están dados por $\{\nu^1, \ldots, \nu^r\}$. Los módulos U_i se denominan **módulos principales indescomponibles**. Siguiendo los razonamientos y la notación de la sección anterior, notaremos por $\{P_1, \ldots,\ P_r\}$ al conjunto base de RG-módulos proyectivos indescomponibles, tal que $\bar{P}_i = U_i$ y por $\{\mathcal{C}_j\}_{1\leq j\leq r}$ a las clases de conjugación de elementos p-regulares de G.

Luego, si $\{\chi_i\}_{1\leq i\leq s}$ son los caracteres irreducibles de los KG-módulos simples $\{V_i\}_{1\leq i\leq s}$, de (3.18) y de la estructura de los grupos de Grothendieck se deduce que

$$\chi_i|_{G_{p'}} = \textstyle\sum_{j=1}^r d_{ij}\varphi^j, \quad 1 \leq i \leq s,$$

$$\nu^i = \textstyle\sum_{j=1}^r c_{ij}\varphi^j, \quad 1 \leq i \leq s.$$

Entonces, si $\Phi = (\varphi^i(x_j))_{1\leq i,j\leq r}$, $\mathbf{H} = (\nu^i(x_j))_{1\leq i,j\leq r}$ y $\mathbf{Z} = (\chi_i(x_j)$, donde $x_j \in \mathcal{C}_j$, tenemos que

$$\mathbf{Z} = \mathbf{D\Phi}, \quad \mathbf{H} = \mathbf{C\Phi}.$$

Lema 3.5 *i) det* Φ *es una unidad de* R.

ii) det $\mathbf{C} \neq \mathbf{0}$.

Demostración:
Como k es un cuerpo de descomposición de G, por (3.2), los k-caracteres de $\{F_1, \ldots,\ F_r\}$ son linealmente independientes sobre k. Estos caracteres están determinados por las filas de $\bar{\Phi}$, por tanto, *det* $\bar{\Phi} \neq 0$. Como R es un anillo local con cuerpo residual k, tenemos que *det* Φ es una unidad de R, probando así *i)*. Para probar *ii)*, aplicando una de las relaciones de ortogonalidad del primer capítulo, obtenemos

$$\frac{1}{|G|}\sum_{m=1}^{s} \chi_i(x_m)\chi_j(x_m^{-1}) = (h_i^{-1}\delta_{ij}), \quad x_m \in \mathcal{C}_m.$$

Entonces, *det* $\mathbf{Z}^t\mathbf{Z} \neq 0$ y por las igualdades anteriores tenemos que

$$\mathbf{Z}^t\mathbf{Z} = \Phi^t\mathbf{D^tD\Phi} = \mathbf{\Phi^tC\Phi}.$$

Como *det* Φ es una unidad en R, tenemos que *det* $\mathbf{C} \neq \mathbf{0}$, como se quería probar. □

Teorema 3.8 Relaciones de ortogonalidad de los caracteres de Brauer

$$i)\ \textstyle\sum_{j=1}^r h_j\varphi^i(x_j)\nu^k(x_j^{-1}) = |G|\delta_{ik}, \quad x_j \in (C)_j,\ 1 \leq j \leq r.$$

$$ii)\ \textstyle\sum_{j=1}^r h_j\varphi^i(x_j)\varphi^k(x_j^{-1}) = |G|\gamma_{ik}, \quad \textit{donde } \mathbf{C^{-1}} = (\gamma_{\mathbf{ij}}).$$

$$iii)\ \textstyle\sum_{j=1}^r h_j\nu^i(x_j)\nu^k(x_j^{-1}) = |G|c_{ik}.$$

Demostración:
Por el lema y las igualdades anteriores sabemos que $\mathbf{C}$ es inversible y que

$$\mathbf{Z}^t\mathbf{Z} = \mathbf{Y},\ \mathbf{Z} = \mathbf{D\Phi},\ \mathbf{H} = \mathbf{C\Phi} = \mathbf{D^tZ},$$

donde $\mathbf{Y} = (|G|h_i^{-1}\delta_{ij})$. Por tanto, operando sobre estas igualdades se obtiene

$$\Phi\mathbf{Y}^{-1}\Phi^t = \mathbf{C^{-1}},\ \mathbf{\Phi Y^{-1}H^t} = \mathbf{I},\ \text{y}\ \mathbf{HY^{-1}H^t} = \mathbf{C}.$$

Se deduce inmediatamente que las fórmulas anteriores implican *ii)*, *i)* y *iii)*, respectivamente; completando así la demostración. $\square$

Daremos ahora una variación del levantamiento de Brauer, también sin demostración, que usaremos en la demostración de una de las propiedades de la matriz de Cartan.

Lema 3.6 *Sean $|G| = p^a \cdot m$, tal que p no divide a m, y λ un carácter de Brauer asociado a un kG-módulo L. Definimos*

$$\theta(x) = \begin{cases} p^a\lambda(x), & x \in G_{p'}, \\ \\ 0, & x \notin G_{p'}. \end{cases}$$

Entonces θ es un carácter virtual de G.

$\square$

Teorema 3.9 *Sea* $\mathbf{C}$ *la matriz de Cartan, entonces det* $\mathbf{C} = p^l$*, para algún entero no negativo l.*

Demostración:
Supongamos que $|G| = p^a \cdot m$, tal que p no divide a m, y sea $\theta_i \in ch\ KG$ el carácter virtual, definido en el lema anterior, que corresponde al carácter de Brauer irreducible $\varphi^i,\ 1 \leq i \leq r$. Luego, tenemos que

$$\theta_i = \sum_{j=i}^{s} a_{ij}\chi_j, \quad a_{ij} \in \mathbb{Z},\ 1 \leq i \leq r.$$

Más aún, tenemos que

$$\begin{aligned} a_{ij} &= (\theta_i,\ \chi_j) = \tfrac{1}{|G|}\textstyle\sum_{x\in G}\theta_i(x^{-1})\chi_j(x) \\ &= \tfrac{p^a}{|G|}\textstyle\sum_{x\in G_{p'}}\varphi^i(x^{-1})\chi_j(x) \\ &= \tfrac{p^a}{|G|}\textstyle\sum_{x\in G_{p'}}\varphi^i(x^{-1})\sum_{k=1}^{r} d_{jk}\varphi^k(x) \\ &= p^a\textstyle\sum_{k=1}^{r} d_{jk}\left\{|G|^{-1}\sum_{x\in G_{p'}}\varphi^i(x^{-1})\varphi^k(x)\right\} \\ &= p^a\textstyle\sum_{k=1}^{r} d_{jk}\gamma_{ki}, \quad \mathbf{C^{-1}} = (\gamma_{\mathbf{ij}}). \end{aligned}$$

Luego, si $\mathbf{A} = (a_{ij})$, como $\mathbf{C^{-1}}$ es simétrica, la igualdad anterior se traduce en

$$\mathbf{A} = p^a\mathbf{C^{-1}D^t}.$$

Entonces, por (3.8) tenemos que

$$\mathbf{AA}^t = p^{2a}\mathbf{C^{-1}D}^t\mathbf{DC^{-1}} = p^{2a}\mathbf{C^{-1}}.$$

Por tanto,

$$(det\ \mathbf{C})(det(\mathbf{AA}^t)) = p^{2a};$$

en particular, *det* $\mathbf{C}$ debe ser una potencia de p. $\square$

Definición 54 *Diremos que un elemento $x \in G$ es p-irregular si $x \notin G_{p'}$.*

Teorema 3.10 *Sea $\{P_1, \dots, P_r\}$ un conjunto base de RG-módulos proyectivos indescomponibles, y τ_i los caracteres sobre K inducidos por los KG-módulos $K \otimes_R P_i$, $1 \leq i \leq r$. Entonces*

i) $\tau_i = \sum_{j=i}^{s} d_{ji}\chi_i, \quad 1 \leq i \leq r.$

ii) $\tau_i(x) = 0$, *para todo elemento p-irregular $x \in G$.*

iii) $\{\tau_1, \dots, \tau_r\}$ *forma una base sobre $\mathbb{Z}$ de caracteres virtuales de G tales que se anulan en los elementos p-irregulares de G.*

Demostración:
Al ser $\bar{P}_i \cong U_i$, $1 \leq i \leq r$, debe ser que $\tau_i|_{G_{p'}} = \nu^i$. Luego, por (3.23) tenemos que

$$\begin{aligned} i_K([K \otimes_R P_i],\ [Z_j]) &= i_k([U_i],\ d[Z_j]) \\ &= i_k([U_i],\ \textstyle\sum_{h=1}^{r} d_{jh}[F_h]) \\ &= d_{ji}. \end{aligned}$$

Como τ_i es el carácter correspondiente al KG-módulo $K \otimes_R P_i$, debe ser que

$$(\tau_i,\ \chi_j) = d_{ji},$$

por la definición de la forma bilineal. Esto implica que

$$\tau_i = \sum_{j=1}^{s} d_{ji}\chi_j, 1 \leq i \leq r.$$

Se puede demostrar, usando la igualdad anterior, que $\{\tau_i\}$ es linealmente independiente; pero extendería demasiado la demostración y no aporta nuevas ideas. Los detalles se pueden ver [C-R]. Probaremos ahora que los caracteres τ_i se anulan en las clases p-irregulares de G. De las relaciones de ortogonalidad de los caracteres sobre K y de (3.8), se deduce que

$$\frac{1}{|G|}\sum_{x \in G} |\tau_i(x)|^2 = \sum_{j=1}^{s} d_{ji}^2 = c_{ii}.$$

Por otro lado, de las relaciones de ortogonalidad de los caracteres de Brauer, tenemos que

$$\frac{1}{|G|}\sum_{y \in G_{p'}} |\tau_i(y)|^2 = \frac{1}{|G|}\sum_{j=1}^{s} h_j \nu^i(x_j)\nu^i(x_j^{-1}) = c_{ii},$$

donde $x_j \in \mathcal{C}_j$. Comparando ambas igualdades, debe ser que $\tau_i = 0$ para todo $x \notin G_{p'}$.

Para terminar la demostración, debemos mostrar que todo carácter virtual $\theta \in ch\ KG$ que se anula en los elementos p-irregulares es combinación lineal a coeficientes en $\mathbb{Z}$ de $\{\tau_i\}$. Supongamos que

$$\theta = \sum a_i \tau_i,$$

y tratemos de encontrar los coeficientes $\{a_i\}$ en $\mathbb{Z}$. Por tanto, nuestro problema es resolver las ecuaciones

$$\theta(x_i) = \sum_{j=1}^{r} a_j \tau_j(x_i) = \sum_{j=1}^{r} a_j \nu_j(x_i), \text{ donde } x_i \in \mathcal{C}_i, \ 1 \leq i \leq r$$

Luego, la matriz de coeficientes es $\mathbf{H} = \mathbf{C\Phi}$ y es inversible, puesto que $\mathbf{C}$ y Φ lo son. Por tanto, basta demostrar que las soluciones $\{a_i\}$ son números enteros. De las relaciones de ortogonalidad de los caracteres de Brauer se tiene que

$$a_j = \frac{1}{|G|} \sum_{i=1}^{r} h_i \theta(x_i) \varphi^j(x_i^{-1}).$$

Como el mapa de descomposición es suryectivo (suponiendo que K es suficientemente grande), podemos suponer que

$$\varphi^j = \sum_{k=1}^{s} m_{jk} \chi_k,$$

para ciertos coeficientes $m_{jk} \in \mathbb{Z}$. Al ser θ un carácter virtual que se anula en los elementos p-irregulares, tenemos que

$$\begin{aligned} a_j &= \tfrac{1}{|G|} \textstyle\sum_{i=1}^{r} \sum_{k=1}^{s} h_i \theta(x_i) m_{jk} \chi_k(x_i^{-1}) \\ &= \textstyle\sum_{k=1}^{s} m_{jk} (\theta, \ \chi_k), \quad \in \mathbb{Z}, \end{aligned}$$

como se quería probar. □

Veamos ahora algunas propiedades adicionales del triángulo de Cartan-Brauer, que se deducen de lo hecho hasta el momento.

Proposición 3.24 *i) El morfismo de Cartan* $c : \mathcal{K}_0(kG) \to G_0(kG)$ *es inyectivo, y su conúcleo es un grupo finito cuyo orden es una potencia de* p.

ii) Im e *consiste en aquellos* $a \in G_0(KG)$ *cuyos caracteres virtuales* α *se anulan en las clases* p*-irregulares de* G.

iii) La aplicación $e : \mathcal{K}_0(kG) \to G_0(KG)$ *es una* **inyección directa***, esto es,* e *es una inyección y la imagen de* e *es un sumando directo sobre* $\mathbb{Z}$ *de* $G_0(KG)$.

□

Para finalizar este capítulo, daremos algunos ejemplos que muestran lo hecho hasta aquí. Algunos de ellos son un caso particular del teorema de Fong-Swan-Rukolaine, que enunciaremos al finalizar la sección.

3.6.1. Ejemplos

a) Sean $G = \mathbb{S}_4, \ p = 2$, y $(\mathbb{Q}_2, \ R, \ k)$ el sistema 2-modular tal que $\mathbb{Q}_2$ es la completación de $\mathbb{Q}$ con respecto a la valuación 2-ádica, R es el anillo de enteros 2-ádicos, y $k \cong R/2 \cdot R \cong \mathbb{Z}/2 \cdot \mathbb{Z}$. En los ejemplos anteriores vimos que hay exactamente dos clases de isomorfismos de $k\mathbb{S}_4$-módulos simples y que la matriz de descomposición y la matriz de Cartan eran las siguientes

$$\mathbf{D} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \\ 1 & 1 \\ 1 & 0 \end{pmatrix}, \quad \mathbf{C} = \begin{pmatrix} 4 & 2 \\ 2 & 3 \end{pmatrix}.$$

Como las clases de elementos 2-regulares son 2 y están dadas por las clases de id, $(1\ 2\ 3)$, la tabla de caracteres de Brauer será:

$k\mathbb{S}_4$	1	8
$\mathbb{S}_4$	$[id]$	$[1\ 2\ 3]$
F_1	1	-1
F_2	2	-1

.

Luego, los caracteres de G inducidos por los RG-módulos proyectivos indescomponibles son

$$\begin{aligned}
\tau_1 &= \textstyle\sum_{j=i}^{s} d_{j1}\chi_i = \chi_1 + \chi_2 + \chi_4 + \chi_5 \\
&= \chi^{(4)} + \chi^{(3,\ 1)} + \chi^{(2,\ 1^2)} + \chi^{(1^4)} \\
\tau_2 &= \textstyle\sum_{j=i}^{s} d_{j2}\chi_i = \chi_2 + \chi_3 + \chi_4 \\
&= \chi^{(3,\ 1)} + \chi^{(2,\ 2)} + \chi^{(2,\ 1^2)}.
\end{aligned}$$

Por tanto, hay dos $k\mathbb{S}_4$-módulos proyectivos indescomponibles $U_1,\ U_2$ de dimensión 8. A saber, la dimensión de U_i está dada por $\tau_i(1)$, entonces

$$\begin{aligned}
dim_k(U_1) &= \tau_1(1) = \chi^{(4)}(1) + \chi^{(3,\ 1)}(1) + \chi^{(2,\ 1^2)}(1) + \chi^{(1^4)}(1) \\
&= 1 + 3 + 3 + 1 = 8 \\
dim_k(U_2) &= \tau_2(1) = \chi^{(3,\ 1)}(1) + \chi^{(2,\ 2)}(1) + \chi^{(2,\ 1^2)}(1) \\
&= 3 + 2 + 3 = 8.
\end{aligned}$$

Mediante un simple cálculo, usando la tabla de caracteres de $\mathbb{S}_4$, se puede ver que efectivamente los caracteres τ_i se anulan en los elementos 2-irregulares. Por ejemplo, para τ_1 tenemos

$$\begin{aligned}
\tau_1(1,\ 2) &= \chi^{(4)}(1,\ 2) + \chi^{(3,\ 1)}(1,\ 2) + \chi^{(2,\ 1^2)}(1,\ 2) + \chi^{(1^4)}(1,\ 2) \\
&= 1 + 1 - 1 - 1 = 0 \\
\tau_1((1,\ 2)(3,\ 4)) &= 1 - 1 - 1 + 1 = 0 \\
\tau_1((1,\ 2,\ 3,\ 4)) &= 1 - 1 - 1 + 1 = 0.
\end{aligned}$$

b) Encontremos ahora la tabla de caracteres de Brauer de $G = \mathbb{S}_4$ para $p = 3$ y sistema modular $(\mathbb{Q}_3,\ R,\ k)$ tal que $\mathbb{Q}_3$ es la completación de $\mathbb{Q}$ con respecto a la valuación 3-ádica, R es el anillo de enteros 3-ádicos en $\mathbb{Q}$, y $k \cong R/3 \cdot R \cong \mathbb{Z}/3 \cdot \mathbb{Z}$. La cantidad de clases3-regulares en $\mathbb{S}_4$ es 4 y están dadas por $[id]$, $[1\ 2]$, $[(1\ 2)(3\ 4)]$ y $[1\ 2\ 3\ 4]$. Luego, tenemos 4 $k\mathbb{S}_4$-módulos simples cuyos caracteres son

	6	3	6	1
$\mathbb{S}_4$	$[1\ 2\ 3\ 4]$	$[(1\ 2)(3\ 4)]$	$[1\ 2]$	$[id]$
F_1	1	1	1	1
F_2	-1	-1	1	3
F_3	1	-1	-1	3
F_4	-1	1	-1	1

.

A través de un simple cálculo, se puede ver que la matriz de descomposición es la siguiente

$$\mathbf{D} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

En consecuencia, existen cuatro $k\mathbb{S}_4$-módulos proyectivos indescomponibles de dimensión 3, cuyos caracteres están dados por

$$\begin{aligned} \tau_1 &= \textstyle\sum_{j=i}^{s} d_{j1}\chi_i = \chi_1 + \chi_3 \\ &= \chi^{(4)} + \chi^{(2,\ 2)} \\ \tau_2 &= \textstyle\sum_{j=i}^{s} d_{j2}\chi_i = \chi_2 = \chi^{(3,\ 1)} \\ \tau_3 &= \textstyle\sum_{j=i}^{s} d_{j3}\chi_i = \chi_4 = \chi^{(2,\ 1^2)} \\ \tau_4 &= \textstyle\sum_{j=i}^{s} d_{j4}\chi_i = \chi_3 + \chi_5 \\ &= \chi^{(2,\ 2)} + \chi^{(1^4)}. \end{aligned}$$

c) Sean G un p-grupo, es decir, un grupo cuyo orden es una potencia de p, y $(K,\ R,\ k)$ un sistema p-modular con $car\ K = 0$ y K suficientemente grande. Luego, la cantidad de clases p-regulares es 1 y está dada por la unidad de G. Por tanto, la única clase de isomorfismos de kG-módulos simples está dada por la reducción de la representación trivial de G sobre K; esto es, los elementos de G actúan trivialmente sobre el único (salvo isomorfismos) kG-módulo simple.

d) Sea $(K,\ R,\ k)$ un sistema p-modular tal que $car\ K = 0$, K suficientemente grande y RG es un anillo semiperfecto. Si G es un grupo finito cuyo orden es coprimo con p, se tiene lo siguiente:

i) Los kG-módulos simples $\{F_i,\ 1 \leq i \leq r\}$ coinciden con los kG-módulos proyectivos indescomponibles $\{U_i,\ 1 \leq i \leq r\}$.

ii) Para cada i, $1 \leq i \leq r$, existe un RG-retículo proyectivo P_i tal que $\bar{P}_i = F_i$.*iii)* Para cada i, $KP_i = K \otimes_R P_i$ es un KG-módulo simple tal que $d[KP_i] = [F_i]$.

iv) Los módulos $\{KP_i,\ 1 \leq i \leq r\}$ son una base de KG-módulos simples.

Demostración:
Al ser $(|G|,\ p) = 1$, resulta que el anillo kG es semisimple. Por tanto, toda sucesión exacta de kG-módulos se parte; en particular, todos los kG-módulos simples son proyectivos. Como la envolvente proyectiva es única salvo isomorfismos, se tiene que $\{F_i,\ 1 \leq i \leq r\}$ es una base de kG-módulos proyectivos indescomponibles que coincide con $\{U_i,\ 1 \leq i \leq r\}$.

Sea $\overline{RG} = RG/(rad\ RG)$. Como este anillo es semisimple y artiniano, tiene una descomposición

$$\overline{RG} \cong \overline{RG}e_1 \oplus \cdots \oplus \overline{RG}e_n,$$

donde $\{e_i\}$ es un conjunto de idempotentes primitivos. Al ser RG un anillo semiperfecto, esta descomposición se levanta a una descomposición de RG

$$RG \cong RGe_1 \oplus \cdots \oplus RGe_n,$$

resultando RGe_i un RG-módulo proyectivo indescomponible. Más aún, RGe_i es un RG-retículo. Sea $P_i = RGe_i$. Entonces $\bar{P_i} = P_i/\wp P_i \cong kG\bar{e_i}$ es un kG-módulo simple, puesto que $\wp G \subseteq rad\ RG$ y su envolvente proyectiva P_i es un módulo indescomponible. Por tanto, debe ser que $\bar{P_i} \cong F_j$, para algún $j,\ 1 \leq j \leq r$. Reordenando, podemos suponer que $\bar{P_i} \cong F_i$, obteniendo de esta manera *ii).* Consideremos ahora el KG-módulo dado por $K \otimes_R P_i = KP_i$. Entonces, por la definición del mapa de descomposición, tenemos que

$$d[K \otimes_R P_i] = [\bar{P_i}] = [F_i].$$

Esto implica que el único factor de composición de KP_i es F_i, es decir que KP_i es un KG-módulo simple. Como la cantidad de KG-módulos simples es igual a la cantidad de kG-módulos simples que es igual a la cantidad de clases de conjugación de G, se deduce que $\{KP_i,\ 1 \leq i \leq r\}$ es una base de KG-módulos simples.

□

Observar que, en los dos últimos ejemplos, todo kG-módulo simple se obtiene por reducción módulo $\wp$ de algún KG-módulo simple. Esto ocurre en una situación un poco más general:

Definición 55 *Un grupo finito G se dice p-soluble si cada factor de la serie de composición de G es un p-grupo o su orden es coprimo con p.*

Teorema 3.11 Fong-Swan-Rukolaine*Sea F un kG-módulo simple, donde G es un grupo finito p-soluble. Existe entonces un KG-módulo simple Z tal que $F \cong Z_0/\wp Z_0$, para cada RG-retículo completo Z_0 en Z.*

□

Capítulo 4

Representaciones modulares del grupo simétrico

En esta sección describiremos representaciones modulares de algunos grupos simétricos, debido a que la completa clasificación de módulos de Specht irreducibles sobre un cuerpo de característica positiva es aún un problema abierto. Actualmente, no existe una manera de determinar los factores de composición para un módulo de Specht general cuando el cuerpo de base es de característica positiva. Por tanto, no se pueden determinar los coeficientes de la matriz de descomposición de $\mathbb{S}_n$, excepto en algunos casos especiales. Mantendremos la notación introducida en el capítulo 2 a lo largo de toda esta sección.

En el capítulo 2 hemos construido las representaciones irreducibles S^μ de $\mathbb{S}_n$ sobre un cuerpo de característica cero; correspondiendo cada módulo simple a una clase de conjugación de $\mathbb{S}_n$. Nos proponemos ahora encontrar la representación modular que se obtiene de éstas al considerar el sistema modular $(\mathbb{Q}_p,\ R,\ \mathbb{F}_p)$, donde $\mathbb{Q}_p$ es la completación de $\mathbb{Q}$ respecto de la valuación p-ádica, R es el anillo de enteros p-ádicos y $\mathbb{F}_p \cong \mathbb{Z}/p \cdot \mathbb{Z}$ es el cuerpo de p elementos.

Proposición 4.1 *Si $v \in S^\mu_{\mathbb{Q}}$ y los coeficientes de los tabloides involucrados en v son todos enteros, entonces v es una combinación lineal con coeficientes en $\mathbb{Z}$ de politabloides estándar.*

Demostración:
Si $v = 0$, no hay nada que probar. Supongamos que $v \neq 0$ y ordenemos los tabloides involucrados en v de menor a mayor según el orden parcial $<$ definido en (23). Sea $\{t\}$ el último tabloide involucrado en v, digamos con coeficiente $a \in \mathbb{Z}$. Por la proposición 2.9, sabemos que dicho tabloide debe ser estándar. Ahora, el lema 2.5 muestra que el último tabloide involucrado en $v - a \cdot e_t$ está antes del tabloide $\{t\}$. Luego, por inducción, tenemos que $v - a \cdot e_t$ es una combinación lineal con coeficientes en $\mathbb{Z}$ de politabloides estándar. Por tanto, v debe ser una combinación lineal con coeficientes enteros de politabloides estándar. $\square$

Corolario 4.1 *Si $v \in S^\mu_{\mathbb{Q}}$ y los coeficientes de los tabloides involucrados en v son todos enteros, entonces podemos reducir todos los coeficientes módulo p y obtener un elemento de $S^\mu_{\mathbb{F}_p}$, donde $\mathbb{F}_p$ es el cuerpo de p elementos.*

Demostración:
Por la proposición anterior, v es una combinación lineal con coeficientes enteros de politabloides estándar,

digamos

$$v = \sum a_i \cdot e_i, \quad a_i \in \mathbb{Z}.$$

Reduciendo módulo p todos los coeficientes de los tabloides en v, obtenemos $\bar{v}$. Sea $\bar{a}_i$ la reducción de a_i, entonces

$$\bar{v} = \sum \bar{a}_i \cdot e_i, \quad a_i \in \mathbb{Z},$$

muestra que $\bar{v} \in S^{\mu}_{\mathbb{F}_p}$. □

Observación: Dada la base de politabloides estándar $\{e_t\}$ de $S^{\mu}_{\mathbb{Q}}$ y el sistema modular $(\mathbb{Q}_p,\ R,\ \mathbb{F}_p)$, podemos construir un $R\mathbb{S}_n$-retículo completo M de $S^{\mu}_{\mathbb{Q}}$ dado por

$$M = \sum R\mathbb{S}_n \cdot e_t, \quad e_t \text{ politabloide estándar.}$$

Sabemos que $S^{\mu}_{\mathbb{Q}}$ está generado por cualquier politabloide estándar bajo la acción de $\mathbb{S}_n$, es decir que $S^{\mu}_{\mathbb{Q}}$ es un módulo cíclico. Entonces, debe ser que

$$M = \sum R \cdot e_t, \quad e_t \text{ politabloide estándar.}$$

Supongamos que $\wp \subset R$ es el único ideal maximal del anillo de valuación discreto R. Luego, $\wp = p \cdot R$ y $R/\wp \cong \mathbb{F}_p$. Por tanto, el $\mathbb{F}_p$-módulo $\bar{M}$ que se obtiene por reducción módulo $\wp$, es el módulo $S^{\mu}_{\mathbb{F}_p}$, cuyos elementos son combinaciones lineales sobre $\mathbb{F}_p$ de los politabloides estándar. Esto da lugar al siguiente corolario:

Corolario 4.2 *Si $\mathbb{F}_p$ es el cuerpo de p elementos, entonces $S^{\mu}_{\mathbb{F}_p}$ es la representación p-modular de $\mathbb{S}_n$ que se obtiene de $S^{\mu}_{\mathbb{Q}}$.*

□

Observación: Por los resultados anteriores, se deduce que los politabloides se pueden escribir como combinación lineal de politabloides estándar sobre cualquier cuerpo. Por tanto, los politabloides estándar generan S^{μ} sobre cualquier cuerpo.

Lema 4.1 *Supongamos que $\theta \in Hom_{\mathbb{Q}\mathbb{S}_n}(M^{\lambda}_{\mathbb{Q}},\ M^{\mu}_{\mathbb{Q}})$ y que todos los tabloides involucrados en $\theta\{t\}$ tienen coeficientes enteros, donde $\{t\} \in M^{\lambda}_{\mathbb{Q}}$. Entonces, la reducción de todos los coeficientes módulo p da un elemento no nulo $\bar{\theta} \in Hom_{\mathbb{F}_p\mathbb{S}_n}(M^{\lambda}_{\mathbb{F}_p},\ M^{\mu}_{\mathbb{F}_p})$, donde $\mathbb{F}_p$ es el cuerpo de p elementos. Si $Ker\ \theta = {S^{\lambda}_{\mathbb{Q}}}^{\perp}$, entonces $Ker\ \bar{\theta} \supseteq {S^{\lambda}_{\mathbb{F}_p}}^{\perp}$.*

Demostración:
Es claro que si θ es un morfismo de $\mathbb{Q}\mathbb{S}_n$-módulos tal que los tabloides de $\theta\{t\}$ tienen coeficientes enteros para todo $\{t\} \in M^{\lambda}_{\mathbb{Q}}$, entonces $\bar{\theta} \in Hom_{\mathbb{F}_p\mathbb{S}_n}(M^{\lambda}_{\mathbb{F}_p},\ M^{\mu}_{\mathbb{F}_p})$. Para demostrar la segunda afirmación, tomemos una base $f_1, \ldots,\ f_k$ de ${S^{\lambda}_{\mathbb{Q}}}^{\perp}$ y extendámosla a una base de $M^{\lambda}_{\mathbb{Q}}$ agregando una base de politabloides estándar de $S^{\lambda}_{\mathbb{Q}}$. Recordemos que esto es posible debido a que ${S^{\lambda}_{\mathbb{Q}}}^{\perp} \cap S^{\lambda}_{\mathbb{Q}} = 0$. Sean $\{t_1\}, \ldots \{t_m\}$ los diferentes tabloides de λ. Definimos la matriz $\mathbf{N}$ por

$$n_{ij} \ = < f_i,\ \{t_j\} > .$$

Habiendo elegido convenientemente la base, podemos suponer que los coeficientes de **N** son enteros; más aún, por reducción en las primeras k filas también podemos suponer que las primeras k filas de **N** son linealmente independientes sobre $\mathbb{F}_p$.

Reduciendo todos los coeficientes de **N** módulo p, obtenemos un conjunto de vectores en $M^{\lambda}_{\mathbb{F}_p}$, donde los últimos $m-k$ vectores son una base estándar de $S^{\lambda}_{\mathbb{F}_p}$, y los primeros k son linealmente independientes y ortogonales a la base estándar de $S^{\lambda}_{\mathbb{F}_p}$. Como la dimensión de S^{λ} es independiente del cuerpo de base, tenemos que

$$dim\ {S^{\lambda}_{\mathbb{F}_p}}^{\perp} = dim\ M^{\lambda}_{\mathbb{F}_p} - dim\ S^{\lambda}_{\mathbb{F}_p} = k.$$

Luego, hemos construido una base de ${S^{\lambda}_{\mathbb{Q}}}^{\perp}$ cuyos elementos dan una base de $S^{\lambda}_{\mathbb{F}_p}$ cuando los coeficientes de los tabloides se reducen módulo p.

Si $Ker\ \theta = {S^{\lambda}_{\mathbb{Q}}}^{\perp}$, entonces todo elemento f_j de la base de ${S^{\lambda}_{\mathbb{Q}}}^{\perp}$ es combinación lineal a coeficientes enteros de tabloides de λ y θ lo anula. Por tanto, cuando reducimos todos los coeficientes de $\theta(f_j)$ módulos p, éstos deben ser cero. Es decir, $Ker\ \bar{\theta} \supseteq {S^{\lambda}_{\mathbb{F}_p}}^{\perp}$. □

Antes de finalizar esta sección, daremos un teorema que extiende al teorema 2.7 dando el mismo resultado sobre cualquier cuerpo de base.

Teorema 4.1 *Sobre cualquier cuerpo, $S^{\lambda} \otimes S^{(1^n)}$ es isomorfo al dual de $S^{\lambda'}$, siendo λ' la partición conjugada de λ.*

Demostración:
Basta con demostrar el caso cuando el cuerpo de base es $\mathbb{F}_p$, el cuerpo de p elementos, puesto que hemos demostrado el resultado cuando el cuerpo de base es $\mathbb{Q}$.

En la demostración del teorema 2.7, dimos un $\mathbb{Q}\mathbb{S}_n$-morfismo θ de $M^{\lambda'}_{\mathbb{Q}}$ en $M^{\lambda}_{\mathbb{Q}} \otimes M^{(1^n)}_{\mathbb{Q}}$ y probamos que $Ker\ \theta = (S^{\lambda'}_{\mathbb{Q}})^{\perp}$. Usando el lema anterior, definimos $\bar{\theta}$ por

$$\bar{\theta} : \{\pi t\} \mapsto sg(\pi)\kappa_{\pi t}\{\pi t\} \otimes u.$$

Luego, $\bar{\theta}$ es un $\mathbb{F}_p\mathbb{S}_n$-morfismo en $S^{\lambda}_{\mathbb{F}_p} \otimes S^{(1^n)}_{\mathbb{F}_p}$ y, por el teorema anterior, su núcleo contiene a $(S^{\lambda'}_{\mathbb{F}_p})^{\perp}$. Por dimensiones, debe ser que $Ker\ \bar{\theta} = (S^{\lambda'}_{\mathbb{F}_p})^{\perp}$. Por tanto,

$$S^{\lambda}_{\mathbb{F}_p} \otimes S^{(1^n)}_{\mathbb{F}_p} \cong M^{\lambda}_{\mathbb{F}_p}/Ker\ \bar{\theta} = M^{\lambda}_{\mathbb{F}_p}/(S^{\lambda'}_{\mathbb{F}_p})^{\perp} \cong (S^{\lambda'}_{\mathbb{F}_p})^{*}.$$

□

4.1. Particiones p-regulares

Hemos visto que $S^{\mu}/(S^{\mu} \cap {S^{\mu}}^{\perp})$ es cero o absolutamente irreducible, y sólo puede ser cero si el cuerpo de base tiene característica positiva. Para distinguir entre las particiones μ tales que S^{μ} está contenido en ${S^{\mu}}^{\perp}$ y aquéllas que no lo verifican, debemos hacer algunas definiciones.

Definición 56 *Sea p un número primo. Una partición μ se dice p-**singular** si para algún i se tiene que*

$$\mu_{i+1} = \mu_{i+2} = \cdots = \mu_{i+p} > 0.$$

De lo contrario, la partición μ se denomina p**-regular**.

Por ejemplo, la partición $\mu = (6^2,\ 5^4,\ 1)$ es p-regular si y sólo si $p \geq 5$.

Lema 4.2 *El número de clases p-regulares de $\mathbb{S}_n$ es igual al número de particiones p-regulares de n.*

Demostración:
Sea $\pi \in \mathbb{S}_n$, y supongamos que está descompuesta como producto de ciclos disjuntos. Luego, es claro que π tiene orden coprimo con p si y sólo si ningún ciclo tiene longitud divisible por p. Por tanto, el número de clases p-regulares de $\mathbb{S}_n$ es igual al número de particiones μ de n tales que ningún sumando μ_i es divisible por p.

Consideremos el siguiente cociente

$$\frac{(1-x^p)(1-x^{2p})\cdots}{(1-x)(1-x^2)\cdots}.$$

Si cancelamos los factores $(1-x^{mp})$ en el numerador y en el denominador, tenemos que el cociente es

$$\prod_{p\not| i}(1-x^i)^{-1} = \prod_{p\not| i}(1+x^i+(x^i)^2+(x^i)^3\cdots),$$

siendo el coeficiente de x^n el número de particiones de n tales que ningún sumando es divisible por p; es decir, la partición $(\ldots,\ 3^c,\ 2^b,\ 1^a)$ corresponde a tomar el monomio dado por $x^a\cdot(x^2)^b\cdot(x^3)^c\cdots$.

Por otra parte, si para cada m separamos en el numerador $(1-x^{mp})$ y $(1-x^m)$ en el denominador, tenemos que

$$\begin{aligned}\tfrac{(1-x^p)(1-x^{2p})\cdots}{(1-x)(1-x^2)\cdots} &= \textstyle\prod_m \tfrac{(1-x^{mp})}{(1-x^m)}\\ &= \textstyle\prod_m(1+x^m+(x^m)^2\cdots+(x^m)^{p-1}).\end{aligned}$$

Aquí cada coeficiente de x^n es el número de particiones de n tales que ningún sumando se repite p veces o más; en particular, este coeficiente es la cantidad de particiones p-regulares de n.

Por tanto, comparando los coeficientes de x^n, se deduce que la cantidad de particiones p-regulares de n es igual a la cantidad de clases p-regulares de $\mathbb{S}_n$. $\square$

Análogamente al capítulo 2, gran parte da las propiedades de los módulos simples estudiados se deducen de resultados combinatorios. Observar que en dichos resultados no se pide que p sea primo, sin embargo esa suposición se debe hacer cuando se trabaja en teoría de representaciones.

Definición 57 *Sea g^μ el entero definido por*

$$g^\mu = M.C.D.\{< e_t,\ e_{t^*} >: e_t,\ e_{t^*} \text{ son politabloides en } S^\mu_{\mathbb{Q}}\}.$$

Como todo politabloide de S^μ es combinación lineal con coeficientes enteros de politabloides estándar, resulta que g^μ es el máximo común divisor de los coeficientes de la matriz de Gram con respecto a una base estándar del módulo de Specht S^μ.

Lema 4.3 *Supongamos que la partición μ tiene z_j sumandos iguales a j. Entonces $\prod_{j=1}^{\infty} z_j!$ divide a g^μ y g^μ divide a $\prod_{j=1}^{\infty}(z_j!)^j$.*

Observación: Como $0! = 1$, no hay problemas en tomar infinitos productos en $\prod_{j=1}^{\infty} z_j!$.

Demostración:
Definamos una relación de equivalencia $\sim$ sobre el conjunto de tabloides de μ por: $\{t_1\} \sim \{t_2\}$ si y sólo si para todo par $i,\ j$ que pertenece a la misma fila de $\{t_1\}$, entonces $i,\ j$ pertenecen a la misma fila de $\{t_2\}$. Es decir, $\{t_2\}$ se obtiene a partir $\{t_1\}$ intercambiando filas. Cada clase de equivalencia tiene orden $\prod_{j=i}^{\infty} z_j!$.

Si $\{t_1\}$ está involucrado en e_t y $\{t_1\} \sim \{t_2\}$, entonces la definición de politabloides muestra que $\{t_2\}$ está involucrado en e_t, siendo los coeficientes de ambos iguales o uno el inverso de otro. Por tanto, cualquier par de politabloides tienen un múltiplo de $\prod_{j=i}^{\infty} z_j!$ tabloides en común; en particular $\prod_{j=i}^{\infty} z_j!$ divide a g^{μ}. Sean t un tablero de μ y t^* el tablero de μ que se obtiene revirtiendo el orden de los coeficientes en cada fila del tablero t. Por ejemplo, si

$$t = \begin{array}{|c|c|c|c|} \hline 1 & 2 & 3 & 4 \\ \hline 5 & 6 \\ \cline{1-2} 7 & 8 \\ \cline{1-2} 9 \\ \cline{1-1} \end{array} \quad , \quad \text{entonces } t^* = \begin{array}{|c|c|c|c|} \hline 4 & 3 & 2 & 1 \\ \hline 6 & 5 \\ \cline{1-2} 8 & 7 \\ \cline{1-2} 9 \\ \cline{1-1} \end{array} \quad .$$

Sea π un elemento del estabilizador de columnas de t tal que para todo i, los números i y $\pi(i)$ pertenecen a filas de t que tienen el mismo tamaño. En el ejemplo anterior, π se puede tomar como cualquier elemento del subgrupo $\mathbb{S}_{\{5,\ 7\}} \times \mathbb{S}_{\{6,\ 8\}}$. Luego, $\{\pi t\}$ es un tabloide que está involucrado en e_t y en e_{t^*} con el mismo coeficiente. Es claro que todos los tabloides que tienen en común e_t y e_{t^*} tienen esta forma. Por tanto, $< e_t,\ e_{t^*} > = \prod_{j=i}^{\infty} (z_j!)^j$; en particular, se deduce que g^{μ} divide a $\prod_{j=i}^{\infty} (z_j!)^j$. En el ejemplo anterior, tenemos que $z_j = 2$ que $j = 2$, entonces $2! = 2/g^{\mu}$ y $g^{\mu}/2^2$. $\square$

Corolario 4.3 *El primo p divide a g^{μ} si y sólo si μ es p-singular.*

Demostración:
μ es p-singular si y sólo si p divide a $z_j!$ para algún j. Por el lema anterior, esto ocurre si y sólo si p divide a g^{μ}. $\square$

Corolario 4.4 *Si t^* se obtiene a partir de un tablero t de μ cambiando de orden los números en cada fila de t, entonces $\kappa_t e_{t^*}$ es un múltiplo de e_t, y este múltiplo es coprimo con p si y sólo si μ es p-regular.*

Demostración:
El corolario 2.3 muestra que $\kappa_t e_{t^*}$ es un múltiplo de e_t, digamos $\kappa_t e_{t^*} = h \cdot e_t$. Entonces

$$\begin{aligned} h = h < e_t,\ \{t\} > \ &= < he_t,\ \{t\} > = < \kappa_t e_{t^*},\ \{t\} > \\ &= < e_{t^*},\ \kappa_t\{t\} > = < e_{t^*},\ e_t > . \end{aligned}$$

Por la demostración del lema anterior sabemos que $h = \prod_{j=1}^{\infty} (z_j!)^j$. Por tanto, p divide a h si y sólo si p divide a $\prod_{j=1}^{\infty} (z_j!)^j$ si y sólo si μ es p-singular. $\square$

Sean μ una partición de n y μ' la partición conjugada de μ. Recordemos que

$$\kappa_t = \sum_{\pi \in C_t} sg(\pi)\pi, \text{ y } \rho_t = \sum_{\pi \in R_t} \pi,$$

donde $C_t \subseteq \mathbb{S}_n$ es el estabilizador de columnas y $R_t \subseteq \mathbb{S}_n$ es el estabilizador de filas.

Lema 4.4 *Supongamos que el cuerpo de base es* $\mathbb{Q}$ *y sea* t *un tablero de* μ*. Entonces*

i) El máximo común divisor de los coeficientes de los tabloides involucrados en $\rho_t\kappa_t\{t\}$ *es* $g^{\mu'}$*.*

ii) $\kappa_t\rho_t\kappa_t\{t\} = \prod(\textit{longitud de ganchos en } [\mu])\kappa_t\{t\}$*.*

Demostración:
Por definición, sabemos que

$$g^{\mu'} = M.C.D.\{< e_{t'},\ \pi e_{t'} > : e_{t'} \text{ es un politabloide estándar y } \pi \in \mathbb{S}_n\}.$$

Pero

$$\begin{aligned} sg(\pi) < e_{t'},\ \pi e_{t'} > &= sg(\pi) < \{t'\},\ \kappa_{t'}\pi\kappa_{t'}\{t'\} > \\ &= \sum\{sg(\pi)sg(\sigma)sg(\tau) :\ \sigma,\ \tau \in C_{t'},\ \tau\pi\sigma \in R_{t'}\} \\ &= \sum\{sg(\omega) :\ \tau \in C_{t'},\ \pi^{-1}\tau^{-1}\omega \in R_{t'}\} \\ &= \sum\{sg(\omega) :\ \tau \in R_t,\ \pi^{-1}\tau^{-1}\omega \in C_t\} \\ &=< \{t\},\ \pi^{-1}\rho_t\kappa_t\{t\} > \\ &=< \pi\{t\},\ \rho_t\kappa_t\{t\} > . \end{aligned}$$

Luego, $g^{\mu'}$ es el máximo común divisor de los politabloides involucrados en $\rho_t\kappa_t\{t\}$.

El corolario 2.3 muestra que $\kappa_t\rho_t\kappa_t\{t\} = c\kappa_t\{t\}$, para algún $c \in \mathbb{Q}$. Para encontrar el valor de c, trabajaremos sobre el álgebra de grupo $\mathbb{Q}\mathbb{S}_n$. Tenemos entonces que

$$\kappa_t\rho_t\kappa_t\rho_t = c\kappa_t\rho_t \quad \text{ en } \mathbb{Q}\mathbb{S}_n.$$

Por otro lado, debido al teorema de Maschke, el ideal a izquierda $\mathbb{Q}\mathbb{S}_n \cdot \kappa_t\rho_t$ de $\mathbb{Q}\mathbb{S}_n$, que es isomorfo a S^μ, tiene un ideal a izquierda complementario U. Esto es, $\mathbb{Q}\mathbb{S}_n = U \oplus \mathbb{Q}\mathbb{S}_n \cdot \kappa_t\rho_t$. Luego, la multiplicación a derecha por $\kappa_t\rho_t$ da una transformación lineal de $\mathbb{Q}\mathbb{S}_n$. Si tomamos una base de $\mathbb{Q}\mathbb{S}_n \cdot \kappa_t\rho_t$ seguida por una base de U, la matriz de la transformación lineal está representada por

$$\begin{pmatrix} c & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & c & \dots & 0 & 0 & \dots & 0 \\ \vdots & & \ddots & \vdots & \vdots & & \vdots \\ 0 & \dots & \dots & c & 0 & \dots & 0 \\ * & * & * & * & \vdots & & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots \\ * & * & * & * & 0 & \dots & 0 \end{pmatrix}.$$

En cambio, si tomamos la base natural $\{\pi :\ \pi \in \mathbb{S}_n\}$ para $\mathbb{Q}\mathbb{S}_n$, la transformación lineal estará representada por una matriz con unos en la diagonal, puesto que la identidad ocurre una sola vez en el producto $\kappa_t\rho_t$ con coeficiente 1.

Comparando las trazas, tenemos que $c \cdot dim\ S^\mu = n!$. Por la fórmula (2.5) para el módulo de Specht S^μ, sabemos que

$$dim\ S^\mu = \frac{n!}{\prod(\text{longitud de los ganchos en } [\mu])}.$$

Por tanto, se tiene que

$$c = \prod(\text{longitud de los ganchos en } [\mu]),$$

como se quería demostrar. $\square$

4.2. Representaciones irreducibles

En el capítulo 2 hemos construído las representaciones irreducibles sobre un cuerpo de característica cero. Ahora, construiremos las representaciones irreducibles de $\mathbb{S}_n$ sobre un cuerpo de característica positiva.

Teorema 4.2 *Sea K un cuerpo de característica positiva. El cociente $S^\mu/(S^\mu \cap S^{\mu\perp})$ es no nulo si y sólo si μ es p-regular.*

Demostración:
$S^\mu \subseteq S^{\mu\perp}$ si y sólo si $< e_t,\ e_{t^*} >= 0$ en K, para cada par de politabloides $e_t,\ e_{t^*}$ en S^μ. Pero esto ocurre si y sólo si p divide a $< e_t,\ e_{t^*} >$ para todo par de politabloides; es decir, si y sólo si p divide a g^μ. Por el corolario 4.3, sabemos que p divide a g^μ si y sólo si μ es una partición p-singular. Por tanto, se deduce que $S^\mu/(S^\mu \cap S^{\mu\perp})$ es no nulo si y sólo si μ es p-regular. $\square$

Definición 58 *Sean K un cuerpo de característica p y μ una partición p-regular. Definimos entonces D^μ_K como*

$$D^\mu_K = S^\mu_K/(S^\mu_K \cap S^{\mu\perp}_K).$$

Probaremos que todos los $K\mathbb{S}_n$-módulos irreducibles están dados por los módulos D^μ_K. Para demostrar que dos de estos módulos no son isomorfos necesitamos el siguiente lema, el cual nos dice que S^λ tiene imagen nula por cualquier elemento de $Hom_{K\mathbb{S}_n}(M^\lambda,\ M^\mu)$, salvo que $\lambda \geq \mu$.

Análogamente al capítulo 2, omitiremos el subíndice K cuando los resultados son independientes del cuerpo de base.

Lema 4.5 *Sean λ y μ dos particiones de n, tal que λ es una partición p-regular. Supongamos que U es un submódulo de M^μ y que θ es un $K\mathbb{S}_n$-morfismo no nulo de S^λ en M^μ/U. Entonces $\lambda \geq \mu$ y si $\lambda = \mu$, entonces $Im\ \theta \subset (S^\mu + U)/U$.*

Demostración:
Sean t un tablero de λ, t^* el tablero de λ que se obtiene invirtiendo el orden de los números en las filas de t. Por el corolario 4.4, tenemos que

$$\kappa_t e_{t^*} = h e_t, \quad \text{donde } h \neq 0.$$

Como θ es un $K\mathbb{S}_n$-morfismo, tenemos que

$$\theta(h e_t) = \theta(\kappa_t e_{t^*}) = \kappa_t \theta(e_{t^*}).$$

Al ser $h \neq 0$, tenemos que $\kappa_t \theta(e_{t^*}) \neq 0$. El lema 2.2 nos dice que $\lambda \geq \mu$, y si $\lambda = \mu$ entonces

$$\theta(e_t) = h^{-1}\kappa_t \theta(e_{t^*}) = \text{ un múltiplo de } e_t + U \in (S^\mu + U)/U.$$

Por tanto, $Im\ \theta \subset (S^\mu + U)/U$ si $\lambda = \mu$, puesto que e_t genera S^λ como módulo cíclico.

$\square$

Corolario 4.5 *Sean λ y μ dos particiones de n, tal que λ es una partición p-regular. Supongamos que U es un submódulo de M^μ y que θ es un $K\mathbb{S}_n$-morfismo no nulo de D^λ en M^μ/U. Entonces $\lambda \geq \mu$ y $U \supseteq S^\mu$.*

Demostración:
El morfismo θ se puede levantar a un elemento de $Hom_{K\mathbb{S}_n}(S^\lambda,\ M^\mu/U)$ definido por

$$S^\lambda \longrightarrow S^\lambda/(S^\lambda \cap S^{\lambda\perp}) \xrightarrow{\theta} M^\mu/U .$$

Por el lema anterior, debe ser que $\lambda \geq \mu$. Si $\lambda = \mu$, entonces $Im\ \theta$ es un submódulo no nulo de $(S^\mu + U)/U$, por tanto U no puede contener a S^μ. En consecuencia, si $U \subseteq S^\mu$ entonces $\lambda > \mu$. $\square$

Teorema 4.3 *Supongamos que el cuerpo de base K tiene característica positiva p. Los $K\mathbb{S}_n$-módulos D^μ tales que μ es una partición p-regular, forman un conjunto completo de $K\mathbb{S}_n$-módulos irreducibles no isomorfos. Cada D^μ es absolutamente irreducible y es isomorfo a su dual. En particular, todo cuerpo es un cuerpo de descomposición de $\mathbb{S}_n$.*

Demostración:
Los teoremas 2.2 y 4.2 muestran que D^μ es absolutamente irreducible y que es isomorfo a su dual.

Supongamos que $D^\mu \cong D^\lambda$. Entonces tenemos un $K\mathbb{S}_n$-morfismo no nulo de D^λ en $M^\mu/(S^\mu \cap S^{\mu\perp})$; luego, por el corolario anterior tenemos que $\lambda \leq \mu$. Análogamente, tenemos que $\mu \leq \lambda$, y por tanto $\lambda = \mu$. En particular, la cantidad de $K\mathbb{S}_n$-módulos D^μ es igual a la cantidad de particiones p-regulares μ. Falta demostrar que éstas son todas las representaciones irreducibles de $\mathbb{S}_n$ sobre K. Para ello, basta ver que $\mathbb{Q}$ es cuerpo de descomposición de $\mathbb{S}_n$: como todo cuerpo K de característica cero es isomorfo a un cuerpo de extensión de $\mathbb{Q}$, si $\mathbb{Q}$ es cuerpo de descomposición de $\mathbb{S}_n$ entonces K es cuerpo de descomposición de $\mathbb{S}_n$. Más aún, si consideramos el sistema p-modular $(\mathbb{Q}_p,\ R,\ \mathbb{F}_p)$, siendo $\mathbb{Q}_p$ un cuerpo completo con respecto a la valuación p-ádica, R el anillo de enteros p-ádicos y $\mathbb{F}_p$ el cuerpo de p elementos, el corolario 3.3 nos dice que $\mathbb{F}_p$ es un cuerpo de descomposición de $\mathbb{S}_n$ y de todos sus subgrupos; en particular, todo cuerpo de característica p es un cuerpo de descomposición de $\mathbb{S}_n$.

Por el teorema 2.3, sabemos que $\mathbb{Q}$ es un cuerpo de descomposición de $\mathbb{S}_n$, ya que los módulos de Specht S^μ son absolutamente irreducibles. Por tanto, todo cuerpo K es de descomposición de $\mathbb{S}_n$ y la cantidad de clases de $K\mathbb{S}_n$-módulos simples es igual al número de clases de conjugación de elementos p-regulares de $\mathbb{S}_n$. Por el lema 4.2 sabemos que la cantidad de clases de conjugación de elementos p-regulares es igual a la cantidad de particiones p-regulares. Luego, el conjunto $\{D^\mu : \mu\ p - \text{regular}\}$ es un conjunto completo de $K\mathbb{S}_n$-módulos simples no isomorfos. $\square$

Observación: Por la proposición 2.5, sabemos que la dimensión del $K\mathbb{S}_n$-módulo $S^\mu/(S^\mu \cap S^{\mu\perp}) = D^\mu$ está dada por el rango de la matriz de Gram con respecto a la base estándar de S^μ. Luego, tenemos el siguiente

Teorema 4.4 *La dimensión de las representaciones irreducibles D^μ de $\mathbb{S}_n$ sobre un cuerpo K de característica p se pueden calcular evaluando el rango de la matriz de Gram con respecto a la base estándar de S^μ.*

$\square$

Por ejemplo, supongamos que $n = 4$ y que $\mu = (2,\ 2)$. Luego, la dimensión de $S^{(2,\ 2)}$ es 2 y la base de politabloides estándar es la siguiente:

$$e_1 = \overline{\begin{matrix} 1 & 2 \\ 3 & 4 \end{matrix}} - \overline{\begin{matrix} 3 & 2 \\ 1 & 4 \end{matrix}} - \overline{\begin{matrix} 1 & 4 \\ 3 & 2 \end{matrix}} + \overline{\begin{matrix} 3 & 4 \\ 1 & 2 \end{matrix}}$$

$$e_2 = \overline{\begin{matrix} 1 & 3 \\ 2 & 4 \end{matrix}} - \overline{\begin{matrix} 2 & 3 \\ 1 & 4 \end{matrix}} - \overline{\begin{matrix} 1 & 4 \\ 2 & 3 \end{matrix}} + \overline{\begin{matrix} 2 & 4 \\ 1 & 3 \end{matrix}}$$

Entonces, la matriz de Gram que se obtiene es

$$\mathbf{A} = \begin{pmatrix} 4 & 2 \\ 2 & 4 \end{pmatrix}.$$

Si la característica de K es 2, el rango de $\mathbf{A}$ es 0 y en consecuencia, $D^{(2,\ 2)}$ es nulo. Si $car\ K = 3$, entonces $rg(\mathbf{A}) = 1$ y resulta que $D^{(2,\ 2)}$ es un $K\mathbb{S}_4$-módulo simple de dimensión 1. Finalmente, si $car\ K > 3$, entonces $rg(\mathbf{A}) = 2$ y la reducción módulo p de $S^{(2,\ 2)}$ es un $K\mathbb{S}_4$-módulo simple.

Teorema 4.5 *La dimensión de toda representación 2-modular irreducible no trivial de $\mathbb{S}_n$ es par.*

Demostración:
Si $\mu \neq (n)$ y t es un tablero de μ, entonces $< e_t,\ e_t >$ es par, puesto que es el orden del estabilizador de columnas de t. Luego, si $car\ K = 2$ tenemos que $< -,\ - >$ es una forma bilineal alternada, y como es sabido, el rango de una forma bilineal alternada es par. Por el teorema anterior se deduce que toda representación 2-modular irreducible no trivial tiene dimensión par. □

4.3. Factores de composición

Daremos en esta sección resultados generales acerca de los factores de composición de M^μ y S^μ cuando el cuerpo de base tiene característica positiva. Estos resultados serán útiles cuando calculemos las matrices de descomposición para las representaciones modulares de $\mathbb{S}_n$.

Si la característica del cuerpo es cero, el problema está resuelto, es decir que los factores de composición de M^μ son conocidos (ver [J]). Sin embargo, el cálculo de los factores de composición de S^μ cuando el cuerpo tiene característica positiva sigue siendo un problema abierto.

Teorema 4.6 *Todos los factores de composición de M^μ son de la forma D^λ tal que $\lambda > \mu$, excepto si μ es p-regular, en cuyo caso D^μ ocurre exactamente solamente una vez.*

Demostración:

Consideremos el siguiente diagrama:

$$\begin{tikzcd}[arrows=dash]
 & M^\mu \arrow[d] & \\
 & S^\mu + S^{\mu\perp} \arrow[dl] \arrow[dr] & \\
S^\mu \arrow[dr] & & S^{\mu\perp} \arrow[dl] \\
 & S^\mu \cap S^{\mu\perp} \arrow[d] & \\
 & 0 &
\end{tikzcd}$$

Por el corolario 4.5, todos los factores de composición de M^μ/S^μ son de la forma D^λ para $\lambda > \mu$. Como $S^{\mu\perp}$ es isomorfo al dual de M^μ/S^μ, debe tener los mismos factores de composición, en orden opuesto. Sabemos que $S^\mu/(S^\mu \cap S^{\mu\perp})$ es no nulo si y sólo si μ es p-regular, y en ese caso, resulta igual a D^μ. Como

$$0 \subseteq (S^\mu \cap S^{\mu\perp}) \subseteq S^\mu \subseteq M^\mu,$$

es una serie de composición de M^μ, el teorema queda demostrado $\square$

Daremos ahora un corolario cuya demostración es una aplicación directa del teorema anterior y de (2.2).

Corolario 4.6 *Si μ es p-regular, S^μ tiene un único primer factor de composición $D^\mu = S^\mu/(S^\mu \cap S^{\mu\perp})$. Si D es factor de composición de $(S^\mu \cap S^{\mu\perp})$, entonces $D \cong D^\lambda$ para algún $\lambda > \mu$. Si μ es p-singular, todos los factores de composición de S^μ son de la forma D^λ con $\lambda > \mu$.*

$\square$

Gracias al corolario anterior podemos conocer parte de la matriz **D** de descomposición de $\mathbb{S}_n$, la cual está dada en el siguiente corolario:

Corolario 4.7 *La matriz **D** de descomposición de $\mathbb{S}_n$ para un número primo p tiene la forma*

$$\begin{pmatrix}
1 & 0 & \dots & \dots & 0 \\
 & 1 & 0 & \dots & 0 \\
 & & \ddots & & \vdots \\
 & & & 1 & 0 \\
 & & & & 1 \\
 & & & &
\end{pmatrix},$$

donde las particiones p-regulares están ubicadas en orden lexicográfico de mayor a menor antes de todas las particiones p-singulares, y los lugares que se omiten en la matriz son aquéllos que todavía no podemos determinar.

□

Ejemplo

Sea $n = 3$. Las representaciones irreducibles de $\mathbb{S}_3$ sobre $\mathbb{Q}$ son $S^{(3)}$, $S^{(2,\ 1)}$ y $S^{(1^3)}$. En particular, $S^{(3)} = D^{(3)}$ es la representación p-modular trivial y $S^{(1^3)}$ es la representación signo, siendo $S^{(1^3)} \cong S^{(3)}$ si y sólo si $p = 2$.

Por el ejemplo (3.3.1a), sabemos que la matriz de descomposición de $\mathbb{S}_3$ para $p = 2$ es

$$\mathbf{D} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Si $p = 3$, tenemos que $S^{(3)} = D^{(3)}$ y $S^{(1^3)} = D^{(1^3)}$ no son isomorfos. Como la cantidad de $\mathbb{F}_3\mathbb{S}_3$-módulos simples es igual a la cantidad de clases de conjugación de elementos p-regulares, éstos forman un conjunto completo de $\mathbb{F}_3\mathbb{S}_3$-módulos simples. Por tanto, ambos dos deben ser factores de composición de $S^{(2,\ 1)}$, resultando uno de ellos isomorfo a $D^{(2,\ 1)}$. A saber, $(2,\ 1)$ es una partición 3-regular de 3, entonces por el teorema anterior sus factores de composición deben ser $D^{(2,\ 1)}$, que ocurre exactamente una sola vez, y posiblemente $D^{(3)}$. Como $dim\ S^{(2,\ 1)} = 2$, se deduce que $D^{(2,\ 1)} \cong D^{(1^3)}$. Por tanto, la matriz de descomposición es la siguiente:

$$\mathbf{D} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Si $p > 3$, todas las particiones son p-regulares, entonces hay 3 $\mathbb{F}_p\mathbb{S}_3$-módulos simples no isomorfos que forman un sistema completo. Por el teorema anterior, éstos deben ser $D^{(3)}$, $D^{(2,\ 1)}$ y $D^{(1^3)}$. Por tanto, tenemos que

$$\mathbf{D} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

4.4. Algunos módulos de Specht irreducibles

Los módulos de Specht S^μ son irreducibles sobre cuerpos de característica cero, y como todo cuerpo es un cuerpo de descomposición de $\mathbb{S}_n$, S^μ es un irreducible sobre un cuerpo de característica positiva si y sólo si es irreducible sobre el cuerpo de p-elementos. Por tanto, éste es el caso que en esta sección trataremos, es decir que $K = \mathbb{F}_p$ será el cuerpo de p-elementos. Como la completa clasificación de los módulos de Specht es un problema abierto, trataremos en esta sección algunos casos particulares.

Lema 4.6 *Supongamos que $Hom_{\mathbb{F}_p\mathbb{S}_n}(S^\mu,\ S^\mu) \cong \mathbb{F}_p$. Entonces S^μ es irreducible si y sólo si S^μ es isomorfo a su dual $S^{\mu *}$.*

Demostración:
Si S^μ es irreducible, entonces su carácter modular φ es real. En particular, el $\mathbb{F}_p\mathbb{S}_n$-módulo dual de S^μ tiene la misma dimensión que S^μ. Luego, S^μ resulta isomorfo a su dual.

Sea U un submódulo irreducible de S^μ. Si S^μ es isomorfo a su dual $S^{\mu *}$, entonces

$$U \cong (S^\mu/U^\perp)^* \cong S^\mu/(U^\perp)^*.$$

Luego, existe un submódulo V de S^μ tal que $S^\mu/V \cong U$. Como la aplicación

$$S^\mu \to S^\mu/V \to U,$$

da un elemento no nulo de $Hom_{\mathbb{F}_p\mathbb{S}_n}(S^\mu,\ S^\mu)$, debe ser que $U \cong S^\mu$. Por tanto, S^μ es irreducible.

$\square$ **Observación:**
Veremos más adelante un ejemplo que muestra que la hipótesis $Hom_{\mathbb{F}_p\mathbb{S}_n}(S^\mu,\ S^\mu) \cong \mathbb{F}_p$ no se puede omitir. Sin embargo, esta condición se cumple para la mayoría de los módulos de Specht.

Sabemos que $\pi\kappa_t = \kappa_{\pi t}\pi$, y que $\pi\rho_t = \rho_{\pi t}\pi$, $\forall \pi \in \mathbb{S}_n$. Luego, tenemos que $\pi\rho_t\kappa_t\{t\} = \rho_{\pi t}\kappa_{\pi t}\{\pi t\}$, $\forall \pi \in \mathbb{S}_n$. Usando el lema anterior y la proposición 4.1 podemos definir:

Definición 59 *Sean $\mathbb{F}_p$ el cuerpo de p elementos y θ el elemento no nulo de $Hom_{\mathbb{F}_p\mathbb{S}_n}(M^\mu,\ S^\mu)$ dado por la siguiente aplicación*

$$\theta : \{t\} \mapsto (\frac{1}{g^{\mu'}}\rho_t\kappa_t\{t\})_p.$$

Es decir, la imagen de $\{t\}$ se obtiene del vector $\frac{1}{g^{\mu'}}\rho_t\kappa_t\{t\} \in \mathbb{S}^\mu_{\mathbb{Q}}$ reduciendo todos los coeficientes de los tabloides módulo p.

Como primera aplicación del lema y la definición anterior tenemos el siguiente teorema:

Teorema 4.7 *i) Si $Im\ \theta \subset S^\mu$, o equivalentemente si $Ker\ \theta \supset S^{\mu\perp}$, entonces S^μ es reducible.*

ii) Si $Im\ \theta = S^\mu$, o equivalentemente si $Ker\ \theta = S^{\mu\perp}$, y si $Hom_{\mathbb{F}_p\mathbb{S}_n}(S^\mu,\ S^\mu) \cong \mathbb{F}_p$, entonces S^μ es irreducible.

Demostración:
Si el cuerpo de base es $\mathbb{Q}$, entonces el lema anterior nos dice que el morfismo φ definido por

$$\varphi\{t\} = \frac{1}{g^{\mu'}}\rho_t\kappa_t\{t\},$$

manda κ_t a un múltiplo no nulo de él mismo. Luego, tenemos que $dim\ Ker\ \varphi = dim\ S^{\mu\perp}_{\mathbb{Q}}$, y por el teorema del submódulo se deduce que $Ker\ \varphi = S^{\mu\perp}_{\mathbb{Q}}$. Por el lema 4.1, sabemos que si trabajamos sobre el cuerpo de p elementos tenemos que $Ker\ \theta \supseteq S^{\mu\perp}$. Por tanto, $Ker\ \theta \supset S^{\mu\perp}$ si y sólo si $Im\ \theta \subset S^\mu$. De aquí se sigue inmediatamente la primera parte del teorema, ya que $Im\ \theta$ es un submódulo propio de S^μ.

Si $Ker\ \theta = S^{\mu\perp}$, entonces θ da un isomorfismo entre $M^\mu/S^{\mu\perp}$ y S^μ. Como $M^\mu/S^{\mu\perp} \cong S^{\mu *}$, resulta que $S^\mu \cong S^{\mu *}$, y por el lema 4.6 se sigue que S^μ es un $\mathbb{F}_p\mathbb{S}_n$-módulo irreducible. $\square$

El siguiente teorema nos da una forma de determinar si un módulo de Specht es reducible a través de un cálculo combinatorio. Sin embargo, este cálculo no siempre es fácil de realizar.

Teorema 4.8 *Supongamos que μ es p-regular. Entonces S^μ es reducible si y sólo si p divide al entero*

$$\frac{\prod(\textit{longitud de los ganchos en } [\mu])}{g^{\mu'}}.$$

Demostración:
Se puede ver que si μ es p-regular o $p \neq 2$, entonces $Hom_{\mathbb{F}_p\mathbb{S}_n}(S^\mu,\ S^\mu) \cong \mathbb{F}_p$ (ver [J] Corolario 13.17). Luego, el teorema anterior muestra que S^μ es reducible si y sólo si $Ker\ \theta \supset S^{\mu\perp}$.

Como μ es p-regular, tenemos que $S^\mu/(S^\mu \cap S^{\mu\perp})$ es no nulo. Luego, por el teorema 2.2, $M^\mu/S^{\mu\perp} \cong S^{\mu *}$ tiene un único submódulo minimal, a saber $(S^\mu + S^{\mu\perp})/S^{\mu\perp}$. Por tanto, S^μ es reducible si y sólo si $Ker\ \theta \supset S^\mu$.

Por (4.4ii) tenemos que

$$\begin{aligned} \theta\kappa_t\{t\} &= (\tfrac{1}{g^{\mu'}}\kappa_t\rho_t\kappa_t\{t\})_p \\ &= (\frac{\prod(\text{longitud de los ganchos en } [\mu])}{g^{\mu'}}\kappa_t\{t\})_p. \end{aligned}$$

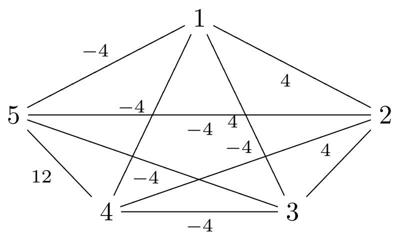
Al ser S^μ un módulo cíclico generado por e_t, tenemos que S^μ es reducible si y sólo si p divide al entero $\frac{\prod(\text{longitud de los ganchos en } [\mu])}{g^{\mu'}}$. □

Ejemplos

i) Si μ es p-regular y p no divide a $\prod$(longitud de los ganchos en $[\mu]$), entonces S^μ es irreducible.

ii) Si μ y su partición conjugada μ' son p-regulares, entonces por el corolario 4.3, p no divide a $g^{\mu'}$. Luego, S^μ es reducible si y sólo si p divide a $\prod$(longitud de los ganchos en $[\mu]$). En particular, S^μ es reducible si $\mu = ((p-1)^x)$, donde $1 < x < p$.

iii) Sean $\mu = (3,\ 2)$ y $t = \begin{array}{|c|c|c|}\hline 1 & 2 & 3 \\ \hline 4 & 5 \\ \cline{1-2}\end{array}$. Un cálculo directo nos muestra que, siguiendo la notación de 2.4, $\rho_t\kappa_t\{t\}$ es igual a



.

Luego, el máximo común divisor de los coeficientes de los tabloides involucrados en $\rho_t\kappa_t\{t\}$ es 4, es decir que $g^{\mu'} = 4$. Si calculamos las longitudes h_{ij} de todos los ganchos $(i.\ j)$ en el diagrama $[\mu]$ y las reemplazamos por los nodos obtenemos el tablero

$$\begin{array}{|c|c|c|}\hline 4 & 3 & 1 \\ \hline 2 & 1 \\ \cline{1-2}\end{array}\ .$$

Entonces, el producto de las longitudes de los ganchos en $[\mu]$ es 24. Por tanto, S^μ es reducible si y sólo si la característica del cuerpo es 2 o 3.

Definición 60 *Decimos que una partición μ de n es una partición de* **tipo gancho** *si es de la forma $\mu = (n)$ o $\mu = (x,\ 1^y)$, tal que $0 \leq x \leq n-1,\ 1 \leq y \leq n$.*

Es claro que el diagrama asociado $[\mu]$ a este tipo de partición es un gancho del nodo $(1,\ 1)$. En particular, la longitud del gancho es n.

Por ejemplo, $(5),\ (4,\ 1),\ (3,\ 1^2),\ (2,\ 1^3)$ y (1^5) son todas las particiones de tipo gancho de 5. A saber,

$$\begin{array}{ll}
[(5)] = \boxed{}\boxed{}\boxed{}\boxed{}\boxed{}\ , & [(4,\ 1)] = \begin{array}{l}\boxed{}\boxed{}\boxed{}\boxed{}\\ \boxed{}\end{array}\ , \\
[(3,\ 1^2)] = \begin{array}{l}\boxed{}\boxed{}\boxed{}\\ \boxed{}\\ \boxed{}\end{array}\ , & [(2,\ 1^3)] = \begin{array}{l}\boxed{}\boxed{}\\ \boxed{}\\ \boxed{}\\ \boxed{}\end{array} \\
\text{y } [(1^5)] = \begin{array}{l}\boxed{}\\ \boxed{}\\ \boxed{}\\ \boxed{}\\ \boxed{}\end{array}\ . &
\end{array} \tag{1}$$

Teorema 4.9 *Supongamos que μ es una partición tipo gancho de n, y que S^μ está definido sobre el cuerpo de p elementos. Entonces S^μ es irreducible si y sólo si cumple una de las siguientes proposiciones:*

i) $\mu = (n)$ *o* $\mu = (1^n)$.

ii) $p \not| n$ *y* $\mu = (n-1,\ 1)$ *o* $\mu = (2,\ 1^{n-2})$.

iii) $p \not| n$ *y* $p \neq 2$.

Demostración:
Como $S^{(n)}$ y $S^{(1^n)}$ son de dimensión 1, ambas son irreducibles. Luego, podemos suponer que $\mu = (a,\ 1^b)$ tal que $a > 1,\ b > 0$ y que $a + b = n$.

Sea $\bar{\kappa_t} = \sum\{sg(\sigma)\sigma :\ \sigma \in \mathbb{S}_{\{2,\ 3,\dots,b+1\}}\}$ tal que

$$t = \begin{array}{l}\boxed{1}\boxed{\text{b+2}}\dots\boxed{\text{b+a}}\\ \boxed{2}\\ \vdots\\ \boxed{\text{b+1}}\end{array}\ .$$

Supongamos por un momento que el cuerpo de base es $\mathbb{Q}$. Un simple cálculo nos muestra que

$$\begin{aligned}
\kappa_t &= \bar{\kappa_t}(1 - (1,\ 2) - (1,\ 3) - \cdots - (1,\ b+1)) \\
&= (1 - (1,\ 2) - (1,\ 3) - \cdots - (1,\ b+1))\bar{\kappa_t}.
\end{aligned}$$

Por otro lado, tenemos que

$$\bar{\kappa_t}\rho_t\kappa_t\{t\} = \rho_t\bar{\kappa_t}\kappa_t\{t\} = b!\rho_t\kappa_t\{t\}.$$

Luego,

$$b!(1-(1,\ 2)-(1,\ 3)-\cdots-(1,\ b+1))\rho_t\kappa_t\{t\}=$$

$$=(1-(1,\ 2)-(1,\ 3)-\cdots-(1,\ b+1))\bar{\kappa_t}\rho_t\kappa_t\{t\}=$$

$$=\kappa_t\rho_t\kappa_t\{t\}=$$

$$=\prod(\text{longitud de los ganchos en }[\mu])\kappa_t\{t\}=$$

$$=(a-1)!b!(a+b)\kappa_t\{t\}.$$

Por el lema 4.3 tenemos que $(a-1)!/g^{\mu'}$ y $g^{\mu'}/((a-1)!)^1$, es decir $g^{\mu'}=(a-1)!$. Entonces la igualdad anterior se traduce en la siguiente:

$$\frac{1}{g^{\mu'}}(1-(1,\ 2)-(1,\ 3)-\cdots-(1,\ b+1))\rho_t\kappa_t\{t\}=(a+b)\kappa_t\{t\}. \tag{2}$$

Sea θ el morfismo definido en (59). La igualdad (2) nos muestra que

$$\theta(1-(1,\ 2)-(1,\ 3)-\cdots-(1,\ b+1))\{t\}=(a+b)\kappa_t\{t\}.$$

Por tanto, si trabajamos sobre el cuerpo de p elementos y p no divide a n, resulta que $Im\ \theta=S^{(a,\ 1^b)}$. En particular, $S^{(a,\ 1^b)}$ es isomorfo a su dual. Pero $Hom_{\mathbb{F}_p\mathbb{S}_n}(S^\mu,\ S^\mu)\cong\mathbb{F}_p$ si $p\neq 2$ o $\mu=(n-1,\ 1)$ ([J] Corolario 13.17). Luego, el lema 4.6 nos dice que S^μ es irreducible si p no divide a n y $p\neq 2$ o $\mu=(n-1,\ 1)$. Como $S^{\mu'}\cong S^\mu\otimes S^{(1^n)}$ sobre cualquier cuerpo, se deduce que S^μ también es irreducible si $p\not|n$ y $\mu=(2,\ 1^{n-2})=(n-1,\ 1)'$.

Hasta aquí hemos probado la suficiencia. Para probar la necesidad, supongamos que p/n. Entonces

$$(1-(1,\ 2)-(1,\ 3)-\cdots-(1,\ b+1))\{t\}\in Ker\ \theta.$$

Sea t^* el tablero tipo gancho que se obtiene invirtiendo el orden de los coeficientes en la primera fila de t. Como $a>1$, todos los tabloides involucrados en e_{t^*} tienen a 1 en la primera fila. Por tanto, $\{t\}=\{t^*\}$ es el único tabloide involucrado en e_{t^*} y en $(1-(1,\ 2)-(1,\ 3)-\cdots-(1,\ b+1))\{t\}$, esto es,

$$<(1-(1,\ 2)-(1,\ 3)-\cdots-(1,\ b+1))\{t\},e_{t^*}>=1.$$

Luego, $(1-(1,\ 2)-(1,\ 3)-\cdots-(1,\ b+1))\{t\}\in Ker\ \theta/S^{\mu\perp}$, es decir que $Ker\ \theta\supset S^{\mu\perp}$. Por el teorema 4.7 tenemos que S^μ es reducible.

En conclusión, hemos probado que si p/n, entonces S^μ es reducible. Por tanto, para finalizar la demostración, debemos probar que S^μ es reducible cuando $\mu=(a,\ 1^b)$, siendo $a>1,\ b>1$ y $p=2$. Dicha demostración se deduce fácilmente de la regla de Littlewood-Richardson (ver [J]) y del hecho que $S^{(n)}\cong S^{(1^n)}$ cuando el cuerpo de base tiene característica 2. □

4.5. Matrices de descomposición de $\mathbb{S}_n$

Como hemos dicho anteriormente, no hay manera de determinar los factores de composición de un módulo de Specht general cuando la característica del cuerpo de base es p. Por tanto, no podemos determinar los coeficientes de las matrices de descomposición de $\mathbb{S}_n$, los cuales dan la multiplicidad de cada representación p-modular irreducible D^μ como factor de composición de S^μ, salvo en algunos casos particulares. Daremos como ejemplo las matrices de descomposición de $\mathbb{S}_5$ sobre cuerpos de característica 2, 3 y 5.

El primer teorema que expondremos es de gran utilidad para el cálculo de matrices de descomposición y tablas de caracteres de $\mathbb{S}_n$. Su demostración se deduce de un caso particular de la regla de Murnaghan-Nakayama, la cual proporciona una manera fácil de encontrar coeficientes en la tabla de caracteres de $\mathbb{S}_n$. Ver [J].

Definición 61 *Dada una partición μ de n y su correspondiente diagrama $[\mu]$. Un* **semigancho** *de $[\mu]$ es una parte conexa sobre el borde derecho del diagrama que puede ser quitada para dejar un diagrama menor $[v]$ contenido en $[\mu]$.*

Por ejemplo, sea $\mu = (4^2,\ 3)$ y notemos a los semiganchos por el conjunto de nodos indicados por $*$. Entonces

$$\begin{array}{|c|c|c|c|}\hline & & & \\ \hline & & * & * \\ \hline & * & * \\ \cline{1-3}\end{array} \quad \text{y} \quad \begin{array}{|c|c|c|c|}\hline & & & * \\ \hline & & * & * \\ \hline & & * \\ \cline{1-3}\end{array}\ ,$$

son los únicos semiganchos de longitud 4 en $(4^2,\ 3)$. Este diagama también contiene un semigancho de longitud 6, dos de longitud 5, dos de longitud 3, dos de longitud 2, y dos de longitud 1. Consideremos ahora los ganchos de $[\mu]$ y sus longitudes. Reemplazando cada longitud en el nodo correspondiente obtenemos el tablero

$$t = \begin{array}{|c|c|c|c|}\hline 6 & 5 & 4 & 2 \\ \hline 5 & 4 & 3 & 1 \\ \hline 3 & 2 & 1 \\ \cline{1-3}\end{array}\ .$$

Comparando, hemos mostrado la propiedad de los diagramas:

Lema 4.7 *Existe una correspondencia 1-1 natural entre los ganchos de $[\mu]$ y los semigamchos de $[\mu]$.*

Demostración:
Es fácil verificar que dicha correspondencia está dada por lo siguiente: el semigancho que comienza en la j-ésima fila y termina en la i-ésima columna corresponden al gancho cuyo nodo es $(i,\ j)$. $\square$

La longitud de una pierna de un semigancho se define como la suma de las longitudes de las piernas de los ganchos que contiene. En el ejemplo anterior, dichas longitudes son 1 y 2 respectivamente

Teorema 4.10 *Si v es una partición de $n-r$, entonces el carácter generalizado de $\mathbb{S}_n$ que corresponde a*

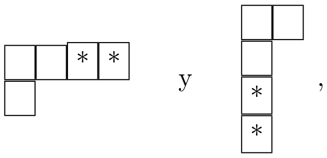
$$\sum\{(-1)^i[\lambda] : [\lambda]/[v] \text{ es un semigancho de longitud } r \text{ y longitud de pierna } i\},$$

es nulo sobre todas las clases de conjugación excepto aquéllas que contengan a un ciclo de longitud r.

$\square$

Hagamos dos ejemplos para entender la idea de este teorema:

i) Sean $n = 5$ y v una partición de 3, digamos $(2,\ 1)$. Aquellos diagramas $[\lambda]$ que contienen a $[v]$ tal que $[\lambda]/[v]$ es un semigancho de longitud 2, se obtienen agregando al diagrama $[v]$ nodos en el borde derecho de manera que los nodos agregados formen un semigancho. Por ejemplo



son los únicos diagramas $[\lambda]$ tales que $[\lambda]/[v]$ es un semigancho de longitud 2. Por tanto, tenemos que

$$\chi^{(4,\ 1)} - \chi^{(2,\ 1^3)} = 0,$$

sobre todas las clases de conjugación de $\mathbb{S}_5$ excepto aquéllas que contengan un ciclo de longitud 2; es decir,las clases de conjugación de elementos 2-regulares.

ii) Si $n = 5$ y $v = 0$, entonces los diagramas $[\lambda]$ tales que $[\lambda]/[\mu]$ es un semigancho de longitud 5 son exactamente las particiones tipo gancho de 5 dadas en (1). Por tanto, el teorema nos dice que

$$\chi^{(5)} - \chi^{(4,\ 1)} + \chi^{(3,\ 1^2)} - \chi^{(2,\ 1^3)} + \chi^{(1^5)} = 0,$$

sobre todas las clases de conjugación de $\mathbb{S}_5$ excepto aquéllas que contengan a un ciclo de longitud 5; en particular, la igualdad anterior vale sobre las clases de conjugación de elementos 5-regulares.

El teorema que expondremos a continuación da resultados parciales, sin embargo, nos alcanza para poder describir las matrices de descomposición de $\mathbb{S}_5$ sobre cuerpos de característica 2, 3 y 5.

Teorema 4.11 *Supongamos que el primo p es impar.*

i) Si $p \not| n$, todas las representaciones S^μ de $\mathbb{S}_n$ dadas por particiones tipo gancho permanecen irreducibles cuando se reducen módulo p. Más aún, si $S^\mu \cong S^\lambda$, siendo ambas particiones de tipo gancho, entonces $\mu = \lambda$.

ii) Si p/n, una parte de la matriz de descomposición de $\mathbb{S}_n$ es la siguiente:

$$\begin{array}{lccccc}
(n) & 1 & & & & \\
(n-1,\ 1) & 1 & 1 & & & \\
(n-2,\ 2) & & 1 & 1 & & \\
\vdots & & & \ddots & & \\
(2,\ 1^{n-2}) & & & & 1 & 1 \\
(1^n) & & & & & 1
\end{array},$$

donde listamos en la primer columna las particiones μ de tipo gancho para identificar la fila correspondiente a S^μ y los coeficientes que se omiten se consideran nulos.

Demostración:
Demostraremos los resultados por inducción. Si $n = 0$, no hay nada que probar. Supongamos entonces que es cierto para $n-1$ y probémoslo para n. Notar que si χ^μ es el carácter de S^μ, entonces

$$Res_{\mathbb{S}_{n-1}}\ \chi^{(x,\ 1^y)} = \chi^{(x-1,\ 1^y)} + \chi^{(x,\ 1^{y+1})}, \quad \text{si } x > 1,\ y > 0,\ x + y = n. \tag{3}$$

Supongamos que p no divide a n. Como p es un primo impar, por el teorema 4.9 sabemos que S^μ es irreducible para toda partición μ de tipo gancho.

Sean μ y λ dos particiones tipo gancho tales que las reducciones m'odulo p de los $\mathbb{Q}\mathbb{S}_n$-módulos S^μ y S^λ son isomorfas. Luego, las restricciones de ambas a $\mathbb{S}_n$ son isomorfas. Como el resultado su supone cierto sobre $\mathbb{S}_{n-1}$, ambas restricciones tienen los mismos sumandos; en particular, se sigue que $\mu = \lambda$, como se quería demostrar.

Supongamos ahora que p divide a n, y que $x > 1,\ y > 0$. Por (4.9*iii*), las representaciones $S^{(x,\ 1^y)}$ son reducibles y por tanto, la restricción de $\chi^{(x,\ 1^y)}$ a $\mathbb{S}_{n-1}$ debe tener por lo menos dos componentes. Como p no divide a $n-1$, las componentes que aparecen en (3) son irreducibles y por tanto deben ser las únicas dos componentes de *Res* $\chi^{(x,\ 1^y)}$. Sean φ_x^+ la componente modular de $\chi^{(x,\ 1^y)}$ tal que

$$Res\ \varphi_x^+ = \chi^{(x-1,\ 1^y)},$$

y φ_x^- aquella componente modular que satisface

$$Res\ \varphi_x^- = \chi^{(x,\ 1^{y-1})},$$

siendo $\varphi_n^- = 0$ y $\varphi_1^+ = 0$. Para terminar la demostración basta mostrar que $\varphi_{x-1}^- = \varphi_x^+$, para todo x; puesto que no puede haber otra igualdad ya que las restricciones a $\mathbb{S}_{n-1}$ son diferentes.

Por el teorema 4.10, la siguiente relación entre caracteres se mantiene sobre todas las clases de conjugación de $\mathbb{S}_n$, excepto sobre la correspondiente a la partición (n). En particular, la igualdad vale sobre las clases p-regulares:

$$\chi^{(n)} - \chi^{(n-1,\ 1)} + \chi^{(n-2,\ 1^2)} - \cdots \pm \chi^{(1^n)} = 0.$$

En términos de caracteres modulares o de Brauer, la igualdad anterior se traduce en la siguiente

$$\varphi_n^+ - (\varphi_{n-1}^- + \varphi_{n-1}^+) + (\varphi_{n-2}^- + \varphi_{n-2}^+) - \cdots \pm \varphi_1^- = 0.$$

Como los caracteres de Brauer de $\mathbb{S}_n$ son linealmente independientes sobre $\mathbb{Q}$, debe ser que $\varphi_{x-1}^- = \varphi_x^+$, para todo x.

Tenemos entonces la siguiente igualdad de caracteres de Brauer sobre las clases p-regulares:

$$\chi^{(x,\ 1^y)} = \varphi_x^+ + \varphi_x^- = \varphi_x^+ + \varphi_{x+1}^+.$$

En consecuencia, se deduce que

$$d[S^{(x,\ 1^y)}] = [D^{(x+1,\ 1^{y-1})}] + [D^{(x,\ 1^y)}];$$

como se quería demostrar. □

De ahora en adelante, notaremos las filas de la matriz de descomposición de $\mathbb{S}_n$ por las particiones y las columnas por particiones p-regulares. Es decir, el coeficiente correspondiente a la μ-ésima fila y a la λ-ésima columna es la multiplicidad de D^λ como factor de composición de S^μ sobre un cuerpo de característica p. Escribiremos χ^μ para designar el carácter de Brauer de S^μ y φ^λ para el carácter de Brauer de D^λ.

Para finalizar, daremos las matrices de descomposición de $\mathbb{S}_5$ sobre cuerpos de característica p tal que p divide al orden del grupo.

4.5.1. Ejemplos

Sea $(\mathbb{Q}_p, R,\ \mathbb{F}_p)$ el sistema p-modular dado por la valuación p-ádica sobre el cuerpo $\mathbb{Q}$ de los racionales, siendo $\mathbb{Q}_P$ la comletación de $\mathbb{Q}$, R el anillo p-ádico de enteros y $\mathbb{F}_p$ el cuerpo de p elementos. Como el orden de $\mathbb{S}_5$ es $2^3 \cdot 3 \cdot 5$, consideraremos las representaciones modulares sobre $\mathbb{F}_2,\ \mathbb{F}_3$ y $\mathbb{F}_5$.

a) Sea $p = 2$. Las clases de elementos 2-regulares de $\mathbb{S}_5$ son $[1\ 2\ 3\ 4\ 5]$, $[1\ 2\ 3]$ y $[id]$, entonces hay 3 clases de isomorfismos de $\mathbb{F}_2\mathbb{S}_5$-módulos simples. Podemos representar a cada una de ellas por el elemento D^μ tal que μ es una partición 2-regular de 5. A saber, las particiones 2-regulares son (5), $(4,\ 1)$ y $(3,\ 2)$, entonces la base de clases de isomorfismo de $\mathbb{F}_2\mathbb{S}_5$-módulos simples está constituida por

$$D^{(5)},\ D^{(4,1)} \text{ y } D^{(3,\ 2)}.$$

Como 2 no divide a 5, el teorema 4.9 nos asegura que los módulos $D^{(5)}$, $D^{(4,1)}$, $D^{(2,\ 1^3)}$ y $D^{(1^5)}$ son irreducibles. Es claro que cuando reducimos módulo 2 las representaciones $S^{(5)}$ y $S^{(1^5)}$, sus imágenes resultan isomorfas, es decir $D^{(5)} \cong D^{(1^5)}$. Por otro lado, como $(2,\ 1^3)$ es la partición conjugada de $(4,\ 1)$, por el teorema 4.1 sabemos que

$$S^{(2,1^3)} \otimes S^{(1^5)} \cong S^{(4,1)^*}.$$

Al ser la reducción de $S^{(4,1)}$ irreducible y $(4,\ 1)$ una partición 2-regular, tenemos que $S^{(4,1)}$ es isomorfo a su dual. Esto implica que

$$S^{(2,1^3)} \otimes S^{(1^5)} \cong S^{(4,1)}.$$

Reduciendo módulo 2 tenemos que

$$D^{(2,1^3)} \otimes D^{(1^5)} \cong D^{(4,1)},$$

siendo $D^{(1^5)}$ la representación trivial de $\mathbb{S}_5$ sobre $\mathbb{F}_2$. De aquí se deduce que

$$D^{(2,1^3)} \cong D^{(4,1)}.$$

Por el ejemplo *iii)* hecho en la sección 4.4, sabemos que la reducción de $S^{(3,\ 2)}$ es reducible si la característica del cuerpo es 2 ó 3. Luego, $S^{(3,\ 2)}$ tiene por lo menos dos factores de composición.

Observar que los $\mathbb{F}_2\mathbb{S}_5$-módulos simples $D^{(5)}$ y $D^{(4,\ 1)}$ se obtienen por reducción módulo 2 de los $\mathbb{Q}\mathbb{S}_5$-módulos simples $S^{(5)}$ y $S^{(4,\ 1)}$. Al confeccionar la matriz de descomposición, veremos que $D^{(3,\ 2)}$ no se obtiene por reducción de un $\mathbb{Q}\mathbb{S}_5$-módulo simple.

Hasta aquí, hemos encontrado los factores de composición de $S^{(5)}$, $S^{(4,1)}$, $S^{(2,\ 1^3)}$ y $S^{(1^5)}$. Para encontrar la matriz de descomposición de $\mathbb{S}_5$ sobre $\mathbb{F}_2$ nos faltan encontrar los factores de $S^{(3,\ 2)}$, $D^{(3,1^2)}$ y $D^{(2^2,1)}$. En ese sentido, usaremos el teorema 4.10 para obtener relaciones lineales entre los caracteres de dichas representaciones y los caracteres modulares irreducibles.

Para $v_1 = (3)$, $v_2 = (2,\ 1)$ y $v_3 = (1^3)$ particiones de 3, el teorema 4.10 nos dice que

$$\chi^{(5)} - \chi^{(3,\ 1^2)} + \chi^{(3,\ 2)} = 0,$$

$$\chi^{(4,\ 1)} - \chi^{(2,\ 1^3)} = 0 \quad \text{y}$$

$$-\chi^{(2^2,\ 1)} + \chi^{(3,\ 1^2)} - \chi^{(1^n)} = 0,$$

sobre los elementos 2-regulares de $\mathbb{S}_5$. La segunda igualdad ya era conocida y no aporta nada nuevo, nos concentraremos en las dos restantes. Operando sobre esas igualdades se obtiene

$$\begin{aligned} \chi^{(3,\ 1^2)} &= \chi^{(5)} + \chi^{(3,\ 2)}, \\ \chi^{(3,\ 1^2)} &= \chi^{(2^2,\ 1)} + \chi^{(1^n)}, \end{aligned} \tag{4}$$

sobre los elementos 2-regulares de $\mathbb{S}_5$. De aquí se deduce que

$$\chi^{(3,\ 2)} = \chi^{(2^2,\ 1)}, \tag{5}$$

lo cual nos muestra que los factores de composición de $S^{(3,\ 2)}$ y de $S^{(2^2,\ 1)}$ son los mismos. Por tanto, si encontramos los factores de composición de $S^{(3,\ 2)}$, por (5) y (4)obtenemos también los factores de composición de $S^{(2^2,\ 1)}$ y $S^{(3,\ 1^2)}$.

Al ser $(3,\ 2)$ una partición 2-regular, sabemos que la reducción de $S^{(3,\ 2)}$ tiene a $D^{(3,\ 2)}$ como factor de composición con multiplicidad 1 y si D^{μ} es factor de composición, entonces $\mu > (3,\ 2)$. Luego, el carácter de Brauer de $S^{(3,\ 2)}$ es de la forma

$$\chi^{(3,\ 2)} = a\varphi^{(5)} + b\varphi^{(4,\ 1)} + \varphi^{(3,\ 2)}, \quad a,\ b \in \mathbb{N}.$$

Si evaluamos la igualdad anterior en 1 y usamos la fórmula de los ganchos para calcular las correspondientes dimensiones, obtenemos la siguiente igualdad:

$$dim\ S^{(3,\ 2)} = a \cdot dim\ D^{(5)} + b \cdot dim\ D^{(4,\ 1)} + dim\ D^{(3,\ 2)},$$

$$5 = a \cdot 1 + b \cdot 4 + dim\ D^{(3,\ 2)}, \quad a,\ b \in \mathbb{N}.$$

La dimensión de $D^{(3,\ 2)}$ viene dada por el rango de la matriz de Gram $\mathbf{A}$ sobre $\mathbb{F}_2$. Usando el ejemplo de la sección 2.4, es fácil ver que dicha matriz es la siguiente:

$$\mathbf{A} = \begin{pmatrix} 4 & -2 & 0 & -1 & -1 \\ -2 & 4 & 1 & 2 & 1 \\ 0 & 1 & 4 & 2 & 1 \\ -1 & 2 & 2 & 4 & 2 \\ -1 & 1 & 1 & 2 & 4 \end{pmatrix}.$$

Reduciendo módulo 2 la matriz anterior, obtenemos una nueva matriz $\bar{\mathbf{A}}$ sobre $\mathbb{F}_2$ dada por

$$\bar{\mathbf{A}} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \end{pmatrix},$$

cuyo rango es claramente 4. Luego, $dim\ D^{(3,\ 2)} = 4$ y esto implica que $a = 1$ y $b = 0$. Por tanto, tenemos que

$$d[S^{(3,\ 2)}] = [D^{(5)}] + [D^{(3,\ 2)}],$$

$$d[S^{(2^2,\ 1)}] = [D^{(5)}] + [D^{(3,\ 2)}],$$

$$d[S^{(3,\ 1^2)}] = 2[D^{(5)}] + [D^{(3,\ 2)}].$$

En conclusión, la matriz de descomposición de $\mathbb{S}_5$ sobre $\mathbb{F}_2$ es la siguiente:

$$\mathbf{D} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \\ 2 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

$\square$

b) Sea $p = 3$. Las clases de elementos 3 regulares de $\mathbb{S}_5$ son $[1\ 2\ 3\ 4\ 5]$, $[1\ 2\ 3\ 4]$, $[1\ 2][3\ 4]$, $[1\ 2]$ y $[id]$. Entonces, la cantidad de clases de isomorfismo de $\mathbb{F}_3\mathbb{S}_5$-módulos simples es 5 y su base está dada por los módulos D^{μ}, donde μ es una partición 3-regular. Es decir que los módulos

$$D^{(5)},\ D^{(4,\ 1)},\ D^{(3,\ 2)},\ D^{(3,\ 1^2)} \text{ y } D^{(2^2,\ 1)},$$

forman una base de $\mathbb{F}_3\mathbb{S}_5$-módulos simples, salvo isomorfismos. Como $p \neq 2$ y p no divide a 5, el teorema 4.9 nos dice que la reducción de todas las representaciones dadas por particiones tipo gancho son irreducibles y no isomorfas entre sí. Esto es

$$d[S^{(5)}] = [D^{(5)}],$$

$$d[S^{(4,\ 1)}] = [D^{(4,\ 1)}],$$

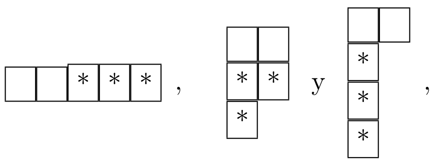
$$d[S^{(3,\ 1^2)}] = [D^{(3,\ 1^2)}],$$

$$d[S^{(2,\ 1^3)}] = [D^{(2,\ 1^3)}] \text{ y}$$

$$d[S^{(1^5)}] = [D^{(1^5)}].$$

En particular, tenemos 5 $\mathbb{F}_3\mathbb{S}_n$-módulos simples que se obtienen por reducción módulo 3 de $\mathbb{Q}\mathbb{S}_5$-módulos simples. Claramente, $D^{(3,\ 2)}$ y $D^{(2^2,\ 1)}$ deben ser isomorfos a algunos de los expuestos anteriormente. Observar que, como $p = 3$, la reducción módulo 3 de ambas representaciones $S^{(3,\ 2)}$ y $S^{(2^2,\ 1)}$ son representaciones reducibles.

Análogamente al ejemplo anterior, usaremos el teorema 4.10 para establecer relaciones lineales entre los caracteres modulares. Sea $v = (2)$ una partición de 2, entonces los diagramas $[\lambda]$ asociados a particiones λ de 5, que satisfacen que $[\lambda]/[\mu]$ es un semigancho de longitud 3, son los siguientes:



siendo las longitudes de las piernas de los semiganchos 0, 1 y 2, respectivamente. Por tanto, tenemos que

$$\chi^{(5)} - \chi^{(2^2,\ 1)} + \chi^{(2,\ 1^3)} = 0,$$

sobre todas las clases de conjugación 3-regulares. Siguiendo el mismo procedimiento con $v = (1^2)$ obtenemos

$$\chi^{(4,\ 1)} - \chi^{(3,\ 2)} + \chi^{(1^5)} = 0,$$

sobre todas las clases de conjugación 3-regulares. De aquí se deduce la siguiente igualdad de caracteres de Brauer sobre las clases de conjugación 3-regulares:

$$\chi^{(2^2,\ 1)} = \varphi^{(5)} + \varphi^{(2,\ 1^3)},$$

$$\chi^{(3,\ 2)} = \varphi^{(4,\ 1)} + \varphi^{(1^5)}.$$

Como $(2^2,\ 1)$ y $(3,\ 2)$ son particiones 3-regulares, $D^{(2^2,\ 1)}$ y $D^{(3,\ 2)}$ son factores de composición con multiplicidad 1 de $S^{(2^2,\ 1)}$ y $S^{(3,\ 2)}$, respectivamente. Más aún, los demas factores de composición de $S^{(2^2,\ 1)}$ y $S^{(3,\ 2)}$

son de la forma D^μ y D^λ para $\mu > (2^2,\ 1)$ y $\lambda > (3,\ 2)$, respectivamente. Luego, debe ser que

$$\varphi^{(2^2,\ 1)} = \varphi^{(2,\ 1^3)} \quad \text{y} \quad \varphi^{(3,\ 2)} = \varphi^{(1^5)}.$$

Se deduce entonces que $D^{(2^2,\ 1)} \cong D^{(2,\ 1^3)}$ y $D^{(3,\ 2)} \cong D^{(1^5)}$; en particular, se tiene que

$$d[S^{(2^2,\ 1)}] = [D^{(5)}] + [D^{(2^2,\ 1)}],$$

$$d[S^{(3,\ 2)}] = [D^{(4,\ 1)}] + [D^{(3,\ 2)}].$$

En conclusión, la matriz de descomposición de $\mathbb{S}_5$ sobre $\mathbb{F}_3$ es la siguiente:

$$\mathbf{D} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

□

c) Para terminar con los ejemplos, supongamos que $p = 5$. Las clases de conjugación de elementos 5-regulares son $[1\ 2\ 3\ 4]$, $[1\ 2\ 3][4,\ 5]$, $[1\ 2][3\ 4]$, $[1\ 2\ 3]$, $[1\ 2]$ y $[id]$. Por tanto, la cantidad de clases de isomorfismos de $\mathbb{F}_5\mathbb{S}_5$-módulos simples es 6 y están representadas por

$$D^{(5)},\ D^{(4,\ 1)},\ D^{(3,\ 2)},\ D^{(3,\ 1^2)},\ D^{(2^2,\ 1)} \text{ y } D^{(2,\ 1^3)}.$$

Por el teorema 4.11, conocemos la imagen del mapa de descomposición de las representaciones dadas por particiones tipo gancho. A saber,

$$d[S^{(5)}] = [D^{(5)}],$$

$$d[S^{(4,\ 1)}] = [D^{(5)}] + [D^{(4,\ 1)}],$$

$$d[S^{(3,\ 1^2)}] = [D^{(4,\ 1)}] + [D^{(3,\ 1^2)}],$$

$$d[S^{(2,\ 1^3)}] = [D^{(3,\ 1^2)}] + [D^{(2,\ 1^3)}],$$

$$d[S^{(1^5)}] = [D^{(1^5)}].$$

En particular, las reducciones de $S^{(4,\ 1)}$, $S^{(3,\ 1^2)}$ y $S^{(2,\ 1^3)}$ son reducibles. Esto también se podía deducir del hecho que 5 divide al entero $\prod($ longitudes de los ganchos de $[\mu])$, para $\mu = (4,\ 1),\ (3,\ 1^2)$ y $(2,\ 1^3)$.

Para encontrar la matriz de descomposición, nos falta conocer las reducciones de $S^{(3,\ 2)}$ y $S^{(2^2,\ 1)}$. Como $p = 5$, tenemos que la reducción de $S^{(3,\ 2)}$ es irreducible; veamos que ocurre con $S^{(2^2,\ 1)}$:

Calculemos las longitudes de los ganchos en el diagrama asociado a $[(2^2,\ 1)]$ y reemplacemos cada nodo del diagrama por la longitud del gancho correspondiente para obtener el tablero

$$\begin{array}{|c|c|} \hline 4 & 2 \\ \hline 3 & 1 \\ \hline 1 & \\ \cline{1-1} \end{array}\ .$$

Luego, $\prod$(longitudes de los gancho de $[(2^2,\ 1)]) = 4!$ y claramente 5 no lo divide. Al ser $(2^2,\ 1)$ una partición 5-regular, se deduce que la reducción módulo 5 de $S^{(2^2,\ 1)}$ es irreducible, es decir que

$$d[S^{(2^2,\ 1)}] = [D^{(2^2,\ 1)}].$$

Sabemos que la reducción de $S^{(1^5)}$ es irreducible, por tanto, debe ser isomorfa a algún D^{μ}, siendo μ una partición 5-regular. Para hallarla, usaremos nuevamente el teorema 4.10:

Supongamos que $v = 0$, entonces los diagramas $[\lambda]$ que cumplen que $[\lambda]/[0]$ es una semigancho de longitud 5 son aquéllos que vienen dados por particiones tipo gancho. Tenemos entonces la siguiente igualdad sobre las clases 5-regulares:

$$\chi^{(5)} - \chi^{(4,\ 1)} + \chi^{(3,\ 1^2)} - \chi^{(2,\ 1^3)} + \chi^{(1^5)} = 0,$$

reemplazando cada carácter por su escritura como combinación lineal de los caracteres de Brauer irreducibles φ^{μ} tenemos que

$$\varphi^{(5)} - (\varphi^{(5)} + \varphi^{(4,\ 1)}) + (\varphi^{(4,\ 1)} + \varphi^{(3,\ 1^2)}) - (\varphi^{(3,\ 1^2)} + \varphi^{(2,\ 1^3)}) + \varphi^{(1^5)} = 0,$$

de donde se deduce que

$$\varphi^{(2,\ 1^3)} = \varphi^{(1^5)},$$

esto es, $D^{(2,\ 1^3)} \cong D^{(1^5)}$.

En conclusión, la matriz de descomposición de $\mathbb{S}_5$ sobre $\mathbb{F}_5$ es la siguiente:

$$\mathbf{D} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Si ordenamos las filas de manera tal que las particiones tipo gancho estén ubicadas por encima de las que no lo son, la matriz de descomposición tiene la forma

$$\mathbf{D} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

como se muestra en el teorema 4.11. □

Bibliografía

[A] Asterisque, *Young Tableaux and Schur functors in algebra and geometry*, 87-88. 1981. Torún, Polonia.

[C-R] C. W. Curtis, I. Reiner, *Methods of Representation Theory, with applications to finite groups and orders*, Wiley Classics Library Edition Published 1990.

[F-H] W. Fulton, J. Harris, *Representation theory, A first course*, Graduate Texts in Mathematics. 1991. Springer-Verlag.

[J] G. D. James, *Representation theory of the symmetric groups*, Lectures Notes in Mathematics, Vol. 682, 1978. Springer-Verlag.

[L] S. Lang, *Algebra, Third Edition.* Addison-Wesley. 1997.

[P] M. H. Peel, *Hook representations of symmetric groups*, Glasgow Math. J. 12. 1971, 136-149.

[S] J. P. Serre, *Representaciones lineales de los grupos finitos.* Ediciones Omega, S. A. 1970.

[V] E. B. Vingberg, *Linear representations of groups*, A Series of Advanced Textbooks in Mathematics. Vol. 2. 1989. Birkhauser Verlag.