UNIVERSIDAD DE GRANADA

Facultad de Ciencias

Grado en Matemáticas

TRABAJO DE FIN DE GRADO

Brauer y la teoría de representación de grupos finitos

Presentado por:
Joaquín Moreno López

Curso académico 2023-2024

Brauer y la teoría de representación de grupos finitos

Joaquín Moreno López

Joaquín Moreno López *Brauer y la teoría de representación de grupos finitos*.

Trabajo de fin de Grado. Curso académico 2023-2024.

Responsable de tutorización

Pascual Jara Martínez
Departamento de Álgebra

Grado en Matemáticas
Facultad de Ciencias
Universidad de Granada

Declaración de originalidad

D./Dña. Joaquín Moreno López

Declaro explícitamente que el trabajo presentado como Trabajo de Fin de Grado (TFG), correspondiente al curso académico 2023-2024, es original, entendido esto en el sentido de que no he utilizado para la elaboración del trabajo fuentes sin citarlas debidamente.

En Granada a 10 de julio de 2024

Fdo: Joaquín Moreno López

A mis abuelos: Ana, Paqui, Luis y Joaquín.

Índice general

Agradecimientos

Agradezco a mis padres la oportunidad que me han dado de dedicar estos años a estudiar, y su infinita paciencia conmigo. Agradezco a mi hermana esa alegría tan característica suya. Agradezco a Natalia todo el cariño y apoyo que me da, y que tanto me ha ayudado. Agradezco a Iván, compañero de batallas en largas noches de estudio. Agradezco también a Pascual, de quien he aprendido mucho este año.

Summary

The purpose of this text is to be a historically supported introduction to modular representation theory.

The text is divided into two main sections:

The first part explains the birth of the representation theory of finite groups. We study the evolution of the concept of character, which was first used by Gauss, and then developed by Weierstrass and Dedekind, who are responsible for creating the modern theory in the context of abelian groups. Afterwards, we produce some of the foundational work of Frobenius in the character theory of general finite groups and make some comments on the simplified versions of the theory created by Schur and Noether. Finally, we introduce briefly the contributions of Dickson, who made the first statements in modular representation theory.

The second part is an analysis of Brauer's work. The basis of modular representation theory was almost completely developed by Brauer. During the 30s, Brauer created the first systematic approach to modular representation theory. This is the content of the chapter "Elementary modular representation theory". The main idea is to create mechanisms to transfer information from characteristic zero to characteristic p. The tool that Brauer invented is reduction mod p, and it is treated in 2.1. Also according to this idea, Brauer developed a complexified version of the natural characters of modular representations, these new characters are called Brauer characters. We study them in 2.2. All these concepts admit a reformulation in terms of Grothendieck groups. This approach was introduced by Swan, and we follow it in 2.3 to prove some classical results. Finally, we illustrate these ideas in an example in 2.4.

During the second half of the 40s, a new trend begins in modular representation theory. The idea is to exploit the p-local structure of the objects studied. Brauer proved during these years what we now call the Three Main Theorems. The purpose of section 3 is to prove these theorems. To do so, we do not follow Brauer's original approach. Instead, we use the module-theoretic approach which was created by Green.

First, we construct induction in 3.2.1, which allows us to transfer structure between subgroups. Then, in 3.2.2 we associate certain invariants to indecomposable modules called vertices and sources. Afterwards, we develop the main tool of the theory, which is Green correspondence, this is done in 3.2.3 and 3.2.5. Once the theory is constructed, we apply it to the study of kG in 3.2.6, and then we prove the three main theorems. Finally, in 3.2.4, we analyse deeply the representation theory of cyclic groups and $SL(2, p)$.

Introducción

Organizamos la introducción tal y como se indica:

1. Objetivos previstos inicialmente

Los objetivos iniciales establecidos en la memoria eran:

(i) Comprender la dimensión y complejidad de la extensión de una teoría.

(ii) Adquisición de técnicas de clasificación de álgebras.

(iii) Comprender la estructura y los problemas planteados en anillos de enteros algebraicos.

(iv) Contextualizar a un matemático en el desarrollo de una teoría.

Estos objetivos han sido cumplidos:

(i) He podido observar en la realización del trabajo que la teoría de representación modular es una teoría muy actual. Hay multitud de conjeturas por estudiar en la materia, y también hay resultados que aún no han sido ni conjeturados. Un ejemplo de esto es la conjetura de Broué. Actualmente no hay ningún enunciado similar para grupos de defecto arbitrarios.

(ii) La teoría de representación modular puede entenderse como un invariante de las álgebras de grupo. Por tanto, todas las técnicas desarrolladas en el trabajo pueden utilizarse para diferenciar álgebras de grupo.

(iii) Los ejemplos particulares en los que uno estudia teoría de representación modular pasan usualmente por considerar un cuerpo de números, y trabajar sobre su anillo de enteros. Luego, es necesario para empezar a trabajar comprender este contexto.

(iv) El trabajo de Brauer en teoría de representación modular ha sido contextualizado en el texto.

2. Antecedentes

La asignatura Álgebra, Grupos y Representaciones es el prerrequisito para lo realizado en este trabajo. En esta asignatura se estudia la teoría en característica 0, que es el antecedente histórico a la teoría modular.

3. Resultados obtenidos y principales fuentes consultadas

Los resultados principales del trabajo son los siguientes:

- Un análisis histórico sobre el nacimiento de la teoría de representación de grupos finitos, y la teoría de representación modular elemental. La principal fuente consultada ha sido [Haw71].
- Un análisis del trabajo de Brauer en teoría de representación modular. La principal fuente consultada han sido los artículos originales de Brauer.
- Un desarrollo de la teoría de representación modular elemental. Se demuestran resultados clásicos importantes como:
    - Teorema de Brauer sobre el número de irreducibles modulares.
    - Propiedades de la matriz de Cartan: Simetría. Su determinante es una potencia de p.
    - Relaciones de ortogonalidad para caracteres de Brauer.
    - Propiedades del triángulo *cde*.

  Las principales fuentes consultadas son: [Ser77, CC81].
- Un desarrollo de la teoría de bloques desde el punto de vista de la teoría de representación local. Los principales resultados desmostrados son los tres grandes teoremas de Brauer. La principal fuente consultada es [Alp86].

Parte I.

La teoría de representación de grupos finitos antes de Brauer

1. De la teoría de representación de grupos finitos ordinaria a la modular

1.1. De Gauss a Dedekind

En el S. XIX Gauss publica las "Disquisitiones Arithmeticae". En este texto fundamental es donde se utiliza por primera vez el término carácter (cf. Art 230 [Gau63]). Este se usa en referencia a ciertas características de las formas cuadráticas estudiadas en el texto.

En el trabajo de Gauss hay implícitamente nociones que hoy identificamos como grupo–teóricas. Concretamente, Gauss viene a probar que las clases de formas cuadráticas enteras con cierto discriminante forman un grupo abeliano.

Dirichlet afrontó en años posteriores la tarea de simplificar y extender el trabajo de Gauss. A él le debemos la notación χ, que introdujo para referirse a los caracteres en el sentido Gaussiano interpretándolos como funciones numéricas. En 1855, Dirichlet dejó Berlin para convertirse en el sucesor de Gauss en Gotinga. En aquellos años Dedekind era "Privadotzent" allí, y asistió durante tres años a las lecciones de Dirichlet en teoría de números. La idea de Dirichlet era publicar un libro en torno a este trabajo, pero murió antes de poder llevar a cabo esta empresa. En su lugar, sería su alumno Dedekind, quien con las notas de clase, y sus propias aportaciones publicaba en 1863 la primera edición de sus lecciones en teoría de números [Ded63].

En la tercera edición del texto, Dedekind añade en los suplementos una definición general de carácter para grupos abelianos. Este hace un breve comentario sobre ellos en el que podríamos decir que está implícita toda la teoría asociada a estos objetos. Los caracteres los define esencialmente como funciones de un grupo abeliano valoradas en los complejos G tal que $\chi(ab) = \chi(a)\chi(b)$. Dedekind dice sobre tales funciones que puede demostrarse que existen y que están controladas a través del teorema de estructura de los grupos finitos abelianos. (cf. [Haw71] p149).

En cualquier caso, Dedekind no fue el responsable de popularizar esta teoría, el responsable fue Weber a través de su exposición al respecto en [Web95]. De esta manera, para el año 1896, la teoría de caracteres para grupos abelianos era bien conocida.

1.2. De Dedekind a Frobenius

Sobre 1880, Dedekind comienza a trabajar en torno al concepto de determinante de grupo. Este concepto es introducido por él mismo en relación al estudio del discriminante en extensiones normales de cuerpos ([Haw71] p.150). Vamos a definir esta noción: Sea K una extensión normal del cuerpo de los números racionales, y sea $G = \{g_1, ..., g_n\}$ su grupo de Galois. Tomamos ahora una base en K $\{\omega_1, ..., \omega_n\}$, y observamos que el discriminante Δ viene dado por $\Delta = D^2$, donde D es el siguiente determinante:

$$D = \begin{vmatrix} \omega_1 g_1 & \omega_2 g_1 & ... & \omega_n g_1 \\ \omega_1 g_2 & \omega_2 g_2 & ... & \omega_n g_2 \\ ... & ... & ... & ... \\ \omega_1 g_n & \omega_2 g_n & ... & \omega_n g_n \end{vmatrix}.$$

En particular, era frecuente, construir un sistema de elementos en K compuesto de un $\omega \in K$, y sus conjugados $\omega g_1, ..., \omega g_n$. Con este sistema, el determinante D, nos queda así:

$$D = \begin{vmatrix} \omega g_1 g_1 & \omega g_2 g_1 & ... & \omega g_n g_1 \\ \omega g_1 g_2 & \omega g_2 g_2 & ... & \omega g_n g_2 \\ ... & ... & ... & ... \\ \omega g_1 g_n & \omega g_2 g_n & ... & \omega g_n g_n \end{vmatrix},$$

de donde es sencillo deducir el determinante de grupo, en tanto que solo hay que omitir el ω. Así pues, dado un grupo $G = \{g_1, ..., g_n\}$, en el que g_1 representa la identidad, definimos un conjunto de indeterminadas x_i asociadas al grupo mediante la relación $x_i = x_{g_i}$, y la operación natural entre ellas $x_i x_j = x_{g_i g_j} = x_k$, para $g_k = g_i g_j$. El determinante de grupo $\theta(x_1, ..., x_n)$ vendrá dado por

$$\theta(x_1, ..., x_n) = \begin{vmatrix} x_{g_1 g_1^{-1}} & x_{g_1 g_2^{-1}} & ... & x_{g_1 g_n^{-1}} \\ x_{g_2 g_1^{-1}} & x_{g_2 g_2^{-1}} & ... & x_{g_2 g_n^{-1}} \\ ... & ... & ... & ... \\ x_{g_n g_1^{-1}} & x_{g_n g_2^{-1}} & ... & x_{g_n g_n^{-1}} \end{vmatrix}.$$

El problema que afronta Dedekind es el de la factorización de este determinante, y la relación de las propiedades de esta factorización con propiedades del grupo G. Una de las primeras cosas que descubre, es que si G es abeliano, sus caracteres aparecen en la factorización del determinante de grupo

$$\theta = \prod_{s=1}^{n} (\sum_{i=1}^{n} \chi_s(g_i) x_i).$$

En particular, observa, que para un grupo abeliano, tal determinante factoriza completamente en factores lineales. A continuación, Dedekind estudia determinantes de grupos no abelianos, en concreto estudia el grupo S_3. Sea $g_1 = 1$, $g_2 = (1,2,3)$, $g_3 = (1,3,2)$, $g_4 = (2,3)$, $g_5 = (1,3)$ y $g_6 = (1,2)$. Entonces, el determinante de grupo de S_3 factoriza como

$$\theta = (u+v)(u-v)(u_1 u_2 - v_1 v_2)^2$$

en donde:

$$\begin{aligned} u &= x_1 + x_2 + x_3 \\ v &= x_4 + x_5 + x_6 \\ u_1 &= x_1 + \rho x_2 \rho^2 x_3 \\ u_2 &= x_1 + \rho^2 x_2 + \rho x_3 \\ v_1 &= x_4 + \rho x_5 + \rho^2 x_6 \\ v_2 &= x_4 + \rho^2 x_5 + \rho x_6 \end{aligned}$$

para ρ una raíz cúbica primitiva de la unidad.

Inspirado por la situación de grupos abelianos, Dedekind intentaría buscar un "sistema de números hipercomplejos" (lo que hoy conocemos como álgebra asociativa), en el que tales determinantes no abelianos factoricen completamente. Dedekind investigaría algunos ejemplos concretos más, y eventualmente formalizaría la siguiente conjetura en torno al número de factores lineales en el determinante de un grupo:

Teorema 1.1 (Conjetura de Dedekind). *El número de factores lineales en el determinante de grupo de G es $[G : G']$, en donde G' es el subgrupo derivado.*

Esta conjetura llegaría a manos de Frobenius a través de una carta de Dedekind del 25 de marzo de 1896. Frobenius había ocupado el puesto de Kronecker en 1892 en Berlín, y para el momento en el que se envía la carta, ya era reconocido como un autor relevante en cuestiones relacionadas con grupos. La conjetura de Dedekind, y la relación de la factorización del determinante de un grupo y su estructura, serían los motores que llevarían a Frobenius a desarrollar una teoría de caracteres para grupos no abelianos.

Antes de comentar el trabajo de Frobenius, es conveniente introducir algunas ideas sobre sistemas de números hipercomplejos que Frobenius utiliza de manera decisiva para su introducción de los caracteres generalizados.

Weierstrass en una carta a Schwarz propone una formulación algebraica para hablar de ciertos sistemas de números que se postulan como extensiones de los números complejos. Concretamente, en ella se considera el problema de construir un cuerpo basado en sistemas de números de la forma

$$x_1 e_1 + \cdots + x_n e_n$$

para $x_i \in \mathbb{R}$. Definir una suma es trivial, sin embargo, el producto es más complicado. Weierstrass muestra que tal producto queda determinado por n^3 números reales a_{ijk} definidos por las igualdades

$$e_j e_k = \sum_{i=1}^{n} a_{ijk} e_i.$$

Además, la asociatividad y la conmutatividad se reduce a las siguientes condiciones sobre los coeficientes de estructura a_{ijk}:

$$a_{ijk} = a_{ikj}$$

$$\sum_i a_{irs}a_{kit} = \sum_i a_{irt}a_{kis}.$$

Estas condiciones, de verificarse, nos dan un anillo conmutativo. Weierstrass demuestra que para $n > 2$ no es posible obtener un cuerpo.

Dedekind por su parte, estudió sistemas similares a estos en el Suplemento X (Sección 199). En él, considera una extensión finita Ω de $\mathbb{Q}$. Si $e_1, \ldots, e_n$ es una base de esta, se tiene que si $e \in \Omega$, entonces

$$e = x_1e_1 + \cdots + x_ne_n.$$

Para expresar que $e_je_k \in \Omega$ utiliza la siguiente condición:

$$e^2 = 2\sum_i H_ie_i,$$

en donde H_i es un polinomio homogéneo de grado 2 con variables x_i y coeficientes racionales. Estas funciones las utiliza para estudiar la estructura de Ω. Concretamente, si derivamos la última ecuación con respecto a x_r obtenemos

$$ee_r = \sum_i \frac{\partial H_i}{\partial x_r}e_i$$

que para $H = det(A')$, con $A' = (\frac{\partial H_i}{\partial x_j})_{ij}$, se tiene que e es un autovalor de A'. Además, todos los conjugados de e, que notamos por $e^{(s)}$, también son autovalores de A'. Por tanto, $det(A' - x) = \prod_s(e^{(s)} - x)$.

Si ponemos $x = 0$, obtenemos que

$$H = det(A') = \prod e^{(s)} = N(e),$$

y vemos que este, que es un polinomio homogéneo de grado n en las variables x_i, descompone en factores lineales

$$\prod_s(\sum_i e_i^{(s)}x_i).$$

Dedekind también consigue un resultado similar considerando los x_i como valores complejos. Concretamente, prueba el siguiente teorema

Teorema 1.2. *Supongamos que los n^3 números complejos a_{ijk} satisfacen las condiciones de asociatividad y conmutatividad antes expuestas, y sea (p_{ij}) la matriz dada por*

$$p_{ij} = \sum_{r,s=1}^{n} a_{rsr}a_{sij}.$$

Entonces, si $det(p_{ij}) \neq 0$, existen números complejos $e_i^{(s)}$ con $i, s = 1 \ldots, n$ tales que para cada $e_1^{(s)}, \cdots, e_n^{(s)}$ se cumple la relación de multiplicación. Además, $det(e_i^{(s)}) \neq 0$ luego los sistemas son linealmente independientes.

Después demuestra que

$$det(A) = \prod_{s=1}^{n} (\sum_{i=1}^{n} e_i^{(s)} x_i)$$

en donde $A = \sum_{k=1}^{n} a_{ijk} x_k$.

Frobenius en su aproximación parte de la observación de que si a_{ijk} es un sistema de coeficientes que verifica la relación de asociatividad y conmutatividad, entonces las matrices $A_k = (a_{ijk})$ conmutan, y $A = \sum_{k=1}^{n} A_k x_k$.

Además, Frobenius contaba con el siguiente resultado:

Teorema 1.3. *Dadas m matrices $A, B \ldots$ de orden n que conmutan, existe una ordenación $a_1, \ldots, a_n$, $b_1, \ldots, b_n, \ldots$ de las raíces características de las matrices tal que para cualquier polinomio en las m variables $u, \ldots$, las raíces características de $f(A, B, \ldots)$ son $f(a_1, b_1, \ldots)$,$f(a_2, b_2, \ldots)$,...*

De esta forma, se puede obtener un sistema en la línea del de Dedekind o Weierstrass partiendo de matrices que conmutan. Si tomamos las matrices $A_1, \ldots, A_m$ y consideramos el polinomio $f(u_1, \ldots, u_m) = u_1 x_1 + \cdots + u_m x_m$, el teorema nos dice que las raíces características de

$$A = f(A_1, \ldots, A_m) = \sum_{k=1}^{m} A_k x_k$$

son las n funciones lineales de x_i de la forma $r_1^{(s)} x_1 + \cdots + r_m^{(s)} x_m$ con $s = 1, \ldots, m$, donde $r_i^{(s)}$ es la s-ésima raíz característica de A_i. De ahí se sigue que

$$det(A) = \prod_{s=1}^{n} (\sum_{i=1}^{m} r_i^{(s)} x_i).$$

Además, si escribimos $A_k = (a_{ijk})$ y tomamos $m = n$, entonces $A_j A_k = A_k A_j$ implica la relación de asociatividad. Si además imponemos la de conmutatividad sobre los a_{ijk} entonces,

$$A_j A_k = \sum_{i=1}^{m} a_{ijk} A_i,$$

y de acuerdo con el teorema 1.3, el lado de la izquierda tiene por raíz característica s-ésima a $r_j^{(s)} r_k^{(s)}$; y el de la derecha a $\sum_{i=1}^{n} a_{ijk} r_i^{(s)}$. En otras palabras,

$$r_j^{(s)} r_k^{(s)} = \sum_{i=1}^{n} a_{ijk} r_i^{(s)}.$$

Vamos a reunir estos resultado en el siguiente teorema:

Teorema 1.4. *Sean los $n^2 m$ números a_{ijk} ($i, j = 1, \ldots, n$; $k = 1, \ldots, m$). Supongamos que cumplen la igualdad*

$$\sum_{s=1}^{n} a_{psj} a_{sqk} = \sum_{s=1}^{m} a_{psk} a_{sqj}.$$

Entonces, si $A_k = (a_{ijk})$, *(*$k = 1, \ldots, m$*) existen números* $r_k^{(s)}$ *(*$s = 1, \ldots, n$*) tales que*

$$det(\sum_{k=1}^{m} A_k x_k) = \prod_{s=1}^{n}(\sum_{i=1}^{m} r_i^{(s)} x_i).$$

Además, si $m = n$*, y* $a_{ijk} = a_{ikj}$*, los* $r_k^{(s)}$ *son las únicas soluciones a*

$$r_j^{(s)} r_k^{(s)} = \sum_{i=1}^{n} a_{ijk} r_i^{(s)}.$$

Por último, cuando $det(p_{ij}) \neq 0$*, se tendrá que* $det(r_k^{(s)}) \neq 0$*.*

Hecha esta disgresión retomamos el trabajo de Frobenius en torno al problema del determinante de grupo.

El 30 de julio de 1896 Frobenius presenta a la Academia de Berlín los trabajos [Fro96b, Fro96a], siendo el primero de estos el que es considerado como el primer artículo en teoría de representación de grupos finitos, a pesar de que el concepto de representación es posterior.

Observemos que si G es un grupo abeliano finito, y tomamos $A = (x_{g_i g_j^{-1}})$, y A_k lo definimos como la matriz obtenida poniendo $x_{g_i g_j^{-1}} = 1$ si $g_i g_j^{-1} = g_k$, y 0 en otro caso, se tiene que

$$A = \sum_{k=1}^{n} A_k x_k,$$

y como G es abeliano, $A_j A_k = A_k A_j$. Aplicando el teorema 1.4, obtenemos la existencia de n sistemas linealmente independientes $r_1^{(s)}, \ldots, r_n^{(s)}$ tales que

$$\theta = detA = \prod_{s=1}^{n}(\sum_{i=1}^{m} r_i^{(s)} x_i).$$

Por comparación, observamos que $\chi^{(s)}(g_k) = r_k^{(s)}$. Por tanto, hemos visto que a través del teorema de Frobenius podemos recuperar la descomposición de Dedekind. Por supuesto, si perdemos la conmutatividad de G, dejamos de estar en las condiciones del teorema. Frobenius frente a esto propone identificar en A formalmente

$$x_{ab} = x_{ba} \quad a, b \in G.$$

De esta forma θ pasa de ser una función en n variables, a una función en k variables donde k es el número de clases de conjugación en G. Además, esta identificación arregla la conmutatividad y nos devuelve al contexto del teorema 1.4.

A continuación utilizamos θ^*, A^*, A_i^* para referirnos a θ, A, A_i tras haber hecho la anterior identificación. Además notamos por $C_1, \ldots, C_k$ a las clases de conjugación de G, siendo C_1 la que contiene la identidad, y x_α la variable que corresponde a la clase C_α.

El teorema nos dice ahora que

$$\theta^*(x_1, \ldots, x_k) = det(A^*) = \prod_{s=1}^{n} (\sum_{\alpha=1}^{k} r_\alpha^{(s)} x_\alpha),$$

de tal manera que obtenemos una relación similar a la que teníamos en el caso abeliano. Frobenius obtiene propiedades importantes de los valores $r_\alpha(s)$, que parecen jugar el papel de los caracteres de Dedekind en este nuevo contexto.

Teorema 1.5. *Sea $h_{\alpha\beta\gamma}$ el número de soluciones de $abc = e$ sujeto a las condiciones $a \in C_\alpha$, $b \in C_\beta$, $c \in C_\gamma$. Sea también h_α el número de elementos en C_α, y pongamos*

$$a_{\alpha\beta\gamma} = \frac{h_{\alpha'\beta\gamma}}{h_\alpha}$$

donde C'_α es la clase de conjugación que contiene a los inversos de C_α. Entonces $a_{\alpha\beta\gamma}$ está en las condiciones del teorema 1.4. Por ello existen k sistemas linealmente independientes $r_1^{(s)}, \ldots, r_k^{(s)}$ $(s = 1, \ldots, k)$ tales que

$$r_\beta^{(s)} r_\gamma(s) = \sum_{\alpha=1}^{k} a_{\alpha\beta\gamma} r_\alpha^{(s)},$$

y

$$det(\hat{A}) := det(\sum_{\gamma=1}^{k} a_{\alpha\beta\gamma} x_\gamma) = \prod_{s=1}^{n} (\sum_{\alpha=1}^{k} r_\alpha^{(s)} x_\alpha)$$

Además, $det(\hat{A})$ comparte los factores lineales de θ^*, luego

$$\theta^*(x_1, \ldots, x_k) = det(A^*) = \prod_{s=1}^{n} (\sum_{\alpha=1}^{k} r_\alpha^{(s)} x_\alpha)$$

Este teorema nos muestra que aunque el determinante de grupo no descompone en general en factores lineales, dos determinantes muy relacionados, a saber θ^* y $det(\hat{A})$, sí que tienen esta propiedad. De hecho, tienen las mismas k-tuplas linealmente independientes como coeficientes de sus factores lineales.

Teniendo esto en cuenta, no es sorpredente que Frobenius defina los k caracteres generalizados $\chi^{(s)}$ según la fórmula

$$\chi^{(s)}(g) = \frac{\lambda^{(s)}}{h_\alpha} r_\alpha^{(s)}$$

en donde $\frac{\lambda^{(s)}}{h_\alpha}$ es un factor de proporcionalidad. Hecha esta definición retomamos la conjetura de Dedekind.

Sea $\Phi = \sum_{g \in G} \mu_g x_g$ un factor lineal de θ. Entonces se cumple que $\mu_a \mu_b = \mu_{ab}$ para todo $a, b \in G$. En consecuencia, $\mu_{aba^{-1}b^{-1}} = 1$, luego podemos ver μ como una función de G/G'. Si definimos ψ por la fórmula $\psi(G'a) = \mu_a$, se tendrá entonces que

$$\psi(G'aG'b) = \psi(G'a)\psi(G'b).$$

Por tanto, ψ es un carácter en el sentido de Dedekind para el grupo abeliano G/G'. Es claro que distintos factores lineales de θ dan lugar a distintos caracteres de G/G', por lo que el número de factores lineales de θ es menor o igual que el orden de G/G'.

Frobenius, a través de argumentos con determinantes, prueba que si ψ es un carácter de G/G', entonces $\Phi = \sum \mu_g x_g$, con $\mu_g = \psi(G'g)$, es un factor de θ, y θ/Φ no es divisible por Φ. De esta manera prueba que el número de factores lineales de θ es igual al número de caracteres de G/G', o lo que es lo mismo, al orden de G/G'.

Además, en virtud del teorema 1.5, un factor lineal $\Phi = \sum \mu_g x_g$ de θ satisface

$$\Phi^* = \sum_{\alpha=1}^{k} (\sum_{g \in C_\alpha} \mu_g) x_\alpha = \sum_{\alpha=1}^{k} (\frac{h_\alpha x_\alpha}{\lambda}) x_\alpha,$$

y como μ_g permanece constante en las clases de conjugación C_α, se sigue que $\mu_g = x_\alpha/\lambda$. Tomando $\lambda = 1$, se tiene

$$\Phi = \sum \chi(g) x_g.$$

Hemos relacionado los caracteres generalizados con los coeficientes de los factores lineales de θ. Esto sugiere un método para estudiar los factores no lineales.

Sea

$$\theta = \prod_{s=1}^{l} \Phi_s^{e(s)} \quad , f^{(s)} = deg(\Phi_s)$$

la factorización de θ en irreducibles. Entonces

$$\theta^* = \prod_{s=1}^{l} (\Phi_s *)^{e(s)},$$

pero de acuerdo con el teorema 1.5,

$$\theta * = \prod_{s=1}^{k} (\eta_s)^{g(s)},$$

en donde η_s son los factores lineales de θ^*. Lo natural es que $k = l$, y que pueda escogerse una ordenación para que

$$(\Phi_s^*)^{e(s)} = (\eta_s)^{g(s)}, \quad \Phi_s^* = (\eta_s)^{f(s)}.$$

Esto resulta ser cierto. Vamos a tomar esto como hipótesis de trabajo: sea

$$\Phi^* = (\frac{1}{\lambda} \sum h_\alpha \chi_\alpha x_\alpha)^f.$$

Si derivamos x_1 $f-1$ veces con respecto a obtenemos

$$\frac{1}{f!}\frac{\partial^{f-1}\Phi^*}{\partial x_1^{f-1}} = \frac{1}{\lambda}\sum h_\alpha \chi_\alpha x_\alpha.$$

Si ponemos $f = \lambda$, entonces

$$\frac{1}{(f-1)!}\frac{\partial^{f-1}\Phi^*}{\partial x_1^{f-1}} = \sum h_\alpha \chi_\alpha x_\alpha = \eta.$$

Por otro lado,

$$\begin{aligned}\frac{1}{(f-1)!}\frac{\partial^{f-1}\Phi^*}{\partial x_1^{f-1}} &= \frac{1}{(f-1)!}(\frac{\partial^{f-1}\Phi}{\partial x_1^{f-1}})^* \\ &= (\sum \mu_g x_g)^* \\ &= \sum_{\alpha=1}^{k}(\sum_{g\in C_\alpha}\mu_g)x_\alpha\end{aligned}$$

en donde μ_g toma el valor del coeficiente de $x_e^{f-1}x_g$ en Φ si $g \neq e$, y toma el valor f en caso contrario. Por comparación de las expresiones, parece que de nuevo μ_g ha de permanecer constante en las clases de conjugación, luego $\chi(g) = \mu_g$. Todas estas ideas se utilizan en la demostración del siguiente teorema:

Teorema 1.6. *Si Φ es un factor irreducible de θ, entonces μ_g tal y como lo hemos definido es un carácter de G (con $\lambda = deg(\Phi)$). Además, factores distintos determinan caracteres distintos, y todos surgen de esta manera, en tanto que el número de factores irreducibles de θ es igual al número de clases de conjugación de G: $l = k$.*

La caracterización de los caracteres como los coeficientes μ_g es una herramienta fundamental en el análisis de θ. A través de este teorema, Frobenius consigue dar fórmulas para expresar los coeficientes de los factores irreducibles en términos de los caracteres.

En resumen, los caracteres de Frobenius, surgen a través de la investigación de los determinantes de grupo que introduce Dedekind.

1.3. De Frobenius a Schur y Noether

Una vez Frobenius desarrolla su teoría de caracteres (cf. [Fro96b]), y la aplica al estudio del determinante de grupo (cf. [Fro96a, Fro03]), Frobenius define el concepto de representación y aplica la teoría desarrollada a su estudio (cf. [Fro97, Fro99]).

De esta manera, en cuestión de una década, Frobenius desarrolla las bases de la teoría de representación de grupos finitos.

La aproximación de Frobenius tenía el problema de ser muy compleja debido a su predilección por argumentos basados en la utilización de determinantes. Por ello, en años sucesivos surgieron reformulaciones de la teoría.

Un ejemplo es la de Burnside (cf. [Bur04]), que se basaba en el uso de la teoría de formas hermíticas. Sin embargo, la más exitosa, y la más sencilla, es la exposición de Schur en [Sch05]. Esta se basa en la utilización de argumentos elementales de álgebra lineal. De hecho, es en este artículo que aparece el conocido hoy como Lema de Schur.

Finalmente, es interesante también citar la exposición de Noether en [Noe29], esta es la primera vez que se hace una exposición módulo–teórica de la teoría de representaciones. En este artículo, aprovecha la teoría de anillos semisimples de Wedderburn para deducir los resultados clásicos de la teoría de Frobenius.

1.4. De la teoría ordinaria a Dickson

Podríamos decir que para comienzos del siglo XX, ya había cierto control sobre la teoría de representación de grupo finitos sobre el cuerpo de los números complejos, en tanto que se había ya desarrollado la exposición de Frobenius, y la simplificación de Schur.

Era natural entonces estudiar el problema análogo en característica p. El primero en afrontar este problema fue Dickson en una serie de artículos publicados a principios de siglo ([Dic07a, Dic07b, Dic03]).

Dickson observa que si p no divide al orden del grupo, la teoría de Frobenius sigue siendo esencialmente válida, sin embargo, cuando el orden del grupo a estudiar es divisible por p surgen patologías que anulan la teoría de característica 0.

Tras el trabajo de Dickson, habría que esperar varias décadas hasta el resurgimiento de la teoría modular con el trabajo de Brauer, que es el que vamos a estudiar con detalle en la siguiente parte.

Parte II.

Brauer y la teoría de representación modular

2. Teoría de representación modular elemental

2.1. La técnica de reducción mod $\mathfrak{p}$ y el homomorfismo de descomposición

En [RB37], Brauer y su alumno Nesbitt, publicaron la primera sistematización de la teoría de representación modular. En este texto se introducen algunos de los conceptos fundamentales en lo que será el devenir de la teoría en sucesivas décadas. Entre estos, el primero es la reducción mod $\mathfrak{p}$.

La idea es sencilla, uno tiene en algún sentido cierto control sobre la teoría de representación de grupos finitos en el contexto de la característica 0. Para proceder al estudio del caso análogo en característica p, a uno le gustaría disponer de un mecanismo para obtener representaciones modulares a partir de representaciones ordinarias. Esto es precisamente lo que formaliza Brauer.

Así pues, comenzamos estableciendo un contexto algebraico apropiado: En lo que sigue supondremos G un grupo finito y $(K, \mathcal{O}, k)$ un sistema p–modular, esto es, un anillo de valoración discreta $\mathcal{O}$, con cuerpo de fracciones K, ideal maximal $\mathfrak{p} = \pi\mathcal{O}$, y cuerpo residual $k = \mathcal{O}/\mathfrak{p}$ de característica p.

Usualmente estos sistemas se formarán de las siguientes maneras:

- Dado un cuerpo de números K, tomamos una valoración $\mathfrak{p}$–ádica no arquimediana, seleccionamos entonces el anillo de valoración asociado $\mathcal{O}$, y el cuerpo residual $k = \mathcal{O}/\mathfrak{p}$.
- En las condiciones anteriores se puede escoger K como la completación $\mathfrak{p}$–ádica del cuerpo de números, de tal manera que ganamos que el anillo de valoración pasa a ser completo en la topología $\mathfrak{p}$–ádica.

Nuestro primer objetivo será probar que dada una K–representación de G, esta es K–equivalente a una $\mathcal{O}$–representación. En lenguaje de módulos, partimos de un KG–módulo V (Todos los módulos los consideramos finitamente generados) , y pretendemos encontrar algún $\mathcal{O}G$–retículo en V (esto es un $\mathcal{O}G$–módulo M con una $\mathcal{O}$–base finita) tal que $KM = V$.

Siempre podemos construir un módulo con estas características. Basta tomar una K–base de V $\{v_1, ..., v_n\}$ y definir $M = \sum_{i=1}^{n} \mathcal{O}Gv_i$. Se sigue que M es finitamente generado sobre $\mathcal{O}$ y además es $\mathcal{O}$–libre de torsión (Como $\mathcal{O}$ es un DIP, eso basta para que sea libre), luego M es un $\mathcal{O}G$–retículo. Puesto que es claro que $KM = V$ por construcción, M es un módulo con las condiciones exigidas.

Una vez tenemos tal M, podemos reducirlo a través de la proyección canónica $\overline{M} = M/\mathfrak{p}M$. Se tendrá entonces que $\overline{M}$ es un módulo anulado por $\mathfrak{p}$, luego adquiere estructura de kG–módulo a través de la acción:

$$(\sum_{g\in G} \overline{a_g} g)\overline{m} = \sum_{g\in G} \overline{a_g g m} \qquad a_g \in \mathcal{O}, m \in M$$

En resumen, la reducción consiste en dado un KG–módulo V, tomar un $\mathcal{O}G$–retículo M en V tal que $KM = V$, y pasar al cociente $\overline{M}$, de tal manera que se obtiene un kG–módulo, es decir, una representación modular.

Hay que destacar que en principio hay más de una elección posible para un $\mathcal{O}G$–retículo en un KG–módulo dado V, y diferentes $\mathcal{O}G$–retículos pueden darnos representaciones modulares no isomorfas.

Por ejemplo, sea $G = \langle x | x^2 \rangle$ el grupo cíclico de orden 2 generado por x. Considérense las $\mathbb{Q}$-representaciones

$$\rho_1(x) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad \rho_2(x) = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$$

Estas representaciones son $\mathbb{Q}$–equivalentes, pero al reducir mod $2\mathbb{Z}_{(2)}$, obtenemos representaciones modulares no $\mathbb{Z}_2$–equivalentes.

A pesar de esta irregularidad, los factores de composición de representaciones modulares obtenidas a través de reducir un KG–módulo dado, son independientes de la elección del $\mathcal{O}G$–retículo. Para trabajar a nivel de factores de composición, conviene utilizar el leguaje de los grupos de Grothendieck. Esta aproximación a la teoría fue introducida por Swan (cf. [Swa60, Swa63]), y es la utilizada en el texto de Serre [Ser77]. En esta sección seguimos el texto [CC81].

Proposición 2.1 (La reducción es única en el grupo de Grothendieck). *Dados M y N $\mathcal{O}G$–retículos tales que $KM = KN = V$, se sigue que $[\overline{M}] = [\overline{N}]$ en el grupo de Grothendieck $G_0(kG)$.*

Prueba. observamos que $M + N$ es un $\mathcal{O}G$–retículo en V tal que $K(M + N) = V$. Por tanto, podemos probarlo para $\mathcal{O}G$–retículos L y M, tales que $L \subset M$. Además como M es noetheriano, podemos suponer también que L es maximal.

Afirmamos que $\mathfrak{p}M \subset L$, de no ser así se tendría que $L \subset \mathfrak{p}M + L$. Por maximalidad de L, $\mathfrak{p}M + L = M$, y el lema de Nakayama nos diría que $M = L$, lo cual no es posible. En consecuencia tenemos que:

$$\mathfrak{p}L \subset \mathfrak{p}M \subset L \subset M$$

Queremos probar que $[\overline{L}] = [\overline{M}]$ en $G_0(kG)$. Esto es lo mismo que probar que $\overline{L}$ y $\overline{M}$ contienen los mismos factores de composición.

Observamos que como mínimo tienen los de $L/\mathfrak{p}M$ en común, así que hay que ver que $\mathfrak{p}M/\mathfrak{p}L$, tiene los mismos factores que M/L.

Observamos que $\mathfrak{p} = (\pi)$ es principal, luego

$$\frac{\mathfrak{p}M}{\mathfrak{p}L} = \frac{\pi M}{\pi L}$$

y la multiplicación por π nos da un isomorfismo entre $M/L \simeq \mathfrak{p}M/\mathfrak{p}L$. En consecuencia, los módulos tienen los mismos factores de composición sobre kG. □

Una vez probado esto, observamos que la reducción nos da una aplicación

$$d : G_0(KG) \to G_0(kG) \qquad [V] \mapsto [\overline{M}]$$

en donde M es cualquier $\mathcal{O}G$–retículo en V tal que $KM = V$. Esta aplicación está bien definida por la proposición anterior, y además resulta ser un homomorfismo de grupos abelianos. Este el contenido de la siguiente proposición

Proposición 2.2. *$d : G_0(KG) \to G_0(kG)$ es un homomorfismo de grupos abelianos que llamamos homomorfismo de descomposición.*

Prueba.

Para probar que d define un homomorfismo, hemos de ver que es aditivo sobre cadenas exactas cortas. Sea entonces una tal cadena

$$0 \to V_1 \to V_2 \to V_3 \to 0.$$

Vamos a tomar un $\mathcal{O}G$–retículo M_2 en V_2 tal que $KM_2 = V_2$. Entonces, $\phi(M_2) = M_3$ es un $\mathcal{O}G$–retículo en V_3 tal que

$$KM_3 = K\phi(M_2) = \phi(KM_2) = \phi(V_2) = V_3.$$

Por su parte, aprovechando la inyectividad, ponemos $M_1 = V_1 \cap M_2$. Así obtenemos una cadena exacta corta en $\mathcal{O}G$–*mod*

$$0 \to M_1 \to M_2 \to M_3 \to 0.$$

Ahora como M_3, es $\mathcal{O}$–proyectivo, la cadena vista en $\mathcal{O}$–módulos escinde, y tensorizar por k conserva la exactitud. De esta manera conseguimos la siguiente cadena exacta

$$0 \to k \otimes M_1 \to k \otimes M_2 \to k \otimes M_3 \to 0.$$

Si ahora utilizamos la identificación $k \otimes M_i \simeq \overline{M}_i$, se queda

$$0 \to \overline{M}_1 \to \overline{M}_2 \to \overline{M}_3 \to 0,$$

de donde $[\overline{M}_2] = [\overline{M}_1] + [\overline{M}_3]$, y por tanto $d(V_2) = d(V_1) + d(V_3)$, tal y como queríamos probar. □

En el artículo [RB37], una vez explicado el procedimiento de reducción, este se aplicaba a los irreducibles ordinarios. Al reducirlos estos no tenían porque seguir siendo irreducibles como representaciones modulares, de esta manera, tomando las multiplicidades de los factores de composición de las representaciones modulares asociadas a las irreducibles ordinarias, Brauer definía los números de descomposición. Estos se configuran como un invariante numérico producto del tránsito de la característica 0 a la característica p.

En el lenguaje de los grupos de Grothendieck, uno puede recuperar los números de descomposición sin más que observar que tomando las bases canónicas de los grupos, $\{[Z_1], ..., [Z_s]\}$, las clases de isomorfía de irreducibles ordinarios; y $\{[F_1], ..., [F_r]\}$, las clases de isomorfía de irreducibles modulares, el homomorfismo de descomposición queda definido a través de las relaciones

$$d[Z_i] = \sum_{j=1}^{r} d_{ij}[F_j] \qquad 1 \leq i \leq s.$$

en donde los número d_{ij}, son los números de descomposición de Brauer. La matriz $D = (d_{ij})^t$ es la matriz de descomposición.

2.2. Los caracteres de Brauer

El segundo concepto introducido en el artículo [RB37] , es el de los caracteres modulares o de Brauer. En vista del éxito de la teoría de caracteres de Frobenius, era natural construir una suerte de teoría análoga para el contexto modular. Así pues, Brauer definió para los elementos del grupo que era posible (estos son los elementos p–regulares) una expresión compleja del carácter natural de las representaciones modulares.

Estos objetos serán especialmente relevantes en el trabajo de Brauer, ya que tenía predilección por los métodos carácter-teóricos. El texto de Goldschmidt [Gol80], escrito en el espíritu de estos trabajos, habla de su teoría modular como una "investigación sobre las propiedades aritméticas de los caracteres de grupo". En esta sección sigo de cerca los textos [Ser77, CC81].

De nuevo sea G un grupo finito. Definimos el conjunto G_{reg} de valores p–regulares de G, estos son los elementos en G con orden coprimo a p. Sea m su exponente, es decir, el mcm de los órdenes de sus elementos. Sea además $(K, \mathcal{O}, k)$ un sistema p–modular tal que $char(K) = 0$, y K sea lo suficientemente grande para G. Esto quiere decir que K contiene todas las raíces m–ésimas de la unidad para K.

Lo primero que hacemos es establecer una correspondencia entre el grupo de raíces m–ésimas de la unidad en K, llámese este grupo μ_K; y el grupo de raíces m–ésimas de la unidad en k, llámese este grupo μ_k. Esta correspondencia nos la da la técnica de reducción mod $\mathfrak{p}$, pues al ser m coprimo con p, establece un isomorfismo entre μ_K y μ_k. Así pues, dado $\overline{\lambda} \in \mu_k$ tenemos una raíz λ asociada en μ_K.

Una vez tenemos esta biyección, estamos en condiciones de definir el carácter de Brauer. Sea pues un kG–módulo L de dimensión n, y sea un elemento $g \in G_{reg}$. Denotamos por

g_L el endomorfismo de L asociado a g. Puesto que el orden de g es coprimo a p, g_L es diagonalizable. Sean $\{\overline{\lambda}_1, ...\overline{\lambda}_n\}$ sus autovalores, todos ellos en μ_k. Definimos entonces

$$\phi_L(g) = \sum_{i=1}^{n} \lambda_i \quad g \in G_{reg},$$

y lo llamamos carácter de Brauer asociado al kG–módulo L.

Para que la expresión compleja mencionada antes fuera posible, era necesaria la existencia de una correspondencia entre los grupos de raíces de la unidad. Por ello, los caracteres de Brauer, solo tienen sentido en elementos p–regulares.

A continuación vamos a probar varios resultados elementales sobre estos objetos.

Proposición 2.3. *Sea L un kG–módulo, entonces:*

i) $\phi_L(1) = n = dim(L)$.

ii) ϕ_L *es una función de clase sobre* G_{reg}.

iii) Si $0 \to L \to L' \to L'' \to 0$ *es una cadena exacta de kG–módulos, entonces:*

$$\phi_{L'} = \phi_L + \phi_{L''}.$$

iv) $\phi_{L\otimes L'} = \phi_L \phi_{L'}$.

v) Si $g \in G$ *tiene* p'*–componente* $s \in G_{reg}$*, la traza del endomorfismo* g_L *es la reducción de* $\phi_L(s)$.

vi) Sea V un KG–módulo con carácter χ*, sea M un retículo en V tal que* $KM = V$*, y sea* $L = \overline{M}$ *su reducción. Entonces* ϕ_L *es la restricción de* χ *a* G_{reg}.

Prueba. Solo probamos la (v) y la (vi).

Para probar (v), basta observar que si $g = ts$ con t la parte p–singular, t_L tiene como autovalores raíces p^n–ésimas de la unidad. Como estamos en un cuerpo de característica p, todos los autovalores son 1, y la propiedad se sigue de $Tr(g_L) = Tr(t_L s_L) = Tr(s_L) = \overline{\phi_L}(s)$.

Ahora estudiamos (vi). Hacemos un abuso de notación y denotamos por g_V a la matriz asociada al endomorfismo g_V en una $\mathcal{O}$–base para un $\mathcal{O}G$–retículo M en V tal que $KM = V$, en donde $g \in G_{reg}$. Sean sus autovalores $\{\zeta_1, \ldots, \zeta_n\}$, todos ellos en $\mathcal{O}$. Entonces, se tiene que

$$\chi(g) = \zeta_1 + \cdots + \zeta_n.$$

Queremos probar que $\{\overline{\zeta_1}, \ldots, \overline{\zeta_n}\}$ son los autovalores de $\overline{g_V}$.

La matriz g_V tiene coeficientes en $\mathcal{O}$, luego su polinomio característico está en $\mathcal{O}[x]$ y es de la forma

$$\prod_{i=1}^{n}(x - \zeta_i).$$

Reduciendo coeficientes, nos queda el polinomio característico de $\overline{g_V}$, que es

$$\prod_{i=1}^{n}(x-\overline{\zeta_i}),$$

(aquí hemos utilizado que los autovalores provienen de un elemento p-regular) luego los autovalores son $\{\overline{\zeta_1},\ldots,\overline{\zeta_n}\}$ tal y como queríamos. □

En la teoría clásica eran especialmente relevantes los caracteres irreducibles, en esta podemos considerar los caracteres de Brauer asociados a los kG–módulos simples. En torno a estos tenemos el siguiente teorema fundamental

Teorema 2.1 (Los caracteres de Brauer forma una K–base de funciones de clase sobre G_{reg})**.** *Sean F_i con $1 \leq i \leq r$ los kG–módulos irreducibles, y sean ϕ_{F_i} con $1 \leq i \leq r$ los caracteres de Brauer asociados. Entonces se tiene que ϕ_{F_i} es una K–base del espacio de funciones de clase sobre G_{reg} con valores en K.*

Prueba. Probamos primero la independencia lineal. Vamos a suponer que

$$\sum_{F_i} a_{F_i}\phi_{F_i} = 0$$

con $a_{F_i} \in K$ con al menos uno de ellos no nulo, y vamos a llegar a contradicción. Podemos suponer sin pérdida de generalidad que los coeficientes están en $\mathcal{O}$. Así pues, reducimos $mod(\mathfrak{p})$, y aplicamos (v) de la proposición anterior:

$$\sum_{F_i}\overline{a_{F_i}}\overline{\phi_{F_i}}(s) = \sum_{F_i}\overline{a_{F_i}}Tr(t_{F_i}) = 0,$$

en donde $s \in G_{reg}$, y $t \in G$. Puesto que se da esta igualdad para todo $t \in G$, se da para todo $t \in kG$. Ahora sea F_1 el irreducible tal que $\overline{a_1} \neq 0$. Sea $u \in End_k(F_1)$ con traza 1. Por el teorema de densidad existe algún $t \in kG$ tal que $t_{F_1} = u$, y $t_F = 0$ para $F \neq F_1$. Sustituyendo en la igualdad obtenida, se tiene que $\overline{a_{F_1}}1 = 0$, lo cual es imposible.

Ahora probamos que es conjunto generador. Sea f una función de clase sobre G_{reg}. la extendemos a G, de tal manera que es de la forma $\sum \lambda_i\chi_i$ con $\lambda_i \in K$ y χ_i caracteres ordinarios irreducibles. Si ahora tomamos la restricción a G_{reg}, por (iii) y (vi) de la proposición anterior, obtenemos una K–combinación lineal de caracteres de Brauer, tal y como buscábamos. □

Como corolarios se siguen dos resultados importantes:

Corolario 2.1 (Los caracteres de Brauer controlan factores de composición)**.** *Dados N, y M kG–módulos con el mismo carácter de Brauer, se tiene que $[N] = [M]$ en $G_0(kG)$.*

Prueba. Sean F_i con $1 \leq i \leq r$ los kG–módulos simples. Sea a_j el número de veces que aparece F_j en la serie de composición de N como factor de composición, y sea b_j el homónimo para M.

Utilizando el hecho de que los caracteres de Brauer son aditivos sobre sucesiones exactas, y la hipótesis de igualdad sobre los caracteres de Brauer de M y N , se sigue que

$$\phi_N = \sum_{i=1}^{r} a_i \phi_{F_i} = \sum_{i=1}^{r} b_i \phi_{F_i} = \phi_M$$

Utilizando que los caracteres irreducibles de Brauer forman una K–base, se sigue que $a_i = b_i$ para $1 \leq i \leq r$, por tanto M y N tienen la misma serie de composición, y en consecuencia, la misma clase en $G_0(kG)$. □

Corolario 2.2 (Teorema de Brauer)**.** *El número de clases de isomorfía de kG–módulos simples es igual al número de clases de conjugación de elementos p–regulares en G.*

Prueba. Solo hay que observar que la dimensión del K–espacio de funciones de clase sobre G_{reg} es exactamente el número de clases de conjugación p-regulares de G. □

El primer corolario nos dice que los caracteres de Brauer recogen la información de los factores de composición de los kG–módulos, tal y como lo hacían los caracteres ordinarios. En el caso de característica 0, los caracteres daban una descripción satisfactoria de la teoría de representaciones porque todos los KG–módulos eran semisimples. En el caso modular, los kG–módulos ya no tienen porqué serlo, y conocer los factores de composición de un módulo no lo caracteriza.

En cuanto al segundo corolario, Brauer prueba este teorema por primera vez en 1935 [Bra35]. Este teorema había sido probado en su versión análoga por Frobenius sobre característica 0, y encuentra un precursor en Dickson para el caso modular, quien lo prueba para grupos abelianos.

Es muy interesante la relación existente entre los caracteres y los grupos de Grothendieck. Para precisarla introducimos la siguiente definición

Definición 2.1 (Caracteres generalizados)**.** -

- Llamamos $Ch(KG)$ el conjunto de caracteres ordinarios generalizados formado por combinaciones $\mathbb{Z}$–lineales de caracteres ordinarios de KG–módulos.
- Llamamos $BCh(kG)$ el conjunto de caracteres de Brauer generalizados formado por combinaciones $\mathbb{Z}$–lineales de caracteres Brauer de kG–módulos.

Tenemos entonces que $Ch(KG)$ es un anillo isomorfo a $G_0(KG)$, y que $BCh(kG)$ es un anillo isomorfo a $G_0(kG)$, de tal manera que las teorías de caracteres de Frobenius, y Brauer respectivamente, quedan integradas en la formulación moderna a través de grupos de Grothendieck. Estos isomorfismos son el contenido de la siguiente proposición.

Proposición 2.4 (Isomorfismo entre anillos de caracteres y grupos de Grothendieck)**.** -

- $G_0(KG) \simeq Ch(KG)$
- $G_0(kG) \simeq BCh(kG)$

Prueba. Definimos para el primer isomorfismo la aplicación $\psi : G_0(KG) \to Ch(KG)$, definida por $[V] \mapsto \chi_V$. Como sabemos que $V \mapsto \chi_V$, es una función aditiva sobre cadenas exactas cortas en KG–*mod*, se sigue que ψ es un homomorfismo aditivo. Ahora observamos que $G_0(KG)$ es $\mathbb{Z}$–libre con base los KG–módulos irreducibles, y $Ch(KG)$ es también $\mathbb{Z}$–libre con base los caracteres ordinarios irreducibles, es claro que ψ es un isomorfismo. Finalmente nos damos cuenta que si U es otro KG–módulo, el carácter de $V \otimes_K U$ es $\chi_V \chi_U$, de donde se sigue que ψ es de hecho un isomorfismo de anillos.

En cuanto al segundo la prueba es totalmente análoga. □

Hecha esta identificación, podemos interpretar en términos carácter–teóricos el homomorfismo de descomposición.

Proposición 2.5. *Existe un diagrama conmutativo:*

$$\begin{tikzcd} G_0(KG) \arrow[r] \arrow[d, "d"'] & Ch(KG) \arrow[d, "d'"] \\ G_0(kG) \arrow[r] & BCh(kG) \end{tikzcd}$$

En donde d es el homomorfismo de descomposición, d' es la restricción a G_{reg}, y las flechas horizontales son los isomorfismos recién presentados.

Prueba Sabemos que para los KG–módulos simples el diagrama conmuta, como esto es una base, se sigue el resultado.□

2.3. El triángulo cde

En esta sección vamos a suponer que:

- G es un grupo finito.
- $(K, \mathcal{O}, k)$ es un sistema p–modular.
- $\mathcal{O}G$ es semiperfecto.
- K es lo suficientemente grande para G.
- $char(K) = 0$.

Vamos a construir un diagrama conmutativo en el que se objetivan los tránsitos de información entre ciertos grupos de Grothendieck asociados a los anillos que aparecen en el sistema

p–modular. Deduciremos algunas propiedades sobre este, y como aplicación obtendremos un par de resultados clásicos, a saber las relaciones de ortogonalidad para los caracteres de Brauer (cf. [RB37, RB]), y propiedades de la matriz de Cartan (cf. [RB37, RB, Bra41b])

La primera observación que hacemos es que existe un isomorfismo canónico entre $K_0(\mathcal{O}G)$ y $K_0(kG)$ inducido por la técnica de reducción.

Proposición 2.6. *la aplicación* $[M] \mapsto [\overline{M}]$ *define un isomorfismo de grupos abelianos* $K_0(\mathcal{O}G) \simeq K_0(kG)$.

<u>Prueba</u>. Partimos de la existencia de un isomorfismo de grupos abelianos dado por

$$\sum_{i=1}^{r} a_i[P_i] \mapsto \sum_{i=1}^{r} a_i[\overline{P}_i] \quad a_i \in \mathbb{Z}.$$

Hemos de comprobar que la aplicación lleva $[M]$ sobre $[\overline{M}]$ para todo $M \in \mathcal{P}(\mathcal{O}G)$. Sabemos por [CC81] p.420 (18.1) que

$$M \simeq P_1^{m_1} \oplus ... \oplus P_r^{m_r}.$$

Por tanto, utilizando la relación de $K_0(\mathcal{O}G)$, se tiene que

$$[M] = \sum_{i=1}^{r} m_i[P_i] \quad en \quad K_0(\mathcal{O}G),$$

Por otro lado,

$$\overline{M} \simeq \overline{P}_1^{m_1} \oplus ... \oplus \overline{P}_r^{m_r},$$

y por tanto,

$$[\overline{M}] = \sum_{i=1}^{r} m_i[\overline{P}_i] \quad en \quad K_0(kG),$$

Se sigue claramente el resultado. □

La siguiente observación, es que la aplicación $P \mapsto K \otimes_O P$ con $P \in \mathcal{P}(\mathcal{O}G)$ define un homomorfismo de grupos abelianos de $K_0(\mathcal{O}G)$ a $G_0(KG)$.

De esta forma podemos construir un homomorfismo $e : K_0(kG) \to G_0(KG)$ sin más que componer el inverso del isomorfismo canónico de la primera observación con este recién definido.

Ahora tomamos $U \in \mathcal{P}(kG)$, y denotamos por $c_i(U)$ la multiplicidad del kG–módulo simple F_i como factor de composición de U. Utilizando que la aplicación $[U] \mapsto [U]$ de kG–*mod* a $G_0(kG)$ es aditiva sobre sucesiones exactas cortas, se define el homomorfismo de Cartan $c : K_0(kG) \to G_0(kG)$ como

$$c[U] = [U] = \sum_{i=1}^{r} c_i(U)[F_i].$$

Definimos también la matriz de Cartan C como la traspuesta de la matriz asociada a c en las bases canónicas.

Ya tenemos todas las piezas del diagrama:

Proposición 2.7. *Existe un diagrama conmutativo*

$$\begin{tikzcd} & K_0(kG) \arrow[dl, "e"'] \arrow[dr, "c"] & \\ G_0(KG) \arrow[rr, "d"] & & G_0(kG) \end{tikzcd}$$

Prueba. Hemos de probar que $d(e[U]) = c[U]$ para cada $U \in \mathcal{P}(kG)$. Por [CC81] p.428 (18.1) se sigue que existe $P \in \mathcal{P}(\mathcal{O}G)$ tal que $\overline{P} = U$. Entonces por definición de e, se tiene que $e[U] = [K \otimes_{\mathcal{O}} P]$. Es claro que P es un $\mathcal{O}G$–retículo en $K \otimes_{\mathcal{O}} P$ tal que $KP = K \otimes_{\mathcal{O}} P$, luego por definición de d,

$$d(e[U]) = [\overline{P}] = [U].$$

Por otro lado, por definición del homomorfismo de Cartan, se sigue que $c[U] = [U]$. □

A continuación, vamos a aprovechar las identificaciones que tenemos entre los grupos de Grothendieck y los anillos de caracteres para construir formas bilineales. Así pues, llamemos $\{Z_1, \dots, Z_s\}$ a los KG-módulos simples, y $\{\zeta_1, \dots \zeta_s\}$ a sus caracteres asociados. Es conocido que tenemos el producto

$$(\zeta, \zeta') = |G|^{-1} \sum_{g \in G} \zeta(g)\zeta'(g^{-1})$$

para K–caracteres cualesquiera ζ y ζ'. Puesto que K es un cuerpo de descomposición, $\{\zeta_1, \dots \zeta_s\}$ es una base ortonormal de $Cf_K(G)$. Además

$$(\zeta, \zeta') = i(M, M') = dim_K Hom_{KG}(M, M'),$$

en donde M y M' son los módulos asociados a los caracteres ζ y ζ'. Usando que $G_0(KG) \simeq Ch(KG)$ podemos definir una forma $\mathbb{Z}$–bilineal $i_K : G_0(KG) \times G_0(KG) \to \mathbb{Z}$ como

$$i_K([M], [M']) = i(M, M') = (\zeta, \zeta')$$

en donde M y M' son KG–módulos con caracteres ζ y ζ'. La relación de ortogonalidad clásica nos da la siguiente relación

$$i_K(Z_i, Z_j) = \delta_{ij} \quad 1 \le i, j \le s.$$

Ahora construimos algo similar sobre k:

Proposición 2.8. *Existe una $\mathbb{Z}$-forma bilineal $i_k : K_0(kG) \times G_0(kG) \to \mathbb{Z}$ tal que*

$$i_k([U], [M]) = dim_k(Hom_{kG}(U, M)) \quad U \in \mathcal{P}(kG), M \in kG - mod$$

que verifica además

$$i_k([U_i], [F_j]) = \delta_{ij} \quad 1 \le i, j \le r$$

Prueba. Primero comprobamos que i_k está bien definida. Sea

$$0 \to M' \to M \to M'' \to 0$$

una sucesión exacta corta de kG–módulos, y tomemos un kG–módulo proyectivo U. Entonces la cadena

$$0 \to Hom_{kG}(U, M') \to Hom_{kG}(U, M) \to Hom_{kG}(U, M'') \to 0$$

es exacta. Por otro lado, seleccionando otra sucesión corta exacta esta vez en $\mathcal{P}(kG)$

$$0 \to U' \to U \to U'' \to 0$$

se sigue por proyectividad que U es suma directa interna de U' y U'' salvo isomorfismo. Por tanto, dado cualquier kG–módulo M se tiene que

$$Hom_{kG}(U, M) \simeq Hom_{kG}(U', M) \dotplus Hom_{kG}(U'', M).$$

A través de estas observaciones concluimos que i_k está bien definida.

Ahora probamos la segunda afirmación. dado U_i, este contiene un único submódulo maximal $rad(U_i)$, y se tiene que $U_i/rad(U_i) \simeq F_i$ para $1 \leq i \leq r$. Aplicando que k es un cuerpo de descomposición se sigue la igualdad esperada.□

Ahora probamos que d y e son adjuntos respecto de las formas bilineales recién definidas.

Teorema 2.2.

$$i_k(U, dZ) = i_K(eU, Z), \quad \textit{para todo } U \in K_0(kG), Z \in G_0(KG)$$

Prueba. Es suficiente probarlo para los generadores. Vamos a hacer una serie de observaciones. Sea $U \in \mathcal{P}(kG)$ y $Z \in kG\text{–}mod$, como $\mathcal{O}G$ es semiperfecto existe un $\mathcal{O}G$–módulo proyectivo P tal que $\overline{P} = U$. Entonces $e[U] = K \otimes_O P$. Por otro lado, sea L un $\mathcal{O}G$–retículo en Z tal que $KL = Z$. Entonces $d[Z] = [\overline{L}]$. Aplicando el teorema de cambio de anillos obtenemos el isomorfismo siguiente

$$K \otimes_O Hom_{\mathcal{O}G}(P, L) \simeq Hom_{KG}(K \otimes_O P, K \otimes_O L).$$

Tenemos también que $Hom_{\mathcal{O}G}(\mathcal{O}G, L) \simeq L$ como $\mathcal{O}G$–módulos, de donde deducimos

$$\overline{Hom_{\mathcal{O}G}(\mathcal{O}G, L)} \simeq \overline{L} \simeq Hom_{kG}(kG, \overline{L}),$$

ahora bien, como P es proyectivo, y Hom aditivo, se sigue que

$$\overline{Hom_{\mathcal{O}G}(P, L)} \simeq Hom_{kG}(\overline{P}, \overline{L}).$$

Utilizando estas observaciones desarrollamos

$$\begin{aligned} i_K(e[U],[Z]) &= dim_K(Hom_{KG}(K \otimes_O P, K \otimes_O L)) \\ &= dim_k(Hom_{kG}(\overline{P}, \overline{L})) \\ &= dim_k(Hom_{kG}(U, \overline{L})) = i_k([U], d[Z]) \end{aligned}$$

y obtenemos el resultado. □

De aquí podemos deducir uno de los resultados clásicos, a saber, que la matriz de Cartan es simétrica.

Corolario 2.3. *Sea C la matriz de Cartan, y sea D la matriz de descomposición de G para el sistema p–modular $(K, \mathcal{O}, k)$, entonces $C = D^t D$.*

Prueba. Sea E^t la matriz asociada al homomorfismo e con respecto a las bases canónicas, como consecuencia del teorema anterior $E = D^t$. Por otro lado la conmutatividad del diagrama se traduce en que

$$C = ED = D^t D$$

□

A continuación, vamos a probar que el homomorfismo de descomposición es sobreyectivo. Para ello vamos a construir una función que va a ser un carácter generalizado. Para probar que es un carácter generalizado tenemos que hacer uso de un teorema de Brauer (cf. [Bra53]). Damos una definición preliminar, enunciamos el teorema sin demostración, y luego lo aplicamos al caso que nos interesa.

Definición 2.2 (p–grupo elemental)**.** Un subgrupo H de G se dirá p–elemental si es producto directo de p–grupos, y un cíclico de orden coprimo a p.

Teorema 2.3 (Criterio de Brauer)**.** *Una función de clase $\phi \in Cf_K(G)$ pertenece a $Ch(KG)$ si y solo si la restricción de ϕ a cualquier p-grupo elemental $H \leq G$ está en $Ch(KH)$.*

Teorema 2.4 ("Brauer lift")**.** *Sea ϕ un carácter de Brauer asociado a un kG–módulo L. Extendemos ϕ a una función de clase $\hat{\phi}$ sobre G según*

$$\hat{\phi}(g) = \phi(s) \quad g \in G$$

donde s es la p'–parte de g. Entonces $\hat{\phi}$ es K–carácter generalizado de G.

Prueba. Es claro que $\hat{\phi}$ está en $Cf_K(G)$. Para probar que es un K-carácter generalizado, bastaría ver que la restricción $\hat{\phi}_H$ está en $Ch(KH)$, para H un p–grupo elemental cualquiera.

Sea entonces $H = A \times B$ un p–grupo elemental, con A de orden p' coprimo a p, y B el p–grupo. La idea va a ser construir un KH–módulo que tenga por carácter $\hat{\phi}$. Comenzamos tomando L_A, la restricción de L al grupo A. Como el orden de A es coprimo a p, se sabe que existe un KA–módulo V tal que su carácter coincide con el carácter de Brauer de L_A. Ahora vamos a tomar el producto tensor externo $V \otimes \mathbb{1}_B$, en donde $\mathbb{1}_B$ es el módulo trivial. Este un KH–módulo, con carácter $\hat{\phi}$. Por aplicación del criterio de Brauer se sigue el resultado. □

Corolario 2.4. *El homomorfismo de descomposición es sobreyectivo.*

Prueba. Basta recordar que podemos interpretar el homomorfismo de descomposición como la restricción de caracteres generalizados a G_{reg}. Por ello, dado un carácter de Brauer ϕ, hemos de comprobar si existe algún carácter generalizado, tal que al someterlo a la restricción nos de ϕ. Tal carácter es $\hat{\phi}$. □

Ahora utilizando un poco de álgebra lineal podemos deducir que e es inyectivo.

Corolario 2.5. *El homomorfismo e es inyectivo.*

Prueba. Tómese $[U] \in Ker(e)$. Utilizando que d y e son adjuntos, se sigue que $i_k([U], d[Z]) = 0$ para todo $[Z] \in G_0(KG)$. Como d es sobreyectivo, se tiene que $i_k([U], [V]) = 0$ para todo $[V] \in G_0(kG)$. Puesto que $K_0(kG)$ y $G_0(kG)$ admiten bases duales con respecto a la forma i_k, $[U] = 0$ y e es inyectivo. □

Consecuencia inmediata de esto es

Corolario 2.6. *Sean P, y P' $\mathcal{O}G$–módulos proyectivos tales que $K \otimes_{\mathcal{O}} P \simeq K \otimes_{\mathcal{O}} P'$, entonces $P \simeq P'$.*

A continuación fijamos notación:

- Z_i con $1 \leq i \leq s$ son los KG–módulos simples.
- ζ^i con $1 \leq i \leq s$ son los caracteres ordinarios irreducibles.
- F_j con $1 \leq j \leq r$ son los kG–módulos simples.
- ϕ^j con $1 \leq j \leq r$ son los caracteres de Brauer irreducibles.
- U_j con $1 \leq j \leq r$ son kG–módulos indescomponibles proyectivos.
- η^j con $1 \leq j \leq r$ son los caracteres de Brauer de $\{U_j\}$.
- P_j con $1 \leq j \leq r$ son $\mathcal{O}G$–módulos proyectivos indescomponibles tales que $\overline{P_j} = U_j$.
- $\mathcal{C}_j$ $1 \leq j \leq r$ son las clases de conjugación de G p–regulares.
- ζ^i_j es el valor de ζ^i en la clase $\mathcal{C}_j$.
- ϕ^i_j es el valor de ϕ^i en la clase $\mathcal{C}_j$.

- η^i_j es el valor de η^i en la clase $\mathcal{C}_j$.
- $C = (c_{ij})$ es la matriz de Cartan.
- $D = (d_{ij})$ es la matriz de descomposición.
- $\Phi = (\phi^i_j)_{r\times r}$
- $H = (\eta^i_j)_{r\times r}$
- $Z = (\zeta^i_j)_{s\times r}$

Observamos que es claro por lo visto hasta ahora que:

$$\eta^i|_{G_{reg}} = \sum_j d_{ij}\phi^j$$
$$\eta^i = \sum_j c_{ij}\phi^j$$

de donde deducimos que

$$Z = D\Phi, \quad H = C\Phi.$$

Ahora vamos a probar los resultados que buscábamos, es decir, las relaciones de ortogonalidad para caracteres modulares, y algunas propiedades de la matriz de Cartan, en concreto vamos a probar tiene determinante una potencia de p.

Comenzamos por probar el siguiente lema:

Lema 2.1. -

(i) Φ *es unimodular sobre* $\mathcal{O}$.

(ii) $det(C) \neq 0$.

Prueba. Como k es un cuerpo de descomposición para G, se tiene que los k–caracteres de $\{F_j\}$ son linealmente independientes sobre k. Estos caracteres están determinados por las filas de la matriz $\overline{\Phi}$, luego $det(\overline{\Phi}) \neq 0$. Como $\mathcal{O}$ es un anillo local con cuerpo de residuos k, $det(\Phi) \neq 0$, y por tanto es una unidad en $\mathcal{O}$ lo que prueba (i).

Para probar (ii) observamos que la segunda relación de ortogonalidad nos da que $det(Z^tZ) \neq 0$. Por otro lado, tenemos que

$$Z^tZ = \Phi^tD^tD\Phi = \Phi^tC\Phi.$$

Como Φ es unimodular, necesariamente $det(C) \neq 0$ probando (ii). □

Estamos en condiciones de probar las relaciones de ortogonalidad.

Teorema 2.5 (Relaciones de Ortogonalidad). *Sea $h_j = |\mathcal{C}_j|$, y $X^i_{j^*}(x) = X^i(x^{-1})$ para $x \in \mathcal{C}_j$. Entonces:*

(i) $\sum_{j=1}^r h_j \phi^i_j \eta^k_{j^*} = |G|\delta_{ik}$.

(ii) $\sum_{j=1}^r h_j \phi^i_j \phi_{j^*} = |G|\gamma_{ik}$ *donde* $C^{-1} = (\gamma_{ij})$.

(iii) $\sum_{j=1}^r h_j \eta^k_j \eta^k_{j^*} = |G|c_{ik}$.

Prueba. Denotemos $Y = (|G|h_i^{-1}\delta_{ij^*})$, entonces tenemos

- $Z^t Z = Y$ de donde $\Phi Y^{-1}\Phi = C^{-1}$, y se sigue (ii).
- $Z = D\Phi$ de donde $\Phi Y^{-1} H^t = I$ y se sigue (i).
- $H = C\Phi = D^t Z$ de donde $HY^{-1}H^t = C$ y se sigue (iii).

□

Probamos ahora otro lema antes de demostrar que $det(C)$ es una potencia de p.

Lema 2.2. *Sea $|G| = p^a m$ con $(p, m) = 1$. Sea ϕ el carácter de Brauer de un kG–módulo L. Entonces*

$$\theta(x) = \begin{cases} p^a\phi(x) & si \quad x \in G_{reg} \\ 0 & si \quad en\ otro\ caso \end{cases}$$

es un carácter generalizado.

Prueba. De nuevo hacemos uso del criterio de Brauer. Hemos de comprobar que $\theta|_H$ está en $Ch(KH)$ para H p–elemental.

Ponemos $H = A \times B$, de tal manera que A es un grupo de orden coprimo a p, y B es un p–grupo de orden p^t con $t \leq a$. Sea también ρ_B el carácter regular de B. Con estos elementos definimos la función ψ K-valuada sobre H:

$$\psi(a, b) = \phi(a)\rho_B(b).$$

Sabemos por el razonamiento en el lema del "Brauer lift" que ϕ_A es un K–carácter de A, por tanto ψ es un K–carácter de H. Ahora observamos que

- Para $x \in H_{reg}$, se tiene que $x \in A$, y $\psi(x) = |B|\phi(x) = p^t\phi(x) = p^{t-a}\theta(x)$, luego $\theta(x) = p^{a-t}\psi(x)$.
- Para $x \notin H_{reg}$ se tiene que $\psi(x) = 0$, luego $\theta(x) = p^{a-t}\psi(x)$ trivialmente.

Hemos visto que $\theta|_H \in Ch(KH)$, por tanto θ es un carácter generalizado. □

Demostramos que $det(C)$ es potencia de p.

Teorema 2.6. *$det(C) = p^l$ para l no negativo.*

Prueba. Sea $|G| = p^a m$ con $(p, m) = 1$. Sea θ_i el carácter generalizado recién definido asociado a ϕ^i para $1 \leq i \leq r$. Entonces $\theta_i = \sum_{j=1}^r a_{ij}\zeta^i$, para $a_{ij} \in \mathbb{Z}$ con $1 \leq i \leq r$. Tenemos entonces:

$$\begin{aligned}
a_{ij} &= \langle \theta_i, \zeta^j \rangle \\
&= |G|^{-1} \sum_{g \in G} \theta_i(g^{-1})\zeta^j(g) \\
&= p^a |G|^{-1} \sum_{g \in G_{reg}} \phi^i(g^{-1})\zeta^j(g) \\
&= p^a |G^{-1} \sum_{g \in G_{reg}} \phi^i(g^{-1}) \sum_{k=1}^r d_{jk}\phi^k(g) \\
&= p^a \sum_{k=1}^r d_{jk}\{|G|^{-1} \sum_{g \in G_{reg}} \phi^i(g^{-1})\phi^k(g)\} \\
&= p^a \sum_{k=1}^r d_{jk}\gamma_{ki}.
\end{aligned}$$

En donde $C^{-1} = (\gamma_{ij})$. Ahora, utilizando la simetría de C, y que la matriz $A = (a_{ij})$ verifica

$$A = p^a C^{-1} D^t$$

se tiene que

$$AA^t = p^{2a} C^{-1} D^t D (C^{-1})^t = p^{2a} C^{-1}$$

por lo que

$$(det(C))(det(AA^t)) = p^l$$

Para l un entero no negativo. □

2.4. Ejemplo: S_4 en $p = 2$

A modo de ejemplo, vamos a analizar la teoría de representaciones del grupo S_4 sobre el primo $p = 2$ (cf. [Ser77]). Comenzamos por recordar la tabla de caracteres de S_4:

Sabemos que hay dos clases 2-regulares: la de 1, y la de (abc). Por tanto, por el teorema de Brauer sabemos que hay dos representaciones irreducibles. La única de grado 1 es la trivial con carácter $\phi_1 = 1$. Por su parte, la representación irreducible de grado 2 de S_4 tras reducir *mod* 2 nos da la representación ρ_2 cuyo carácter ϕ_2 toma el valor -1 para el elemento (abc).

	1	(ab)	$(ab)(cd)$	(abc)	$(abcd)$
χ_1	1	1	1	1	1
χ_2	1	-1	1	1	-1
χ_3	2	0	2	-1	0
χ_4	3	1	-1	0	-1
χ_5	3	-1	-1	0	1

Figura 2.1.: Tabla de [Ser77]

En consecuencia, no es suma de la trivial, pues de ser así tendríamos $\phi_2 = 2\phi_1 = 2$, por tanto es irreducible. Nos queda entonces la siguiente tabla de caracteres:

	1	(abc)
ϕ_1	1	1
ϕ_2	2	-1

Figura 2.2.: Tabla de [Ser77]

Ahora calculamos la matriz de descomposición expresando las restricciones a G_{reg} de $\chi_1, \ldots, \chi_5$ en función de ϕ_1 y ϕ_2:

$$\begin{aligned}
\chi_1 &= \phi_1. \\
\chi_2 &= \phi_1. \\
\chi_3 &= \phi_2. \\
\chi_4 &= \phi_1 + \phi_2. \\
\chi_5 &= \phi_1 + \phi_2.
\end{aligned}$$

luego la matriz de descomposición es

$$D = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

Ahora calculamos los caracteres Φ_1 y Φ_2, de los indescomponibles proyectivos a través de la traspuesta de D:

$$\begin{aligned}
\Phi_1 &= \chi_1 + \chi_2 + \chi_4 + \chi_5. \\
\Phi_2 &= \chi_3 + \chi_4 + \chi_5.
\end{aligned}$$

La matriz de Cartan la calculamos a través de la relación DD^t:

$$C = \begin{pmatrix} 4 & 2 \\ 2 & 3 \end{pmatrix},$$

observamos que tiene determinante $8 = 2^3$. Finalmente, descomponemos los caracteres de los proyectivos indescomponibles sobre G_{reg} utilizando la matriz de Cartan:

$$\Phi_1 = 4\phi_1 + 2\phi_2.$$
$$\Phi_2 = 2\phi_1 + 3\phi_2.$$

3. Teoría de representación local: los bloques

3.1. Introducción

La segunda etapa del trabajo de Brauer en torno a la teoría de representación modular se configura sobre la idea de una teoría de representación local. El objetivo ahora es explicar fenómenos globales a través de la estructura p–local de los objetos estudiados.

En la página 17 de [RB37] se introduce por primera vez el concepto de bloque. La función del bloque es coordinar la teoría de representación ordinaria y la teoría de representación modular recién elaborada. Brauer dice a modo de motivación antes de introducir el concepto: " We discuss the representation of Γ [esto es nuestro álgebra de grupo kG] now from the point of view of the theory of representations " en donde con "Theory of representations" claramente se refiere a lo desarrollado en el artículo. Para exponer el concepto original seguimos [RB], ya que en él la exposición es más clara.

Así pues, sea un grupo finito G, y un sistema p–modular $(K, \mathcal{O}, k)$ en donde K es de característica 0, y es lo suficientemente grande para G. Esto es para situarnos en lenguaje moderno en el contexto original del artículo, en el que uno tiene disponible la teoría de representación ordinaria de Frobenius. Vamos a considerar las álgebras KG, y kG respectivamente y sus respectivos centros $Z(KG)$, y $Z(kG)$. Si ahora se seleccionan representaciones irreducibles V, y F, sobre K, y k respectivamente se tiene que:

$$V(Z(KG)) = \omega I, \quad F(Z(kG)) = \phi I.$$

En donde, ω es un entero de K, ϕ un elemento de k e I es la matriz identidad. Se dice que dos representaciones irreducibles sobre k están en el mismo bloque si $\phi_1 = \phi_2$, donde estos valores vienen a representar al centro del álgebra kG. Tómese ahora un kG–módulo indescomponible proyectivo U, entonces diremos que este está en el bloque B, si su irreducible asociado está en B. Dados dos indescomponibles proyectivos U_τ, y U_λ, estarán en el mismo bloque si existe una cadena

$$U_\tau, U_1, \ldots, U_n, U_\lambda,$$

tal que dos módulos consecutivos comparten algún factor de composición. Finalmente, dada una representación ordinaria irreducible V, si suponemos que esta tiene al reducirla como factor de composición al kG–módulo F, entonces con la notación anterior, se tiene que $\overline{\omega} = \phi$, y decimos también que V está en el bloque de F.

Hemos organizado en la noción de bloque: representaciones ordinarias irreducibles, representaciones modulares irreducibles, y los indescomponibles proyectivos.

Una vez introducido el concepto se prueban algunas nociones básicas, como que tanto la matriz de descomposición, como la matriz de Cartan adquieren forma de matriz por bloques cuando se construyen considerando la organización de la información que dan los bloques.

En [RB], se define el tipo de un bloque. Así pues, un bloque B será de tipo α cuando toda representación irreducible ordinaria V_i en B tenga grado v_i verificando $v_i \equiv 0 \quad mod(p^\alpha)$, y al menos una de ellas cumple $v_i \not\equiv 0 \quad mod(p^{\alpha+1})$. En torno al tipo prueba varios resultados, como el teorema 1, sobre bloques del "más alto tipo"; o el teorema 2, sobre bloques del "más bajo tipo", ambos enunciados en la página 565 de [RB]:

Teorema 3.1 (Sobre bloques del más alto tipo)**.** *Sea G un grupo finito de orden $g = p^a g'$, donde p es un primo, $(g', p) = 1$. Una representación irreducible V de orden $v \equiv 0 \quad mod(p^a)$ permanece irreducible como representación modular (esto es al reducirla), y es su propio proyectivo indescomponible asociado. Además V constituye en sí mismo su bloque asociado. El carácter ζ de V se anula en todos los elementos de orden divisible por p.*

Teorema 3.2 (Sobre bloques del más bajo tipo)**.** *Sea t el número de clases de conjugación C de G tal que:*

- *El número de elementos en C es coprimo respecto de p.*
- *Los elementos de C tienen orden coprimo respecto de p.*

Entonces existen exactamente t bloques conteniendo al menos una representación ordinaria irreducible con orden coprimo con respecto a p.

En [Bra39] Brauer enuncia una serie de aplicaciones de los resultados expuestos en [RB]. Entre ellos destaco el teorema II:

Teorema 3.3 (Aplicación de [RB])**.** *Sea G un grupo simple de orden $g = pqr^m$ donde p, q, y r son primos distintos. Entonces $g = 60$ o $g = 168$.*

En 1944 se publica [Bra44], en él Brauer introduce un refinamiento del concepto de tipo. Este concepto es el de defecto de un bloque. Sea G un grupo de orden $g = g'p^a$, y sea B un bloque de tipo α. Entonces decimos que B tiene defecto $d = a - \alpha$. De esta forma el defecto se configura como una relativización del tipo, que nos permite estudiar bloques en abstracto, sin necesidad de tener en cuenta el orden del grupo a estudiar. Con este lenguaje, por ejemplo, los bloques de tipo más alto de [RB] son bloques de defecto 0, y el teorema antes expuesto describe la estructura de estos bloques. Brauer en 1941 publica [Bra41a], en relación a este artículo dice W. Feit en el obituario:"In my opinion [it] is one of the most remarkable and original papers that he ever wrote ". (cf. p8 [Fei79]). En este artículo, Brauer da información muy precisa sobre la estructura de los bloques de defecto 1. Es en este trabajo en el que incluye la definición de lo que hoy se conoce como árbol de Brauer. La idea es que dado un bloque B de defecto 1 a este se le asigna un grafo lineal donde cada vértice es una familia de caracteres ordinarios irreducibles p-conjugados, y cada arista es un carácter de Brauer irreducible asociado al bloque. Dos vértices estarán conectados en esencia si contienen un factor de composición común. Una vez hecha esta construcción se deducen propiedades al respecto de este grafo, un ejemplo de esto es el teorema 14 (cf p958 [Bra41a]):

Teorema 3.4. *Si todos los caracteres modulares de un bloque B de tipo $a-1$ son reales, entonces su árbol asociado es un polígono abierto.*

Estos resultados los aplicará en [Bra42a], y [Bra42b]. Concretamente prueba el siguiente teorema en el segundo artículo:

Teorema 3.5 (Aplicación de [Bra41a])**.** *Sea G un grupo finito de transformaciones lineales en n variables. Supongamos que el orden g de G contiene como factor primo p a la primera potencia, y que G no contiene subgrupo normal de orden p. Entonces $p \leq 2n+1$. La igualdad se da cuando G, considerado como ´´collineation group" sea isomorfo a $LF(2,p)$ (Linear fractional group).*

Volviendo ahora al artículo de 1944 [Bra44], es en este en el que se observa el inicio de una visión local. Brauer describe el objetivo del artículo así: "The main object of this paper is to give a direct characterization of the blocks. For instance, we shall show that the number of blocks of given positive defect d is completely determined by the structure of certain subgroups N of G which are the normalizers N of the subgroups H of order p^d" (cf. p110 [Bra44]). Así pues, este texto pretende dar una información de naturaleza global, como puede ser el número de bloques de defecto d, a través de información proveniente de la estructura p–local del grupo, es decir los normalizadores de los p–subgrupos de orden p^d.

El artículo [Bra44] es el primero de una serie seguida por [Bra46a, Bra46b]. En el primero define el defecto como cantidad aritmética, en el segundo se produce una evolución de este concepto, en concreto define un grupo de defecto asociado al bloque. Este es un p–subgrupo de orden p^d, con d el defecto como cantidad aritmética, que está bien definido salvo conjugación. El grupo de defecto es una estructura algebraica que mide la complejidad del bloque al que está asociado. Sobre esta noción Brauer enuncia el primer y segundo gran teorema ambos en la línea de una teoría local. Ambos dan conexiones profundas entre los bloques de un grupo y los bloques de ciertos p–subgrupos. Sin embargo, estos teoremas no serían probados hasta [Bra56, Bra59].

Es interesante observar las grandes distancias entre la fecha de publicación de los enunciados de los grandes teoremas, y sus demostraciones. Esto se debe a que en parte Brauer pensaba que su trabajo en teoría de representación modular no le interesaba a nadie. Dice Feit al respecto en [Fei79]: "The ten year delay in the publication of the proofs of the First and Second Main Theorems of block theory was only partly due to the fact that Brauer was working on other things. It was also partly due to the fact that he felt that no one was interested in his work on modular representations. This was not really the case". Finalmente Brauer introduce lo que se llamará "Brauer pair" en el artículo [Bra71b]. Utilizando este concepto prueba el tercer gran teorema que trata sobre el bloque principal, que es el que contiene el módulo trivial. En el cuerpo del capítulo se probarán los tres grandes teoremas.

Cabe destacar que, a pesar de que prácticamente toda la teoría de representación modular provenga íntegramente del trabajo de Brauer, hubo ciertos matemáticos trabajando en paralelo en la materia, incluso publicando demostraciones de los resultados de Brauer antes que el propio Brauer. Entre estos matemáticos Brauer menciona en [Bra71a] a Osima, Rosenberg, Iizuka, Nagao, Curtis y Reiner.

En paralelo a Brauer, en los años 60, Green inicia una aproximación alternativa a la teoría de representación modular. Esta tiene un sabor módulo-teórico frente al gusto de Brauer por los métodos carácter-teóricos.

La primera de las publicaciones de Green en torno a la teoría de representación modular es [Gre59], este artículo parte del trabajo de Higman [Hig54].

Dado G un grupo y $H < G$, podemos transferir estructura entre módulos para G, y módulos para H. A saber, si M es un kG–módulo, se puede ver como un kH–módulo M_H sin más que olvidar parte de la estructura original. Por su parte, dado un kH–módulo L, se puede obtener un kG–módulo L^G a través del producto tensor $kG \otimes_{kH} L$. La primera técnica se llama restricción, y la segunda inducción.

Ahora dado M un kG–módulo decimos que este es H–proyectivo para $H < G$, si existe un kH–módulo L, tal que M es isomorfo a un sumando directo de L^G.

Introducida esta notación podemos entender el criterio de Higman:

Teorema 3.6 (Criterio de Higman). *Sea M un kG–módulo, entonces es H–proyectivo si y solo si alguna de las siguientes:*

(i) M es componente de M_H^G.

(ii) M tiene un kH-endomorfismo η tal que $\sum_{x \in G} x^{-1} \eta x$ es la identidad en M.

Como consecuencia, obtiene el resultado

Corolario 3.1. *Sea P un p–subgrupo de Sylow de G, entonces todo kG–módulo es P–proyectivo.*

Introducimos algo más de notación para presentar el trabajo de Green. Sea M un kG–módulo, y sea $\mathcal{V}(M)$ el conjunto de subgrupos H de G tal que M es H–proyectivo. Observamos que $\mathcal{V}(M)$ es no vacío, pues G es un grupo en ese conjunto. Ahora como es finito este ha de admitir un elemento minimal. El teorema 4 de [Gre59] nos dice que :

Teorema 3.7 (Introducción del vértice). *Si M es indescomponible, entonces existe V subgrupo de G tal que:*

(i) M es V–proyectivo.

(ii) Si M es H–proyectivo para H un subgrupo de G, entonces hay algún conjugado de V que es subgrupo de H.

V está definido de manera única salvo conjugación y se denomina vértice de M.

Para este teorema es de vital importancia controlar el módulo $(M^G)_D$ para M un kH–módulo, y H, D subgrupos apropiados de G. La descripción de este módulo la da el Teorema de Mackey. A modo de curiosidad Green probó el teorema sin saber de la existencia del trabajo de Mackey.

Asociada con la noción de vértice está la de fuente. Esto es si M es un kG–módulo indescomponible con vértice V, se dirá fuente de M a cualquier kV–módulo S indescomponible.

Por último, en este mismo artículo Green investiga los vértices de un bloque fijo dado. (Esto tiene sentido porque los bloques también pueden entenderse como álgebras indescomponibles que ocurren en la descomposición de kG cf. [Alp86]). utilizando la definición original de defecto de Brauer [Bra46a], Green prueba:

Teorema 3.8. *El vértice de un módulo indescomponible de un bloque B es un subgrupo del defecto D del bloque. Además hay un módulo sobre B que tiene por vértice D.*

Para el momento en el que se publica [Gre62], el entendimiento que había sobre el grupo de defecto había mejorado bastante. Destacan los trabajos de Osima ([Osi55]), y Rosenberg ([Ros61]), ambos con una perspectiva más anillo-teórica. Concretamente Rosenberg extiende la noción de grupo de defecto a los idempotentes primitivos centrales del álgebra kG. Un idempotente como el descrito genera un bloque. Esta puede interpretarse como un sumando directo indescomponible del álgebra kG, vista como un módulo para $G \times G$. Green prueba en [Gre62], que el vértice de este módulo es $\{(g, g) : g \in D\}$, para D el defecto del bloque.

Sin duda, la aportación más importante de Green a la teoría es su correspondencia. Esta es una herramienta que describe el comportamiento de los módulos frente a la inducción y a la restricción. En [Gre72] prueba que la correspondencia nos da una equivalencia entre ciertas categorías apropiadamente definidas. (En esencia nos da una equivalencia estable entre categorías de módulos para G y ciertos subgrupos de G).

Lo que quiero destacar con esta historia es que con [Bra44], Brauer inicia una visión local de la teoría de representación modular, la cual cristaliza en sus tres grandes teoremas, y que luego será continuada en el trabajo de Green.

3.2. Los tres grandes teoremas

En esta parte seguimos de cerca la exposición de Alperin [Alp86]. Esta es puramente módulo-teórica. Nuestro objetivo será probar los tres grandes teoremas de Brauer utilizando la teoría que desarrolla Green. Concretamente definiremos vértices y fuentes para kG–módulos indescomponibles, y a continuación la correspondencia de Green. Con estas herramientas afrontamos el estudio de los bloques desde un punto de vista módulo-teórico. Definiremos el defecto de un bloque y probaremos el primer, segundo, y tercer gran teorema de Brauer. También analizaremos la teoría de representación modular de los grupos cíclicos y de $SL(2, p)$ a modo de aplicación de la teoría desarrollada.

3.2.1. La inducción

En lo que sigue sea G un grupo finito, p un primo fijo, y sea k un cuerpo de característica p algebraicamente cerrado.

Lo primero que vamos a hacer es desarrollar herramientas que nos permitan relacionar kG–módulos con kH–módulos para $H \leq G$.

A modo de motivación, la teoría de espacios vectoriales está en algún sentido muy controlada debido a la existencia de bases. ¿Qué es una base? Una base es un subconjunto de un espacio vectorial tal que toda aplicación de conjuntos sobre otro espacio vectorial, se levanta a una aplicación lineal. En general este es esencialmente el concepto matemático de libre. A saber, podemos definir kG–módulo libre como aquel tal que existe un subconjunto de tal forma que toda aplicación de conjuntos sobre cualquier otro kG–módulo se levante a un kG–homomorfismo. Vamos a construir una noción de libre que extienda a esta apropiada para el objetivo que perseguimos.

Definición 3.1 (kG–módulo H–libre)**.** Decimos que un kG–módulo U es H–libre , donde H es un subgrupo de G, si existe un kH–submódulo X de U tal que cualquier kH–homomorfismo de X a cualquier kG–módulo V se levanta a un único kG–homomorfismo de U a V. Llamamos a X una base de U.

Conviene observar, que este concepto efectivamente extiende al usual. Si uno toma como subgrupo H el trivial, es claro que ser 1–libre es ser libre.

Probamos ahora que dados dos kG–módulos H–libres, si sus bases son isomorfas entonces los kG–módulos también.

Lema 3.1. *Sean U y V kG–módulos H–libres con respecto a X e Y respectivamente, tal que $X \simeq Y$. Entonces U y V son isomorfos.*

Prueba. Hemos de construir un kG–isomorfismo de U a V. La idea es levantar el que se tiene por hipótesis de X a Y a uno de U a V. Sea f el isomorfismo de X a Y, y sea g su inverso. Tomamos el kH–homomorfismo $i_V f : X \to V$, donde i_V es la inclusión, y lo levantamos a $\bar{f}$. Haciendo lo mismo para g obtenemos $\bar{g}$. Se tiene entonces que $i_U = \bar{g}\bar{f}i_U$. Puesto que el levantamiento es único, y se tiene que $i_U = id_u i_U$, se sigue que $\bar{g}\bar{f} = id_U$. Por tanto $\bar{f}$ nos da un isomorfismo de U a V. □

Nos preguntamos si existen kG–módulos H–libres para H un subgrupo no trivial, la siguiente proposición nos responde afirmativamente.

Proposición 3.1. *Sea X un kH–módulo con H un subgrupo de G, entonces existe un kG–módulo H–libre.*

Prueba. Vamos a construir un kG–módulo a partir de X y luego probamos que es H–libre. Sea S un conjunto de representantes de coclases a la izquierda de H en G, tal que $1 \in S$. Tomamos para $s \in S$ el conjunto $\{s\} \times X$, y lo dotamos de estructura de espacio vectorial aprovechando la estructura de X. Ahora tomamos la suma directa externa de estos espacios, de tal forma que los elementos de esa suma sean de la forma $\sum_{s \in S}(s, x_s)$.

Ahora dotamos a este espacio de estructura de kG–módulo:

$$g(s, x) = (t, hx), \quad gs = th,$$

en donde $g \in G$, $s \in S$, $x \in X$. Comprobamos que efectivamente es un kG–módulo. si $g't = uh'$

$$
\begin{aligned}
g'(g(s,x)) &= g'(t,hx) \\
&= (u,h'hx) \\
&= (g'g)(s,x).
\end{aligned}
$$

Veamos que es H–libre. Sea $\phi : \{1\} \times X \to V$ un kH-homomorfismo a un kG–módulo V. Definimos una transformación lineal Φ tal que $\Phi(s,x) = s\phi(x)$. Esta extiende a ϕ y además es un kG–homomorfismo:

$$
\begin{aligned}
\Phi(g(s,x)) &= \Phi((t,hx)) \\
&= t\phi(hv) \\
&= th\phi(x) \\
&= g(s\phi(x)) \\
&= g\Phi(s,x).
\end{aligned}
$$

Además, si Ψ es otro levantamiento de ϕ,

$$\Psi(s,x) = \Psi(s(1,x)) = s\Psi(1,x) = s\phi(x) = \Phi(s,x)$$

□

A continuación damos un criterio útil para determinar si un kG–módulo generado a partir de un kH–módulo es H–libre.

Proposición 3.2. *Si U es un kG–módulo generado por un kH–módulo X, entonces U es H–libre si y solo si,*

$$dim(U) = |G : H| dim(X)$$

Prueba. Si U es H–libre con respecto de X, entonces es isomorfo al módulo recién construido que es una suma de $|G : H|$ espacios vectoriales cada uno con dimensión $dim(X)$.

Sea ahora U un kG–módulo generado por X tal que $dim(U) = |G : H|dim(X)$, queremos ver que es H–libre. Sea entonces U' H–libre respecto al kH–módulo $X' \simeq X$, entonces, por la hipótesis, $dim(U) = dim(U')$. Hemos de ver que el kG–homomorfismo que extiende a $X \simeq X'$ es un isomorfismo. Ahora, la extensión tiene por imagen en U un kG–módulo que contiene a X, por tanto debe de ser todo U. Por tanto, tenemos una aplicación sobreyectiva entre espacios de la misma dimensión que además es un kG–homomorfismo, es decir, un isomorfismo.□

Estos módulos H–libres se suelen trabajar a través de una expresión como producto tensor. Sea V un kH–módulo, con $H \leq G$. Formamos el producto tensor de espacios vectoriales $kG \otimes V$. Denotamos ahora por $kG \otimes_{kH} V$ al cociente generado por los elementos de la forma $ah \otimes v - a \otimes hv$, en donde $a \in kG$, $h \in H$, y $v \in V$. Dotamos ahora a este espacio de estructura de kG–módulo a través de la acción $g(a \otimes v) = ga \otimes v$, en donde $g \in G$, $a \in kG$ y $v \in V$. A este kG–módulo lo llamamos inducido por el kH–módulo V, y lo denotamos por V^G.

Lo primero que hemos de probar, es que esta construcción nos da módulos H–libres.

Lema 3.2. *El módulo inducido V^G es H–libre con respecto V. Además, V^G es la suma directa de espacios vectoriales $V^G = \sum_{s\in G/H} s \otimes V$.*

Prueba. Vamos a tomar U un kG–módulo H–libre respecto de V. Por los resultados establecidos, se tiene que $U = \sum_{s\in G/H} sV$. Definimos una aplicación lineal $\phi : kG \otimes V \to U$ tal que $\phi(g \otimes v) = gv$. La bilinealidad nos garantiza la existencia de tal función. Es fácil ver que la imagen de ϕ es todo U. Además,

$$\phi(gh \otimes v - g \otimes hv) = ghv - ghv = 0$$

luego ϕ induce una aplicación lineal Φ de V^G sobre U. Además, esta es un kG–homomorfismo, a saber

$$\begin{aligned} \Phi(g'(g \otimes v)) &= \Phi(g'g \otimes v) \\ &= g'gv \\ &= g'\Phi(g \otimes v) \end{aligned}$$

Ahora como en V^G, $gh \otimes v = g \otimes hv$, y $hv \in V$, $V^G = \sum_{s\in G/H} s \otimes V$,
y $dim(V^G) \leq |G : H| dim(V) = dim(U)$, de donde se sigue que $U \simeq V^G$. □

Ahora probamos una serie de propiedades útiles sobre la inducción:

Proposición 3.3 (Lema Ómnibus). *Sean V, V_1, y V_2 kH–módulos donde H es un subgrupo de G, y sea U un kG–módulo.*

(i) *Si V es libre (proyectivo) entonces V^G es libre (proyectivo).*

(ii) $(V_1 \oplus V_2)^G \simeq V_1^G \oplus V_2^G$

(iii) $(V*)^G \simeq (V^G)*$

(iv) *Si W es un kL–módulo para $L \leq H$, entonces $(W^H)^G \simeq W^G$*

(v) $U \otimes V^G \simeq (U_H \otimes V)^G$

(vi) $Hom_{kG}(V^G, U) \simeq Hom_{kH}(V, U_H)$

(vii) $Hom_{kG}(U, V^G) \simeq Hom_{kH}(U_H, V)$

(viii) *Si $\gamma \in Hom_{kH}(U_H, V)$, la aplicación $u \mapsto \sum_{s\in G/H} s \otimes \gamma(s^{-1}u)$ está en $Hom_{kH}(U_H, V^G)$, y nos da un isomorfismo $Hom_{kH}(U_H, V) \to Hom_{kG}(U, V^G)$*

(ix) *Si $\alpha \in Hom_{kH}(V_1, V_2)$ entonces existe un único $\alpha^G \in Hom_{kG}(V_1^G, V_2^G)$ que extiende a α.*

(x) *Si la cadena*

$$0 \longrightarrow V_1 \xrightarrow{\alpha} V \xrightarrow{\beta} V_2 \longrightarrow 0$$

es exacta, entonces la cadena

$$0 \longrightarrow V_1^G \xrightarrow{\alpha^G} V^G \xrightarrow{\beta^G} V_2^G \longrightarrow 0$$

también es exacta. Además, la primera escinde si y solo si la segunda lo hace.

Prueba. Probamos (ii). Queremos ver que $(V_1 \oplus V_2)^G \simeq V_1^G \oplus V_2^G$. Para ello observamos que $V_1^G \oplus V_2^G$ está generado por $V_1 \oplus V_2$, que es un kH–submódulo, y además se tiene que

$$\begin{aligned} dim(V_1^G \oplus V_2^G) &= dim(V_1^G) + dim(V_2^G) \\ &= dim(V_1)|G:H| + dim(V_2)|G:H| \\ &= |G:H|(dim(V_1) + dim(V_2) \\ &= |G:H|dim(V_1 \oplus V_2) \end{aligned}$$

lo que lo hace H–libre respecto de $V_1 \oplus V_2$. En consecuencia se sigue el isomorfismo.

Probamos (iv). Observamos que:

$$\begin{aligned} dim((W^H)^G) &= |G:H|dim(W^H) \\ &= |G:H||H:L|dim(W) \\ &= |G:L|dim(W) \end{aligned}$$

Hemos de probar entonces que $(W^H)^G$ está generado por un kL–modulo isomorfo a W. Ahora bien, como $1 \otimes W \simeq W$ genera $(W^H)^G$ como kG–módulo se sigue el resultado.

Ahora probamos (i). Como tenemos (ii), solo tenemos que probarlo para libres. Sea entonces V un kH–módulo libre, esto es un kH–módulo 1-libre, entonces $V \simeq X^H$ donde X es un k–módulos. Por tanto $V^G \simeq (X^H)^G \simeq X^G$ que es un kG–módulo libre.

Probamos (iii). Sea U H–libre respecto de V, hemos de ver que U^* es H–libre respecto de V^*. A saber, como $U \simeq V^G$, $(V^G)^* \simeq U^* \simeq (V^*)^G$. Sea U la suma directa $\sum sV$, y sea $\hat{V}$ el conjunto de funcionales lineales de U que se anulan en sV para $s \notin H$. Esto es un kH–submódulo de U^* y $\hat{V} \simeq V^*$. Ahora como $dim(U) = dim(U^*)$, y $dim(\hat{V}^*) = dim(V)$, es suficiente ver que U^* está generado por $\widehat{V}$ como kG–módulo. Sean entonces $s, t \in S$, $v \in V$, y $\phi \in \widehat{V}$, entonces $(t\phi)(sv) = \phi(t^{-1})sv)$ por lo que este será cero si $tH \neq sH$. Por tanto, $t\widehat{V}$ está compuesto de los funcionales lineales que se anulan en todo sV para $sH \neq tH$. Como U es suma directa de sV, todo funcional lineal se expresa como combinación de tales elementos.

Probamos (v). Razonamos esencialmente igual a los anteriores, observamos que $U \otimes V^G$ está generado por $U_H \otimes V$ ($u \otimes gv = g(g^{-1}u \otimes v) \in g(U \otimes V)$ para $g \in G$, $u \in U$, $v \in V$), de tal forma que estudiando la dimensión se sigue el isomorfismo. Efectivamente

$$\begin{aligned} dim(U \otimes V^G) &= dim(U)dim(V^G) \\ &= |G:H|dim(U_H \otimes V). \end{aligned}$$

Probamos (vi). Si α es un elemento de $Hom_{kH}(V, U_H)$, entonces α admite una única extensión $\hat{\alpha} \in Hom_{kG}(V^G, U)$, y cualquier elemento de $Hom_{kG}(V^G, U)$ surge así, porque es la extensión de la restricción a V.

Probamos (vii). basta observar que

$$\begin{aligned} Hom_{kG}(U, V^G) &\simeq Hom_{kG}((V^G)^*, U^*) \\ &\simeq Hom_{kG}((V^*)^G, U*) \\ &\simeq Hom_{kH}(V^*, (U^*)_H) \\ &\simeq Hom_{kH}(U_H, V). \end{aligned}$$

Probamos (viii). Para cada $\gamma \in Hom_{kH}(U_H, V)$ hemos definido una transformación lineal γ' de U a V^G. Hemos de probar que γ' es un kG–homomorfismo, y que la aplicación que envía γ a γ', es un isomorfismo de $Hom_{kH}(U_H, V)$ a $Hom_{kG}(U, V^G)$.

Por construcción de la fórmula de γ', vemos que la aplicación que asocia γ' a γ es lineal e inyectiva, en tanto que $\gamma \neq 0$ obliga $\gamma' \neq 0$, pues $\gamma'(u) = 1 \otimes \gamma(u) + \cdots$ tiene como primer término a $\gamma(u)$. Como $Hom_{kG}(U, V^G)$ y $Hom_{kH}(U_H, V)$ tienen la misma dimensión ya tenemos el isomorfismo. Basta comprobar que γ' es un homomorfismo de módulos.

Si $g \in G$ y $u \in U$, entonces

$$\begin{aligned} \gamma'(gu) &= \sum_{s \in G/H} s \otimes \gamma(s^{-1}gu) \\ &= \sum g(g^{-1}s) \otimes \gamma(s^{-1}gu) \\ &= g \sum g^{-1}s \otimes \gamma(s^{-1}gu) \\ &= g \sum_{t \in G/H} t \otimes \gamma(t^{-1}u), \end{aligned}$$

porque los elementos $g^{-1}s$ nos dan otro conjunto de representantes de coclases. Si $t = sh_t$, $h_t \in H$ entonces:

$$\begin{aligned} \sum t \otimes \gamma(t^{-1}u) &= \sum sh_t \otimes \gamma(h_t^{-1}su) \\ &= \sum s \otimes h_t h_t^{-1} \gamma(su) \\ &= \sum s \otimes \gamma(su) \\ &= \gamma'(u), \end{aligned}$$

luego $\gamma'(gu) = g\gamma'(u)$.

Probamos (ix). Si $\alpha \in Hom_{kH}(V_1, V_2)$, entonces α puede verse como si tuviera imagen en $1 \otimes V_2 \subset V_2^G$, un kG-módulo, luego existe una única extensión a un kG–homomorfismo de

V_1^G a V_2^G. También es claro que para $v_s \in V$

$$\alpha^G(\sum_{s \in G/H} s \otimes v_s) = \sum_{s \in G/H} s \otimes \alpha(v_s),$$

en tanto que

$$\begin{aligned}\alpha^G(s \otimes v_s) &= \alpha^G(s(1 \otimes v_s)) \\ &= s\alpha^G(1 \otimes v_s) \\ &= s(1 \otimes \alpha(v_s)).\end{aligned}$$

Probamos (x). La exactitud de la segunda cadena es fácil de ver. Por la fórmula recién estudiada tenemos que $\alpha^G(s \otimes V) = s \otimes \alpha(V_1)$, y el núcleo de β^G es $s \otimes \alpha(V_1)$, en tanto que $\alpha(V_1)$ es el núcleo de β. La inyectividad y sobreyectividad de α^G y β^G respectivamente es clara.

Además, supongamos que la primera cadena escinde: Sea $\gamma \in Hom_{kH}(V_2, U)$ con $\beta\gamma$ la identidad en V_2. Entonces, $\beta^G\gamma^G$ extiende $\beta\gamma$ aun kG–homomorfismos de V_2^G a V_2^G, que debe ser la identidad por unicidad.

Finalmente, supongamos que $\psi \in Hom(V_2^G, V^G)$ y $\beta^G\gamma$ es la identidad en V_2^G. Sea π el kH–homomorfismo de V^G en V que verifica $\pi(1 \otimes v) = v$, y $\pi(s \otimes v) = 0$ si $s \notin H$. Definimos la aplicación ϕ de V_2 a V dada por

$$\phi(v_2) = \pi\psi(1 \otimes v_2),$$

que es un kH–homomorfismo. Veamos que $\beta\phi$ es la identidad de V_2. Sea $v_2 \in V_2$, luego

$$\psi(1 \otimes v_2) = \sum s \otimes u_s,$$

donde s está en un conjunto de representantes que contiene a 1 y $u_s \in V$. Observamos que

$$\beta^G(\psi(1 \otimes v_2)) = \sum s \otimes \beta(u_s),$$

tiene que ser $1 \otimes v_2$, pues $\beta(u_1) = v_2$. En consecuencia,

$$\begin{aligned}\phi(v_2) &= \pi\psi(1 \otimes v_2) \\ &= \pi(\sum s \otimes u_s) \\ &= u_1,\end{aligned}$$

luego $\beta\phi(v_2) = v_2$.$\square$

El siguiente resultado nos permite describir el proceso de inducir primero, y después restringir en términos de la restricción seguida de inducción. De esta forma podemos relacionar la inducción a G con construcciones que usualmente tratan con subgrupos propios.

Fijamos dos subgrupos de G, a saber H y L. Si $g \in G$ el subconjunto LgH lo llamamos doble coclase de G. Observamos que G es unión disjunta de estas dobles coclases. Sea S un conjunto de representantes de estas dobles coclases. Si V es un kH–módulo, entonces $s \otimes V$ es un sumando de V^G y es un módulo para sHs^{-1}. Observamos que si $h \in H$, $v \in V$

$$shs^{-1}(s \otimes v) = sh \otimes v = s \otimes hv,$$

de donde se sigue que shs^{-1} actúa sobre $s \otimes v$ de acuerdo a como h actúa sobre v. Este es un ejemplo de transporte de estructura, $s \otimes V$ es el $k[sHs^{-1}]$–módulo correspondiente al kH–módulo V. Denotamos por $s(V)$ a cualquier $k[sHs^{-1}]$–módulo en correspondencia con el kH–módulo V de tal manera que $s(V) \simeq s \otimes V$. Ahora $L \cap sHs^{-1}$ es un subgrupo de sHs^{-1}, de tal forma que podemos tomar la restricción de $s(V)$ a $L \cap sHs^{-1}$. Por último, como $L \cap sHs^{-1}$ está contenida en L se puede inducir a L. Estamos en condiciones de enunciar el resultado:

Teorema 3.9 (Teorema de Mackey).

$$(V^G)_L \simeq \bigoplus_{s \in L \backslash G/H} (s(V)_{L \cap sHs^{-1}})^L$$

Prueba. Para cada $s \in S$, denotamos por T_s un conjunto de representantes de coclases a izquierda de $L \cap sHs^{-1}$ en L. Sabemos por teoría de grupos que LsH es la unión disjunta de coclases tsH con $t \in T_s$. Por tanto V^G es la suma directa de todos los subespacios $ts \otimes V$ para $t \in T$ y $s \in S$. Ahora observamos que para s fijo, la suma sobre t, que llamamos V_s es un kL–módulo. Además (V_L^G) es la suma directa en $s \in S$ de los V_s. Basta probar ahora que $V_s \simeq (s(V)_{L \cap sHs^{-1}})^L$.

Estudiamos dimensiones, $dim(V_s) = |L : L \cap sHs^{-1}| dim(V)$. Además, $s \otimes V \subset V_s$ y $s \otimes V$ como $k[L \cap sHs^{-1}]$-módulo es isomorfo a $s(V)$. Basta ver que V_s está generado como kL–módulo por $s \otimes V$. Como $LsH = T_s sH$ esto es claro. $\square$

3.2.2. Vértices y fuentes

En la sección anterior hemos extendido la noción de módulo libre. Ahora hacemos lo propio con la noción de proyectivo. La proyectividad es el concepto categórico de la idea de libre. Así, todo módulo libre es inmediatamente proyectivo, sin embargo el recíproco no es cierto. La ventaja de la proyectividad es que es categórica y preserva algunas de las virtudes de lo libre.

Una definición operativa de módulo proyectivo, es la de ser sumando directo de un libre, esto podemos trasladarlo tal cual al contexto de los H–libres, así lo hacemos:

Proposición 3.4 (Definiciones de H–proyectivo). *Sea U un kG–módulo y H un subgrupo de G, entonces equivalen:*

(i) U es sumando directo de un H–libre.

(ii) Si ϕ es un homomorfismo del kG–módulo V sobre U, y ϕ descompone como kH–homomorfismo entonces ϕ descompone.

(iii) Si ϕ es un homomorfismo sobreyectivo del kG–módulo V sobre el kG–módulo W, y ψ es un homomorfismo de U en W, entonces existe un kG–homomorfismo ρ de U a V con $\phi\rho = \psi$.

(iv) U es sumando directo de $(U_H)^G$.

Prueba. La demostración de la equivalencia de las tres primeras es formalmente idéntica a la de los proyectivos normales. La única que hay que justificar es la última.

Para empezar, es claro que si se da (iv) se sigue inmediatamente (i). Por otro lado, hay un kG–homomorfismo de $(U_H)^G$ sobre U tal que escinde como kH–homomorfismo: si tomamos la identidad de U_H a U, lo podemos extender a un kG–homomorfismo de $(U_H)^G$, y este escinde sobre H. Por tanto si (ii), entonces (iv).□

Los módulos satisfaciendo estas propiedades se dirán H–proyectivos. Nos interesa ahora la pregunta de para qué subgrupos H de G, es un kG–módulo H–proyectivo. Una primera respuesta nos la da el siguiente teorema

Teorema 3.10 (Condición suficiente para H–proyectivo). *Si H es un subgrupo de G conteniendo un p–subgrupo de Sylow de G, entonces todo kG–módulo es H–proyectivo.*

Prueba. La demostración es una reformulación de la del teorema de Maschke.

Si suponemos que $H = 1$, entonces el grupo G tiene orden no divisible por p, el teorema de Maschke nos dice que todo kG–módulo es semisimple, luego proyectivo, que es lo mismo que 1–proyectivo.

Ahora suponemos que H es no trivial. Sea $\phi : V \to U$ un morfismo de kG–módulos de U a V tal que escinde visto en kH–*mod*. Queremos ver que también lo es en kG–*mod*.

Como escinde visto desde kH, se tiene que $Ker(\phi) = W$ es un sumando directo de V como kH–módulo. Vamos a tomar la proyección $\pi : V \to W$, y definimos el kG–homomorfismo

$$\pi' = \frac{1}{|G : H|} \sum_{s \in G/H} s\pi s^{-1}.$$

La clave está en que es posible definir tal morfismo por la hipótesis de que H contiene un p–subgrupo de Sylow de G. Es fácil comprobar que π' es efectivamente un kG–homomorfismo, $\pi'(V) = W$, y que π' actúa como la identidad sobre W. De esta forma, se sigue que ϕ escinde como kG-homomorfismo. □

Obtenemos un corolario, que nos da también una condición suficiente, esta vez para que un kG–módulo sea proyectivo

Introducimos una notación que utilizaremos frecuentemente. Si U, y V son kG–módulos tal que U es isomorfo a un sumando directo de V, escribiremos $U|V$. El siguiente teorema es fundamental.

Corolario 3.2. *Si H es un subgrupo de G que contiene un p–subgrupo de Sylow, y U es un kG–*

módulo tal que U_H es proyectivo, entonces U es proyectivo.

Prueba. Como U es H–proyectivo por hipótesis, se tiene que $U|(U_H)^G$, pero por el lema Ómnibus, U_H proyectivo implica $(U_H)^G$ proyectivo. En resumen U es sumando directo de un proyectivo, y por tanto es proyectivo. $\square$

Teorema 3.11 (Vértices y fuentes)**.** *Sea U un kG–módulo indescomponible.*

(i) Existe un p–subgrupo Q de G, único salvo conjugación en G, tal que U es H–proyectivo si y solo si H contiene un conjugado de Q.

(ii) Existe un único kQ–módulo S, único salvo conjugación en $N_G(Q)$, tal que $U|S^G$.

Al subgrupo Q se le dice vértice de U, y al módulo S fuente de U. La idea es que cuánto más cerca esté Q de ser trivial, más cerca estará U de ser proyectivo. De hecho U es proyectivo si y solo si $Q = 1$.

Prueba. Como U es relativamente proyectivo para cualquier p–subgrupo de Sylow, podemos elegir un p–subgrupo de orden mínimo Q tal que U sea Q–proyectivo.

En particular, se tiene que $U|(U_Q^G)$, por lo tanto hay un sumando indescomponible S de (U_Q), tal que $U|S^G$.

Ahora si H es un subgrupo de G que contiene a Q, entonces $U|(S^H)^G$, en tanto que $(S^H)^G \simeq S^G$, por tanto U es H–proyectivo. Esto también implica que U es ghg^{-1}–proyectivo vía transporte de estructura.

Por otro lado suponemos que H es un subgrupo de G con U H–proyectivo, y que V es un kH–módulo indescomponible con $U|V^G$. Hemos de probar que H contiene un conjugado de Q, y que si $H = Q$ entonces V es conjugado de S por un elemento de $N_G(Q)$. Una vez probado esto como $U|S^G$, tenemos trivialmente que $U|g(S)^G$, para cualquier $g \in G$, y si además $g \in N_G(Q)$, $g(S)$ es un kQ–módulo, y esto termina la prueba.

Así pues, como $S|U_Q$ y $U|V^G$, se sigue que $S|(V^G)_Q$. Utilizamos el teorema de Mackey,

$$(V^G)_Q \simeq \bigoplus_{s \in Q\backslash G/H} (s(V)_{Q\cap sHs^{-1}})^Q,$$

donde, por Krull-Schmidt, $S|(s(V)_{Q\cap sHs^{-1}})^Q$ para algún $s \in G$. Esto implica que $U|(s(V)_{Q\cap sHs^{-1}})^G$, por ser $U|S^G$, luego nuestra elección de Q obliga a que $Q = Q \cap sHS^{-1}$, lo cual implica que H contiene un conjugado de Q. Además si $Q = H$, entonces $Q \cap sQs^{-1} = Q$ significa que $s \in N_G(Q)$, por tanto $S \simeq s(V)$ y $V \simeq s^{-1}(S)$. $\square$

Enunciamos a continuación algunos lemas, en los que intervienen estos invariantes recién definidos.

Lema 3.3. *Si U es un kG–módulo indescomponible con vértice Q, y H es un subgrupo conteniendo a Q entonces existe un kH–módulo indescomponible V satisfaciendo cualesquiera dos de las siguientes propiedades*

(i) $V|U_H$.

(ii) $U|V^G$.

(iii) *V tiene vértice Q .*

El motivo para enunciar este resultado así, es que utilizando la correspondencia de Green, (que exponemos después) puede probarse que existe un módulo verificando las tres simultáneamente.

Lema 3.4. *Si U es un kG–módulo indescomponible con vértice Q y fuente trivial, y H es cualquier subgrupo de G, entonces U_H tiene un sumando indescomponible con un vértice conteniendo a $Q \cap H$.*

Lema 3.5. *Sea U un kG–módulo tal que U_N es indescomponible, donde N es un subgrupo normal de G. Si Q es un vértice de U, entonces QN/N es un p–subgrupo de Sylow de G/N.*

3.2.3. Intersección trivial

En esta sección vamos a estudiar un caso particular de la correspondencia de Green, que es la herramienta principal en esta aproximación a la teoría de representaciones.

Vamos a fijar un p–subgrupo de Sylow P de G y asumimos que es un subgrupo de intersección trivial. Esto es que para todo $g \in G$, $P \cap gPg^{-1}$ es o bien P, o bien 1. Vamos a denotar por L a $N_G(P)$, de tal manera que si $g \in G$ pero $g \notin L$ entonces $P \cap gPg^{-1} = 1$. Enunciamos el resultado principal de la sección:

Teorema 3.12 (Correspondencia de Green para el caso de intersección trivial)**.** *Existe una correspondencia biyectiva entre clases de isomorfía de indescomponibles no proyectivos de kG–módulos y de kL–módulos, tal que si U y V son tales módulos, para G y L respectivamente, entonces*

- $U_L \simeq V \oplus Q$.
- $V^G \simeq U \oplus R$.

donde Q, y R son kL y kG–módulos proyectivos respectivamente.

Esta correspondencia está determinada por la restricción o por la inducción.

<u>Prueba</u>. Por el teorema de Mackey

$$(V^G)_L \simeq \bigoplus_{s \in L \backslash G/H} (s(V)_{L \cap sHs^{-1}})^L,$$

sabemos que $(V^G)_L$ es una suma directa de V y módulos inducidos de subgrupos $L \cap sLs^{-1}$, donde $s \notin L$. ahora como P y sPs^{-1} son los únicos p–subgrupos de Sylow de L y sLs^{-1}, se tiene que $P \cap sPs^{-1}$ es el p–subgrupo de Sylow de $L \cap sLs^{-1}$. Por tanto, si $s \notin L$, la hipótesis de intersección trivial nos da que $L \cap sLs^{-1}$ tiene orden no divisible por p, luego todo módulo es semisimple, y en consecuencia proyectivo. Por tanto tenemos que $(V^G)_L \simeq V \oplus Y$ en donde Y es un kL–módulo proyectivo, en tanto que los inducidos de proyectivos son proyectivos.

Ahora expresamos $V^G \simeq U_1 \oplus \ldots \oplus U_n$ donde los U_i son indescomponibles. Como L contiene un p–Sylow de G, tenemos que U_i es proyectivo si y solo si $(U_i)_H$ es proyectivo. Ahora, como $(V^G)_L$ tiene un único sumando indescomponible no proyectivo, podemos escoger notación de tal manera que $U = U_1$, sea no proyectivo, y Q sea el proyectivo obtenido a partir de la suma de los demás. Tenemos entonces que $V^G \simeq U \oplus Q$, y también tenemos que $U_L \simeq V \oplus R$, donde R es proyectivo, en tanto que $V \oplus Y \simeq (V^G)_L \simeq U_L \oplus Q_L$.

Supongamos ahora que U es cualquier kG–módulo indescomponible no proyectivo. Se sigue que U surge como hemos descrito en el argumento. L contiene un p–Sylow de G, luego todo kG–módulo es L–proyectivo. en particular hay un kL–módulo proyectivo V tal que $U|V^G$, y V ha de ser no proyectivo por ser V^G no proyectivo. Por los argumentos expuestos $U_L \simeq V \oplus R$, para algún kL–módulo proyectivo R.

Hemos construido una correspondencia como la descrita en el enunciado, y además hemos mostrado que es biyectiva. □

Como consecuencia de esta correspondencia se sigue el siguiente corolario

Corolario 3.3. *Si U_1, y U_2 son kG–módulos indescomponibles no proyectivos, y V_1, V_2 son sus kL–módulos correspondientes, entonces existe una sucesión exacta indescomponible (que no escinde)*

$$0 \to U_1 \to U \to U_2 \to 0$$

si y solo si existe una sucesión exacta indescomponible (que no escinde)

$$0 \to V_1 \to V \to V_2 \to 0.$$

Observamos que esta correspondencia, nos da una identificación de módulos salvo proyectivos, este va a ser el contenido del siguiente teorema. Definimos para U_1, y U_2 kG–módulos el espacio $\overline{Hom}_{kG}(U_1, U_2)$, que es el cociente del espacio vectorial $Hom_{kG}(U_1, U_2)$ sobre el subespacio de todos los homomorfismos de U_1 a U_2 tal que factorizan a través de un kG–módulo proyectivo.

Con esta definición tenemos

Teorema 3.13 (Identificación salvo proyectivos). *Si U_1, y U_2 son kG–módulos indescomponibles no proyectivos y V_1, V_2 son sus kL–módulos correspondientes*

$$\overline{Hom}_{kG}(U_1, U_2) \simeq \overline{Hom}_{kL}(V_1, V_2)$$

3.2.4. Ejemplo: Grupos cíclicos

Comenzamos por estudiar los kG–módulos simples con G un grupo cíclico de orden $n = p^a e$ en donde $(p, e) = 1$.

El teorema de Brauer sobre el número de irreducibles modulares, nos dice que habrá tantos kG–módulos simples como clases de conjugación p–regulares haya en G. En nuestro caso, por ser G cíclico, sabemos que hay e clases. Por tanto, hemos de construir e kG–módulos simples no isomorfos entre sí.

Observamos que el polinomio $x^e - 1$ es separable sobre k, en tanto que $(p, e) = 1$. Por tanto, en k hay e raíces e-ésimas de la unidad. Sea λ una de esas raíces. Vamos a construir un kG-módulo asociado a λ. Para ello consideramos un k-espacio vectorial de dimensión 1, y lo dotamos de estructura de kG-módulo a través de la acción

$$g^i v = \lambda^i v$$

en donde g es un generador de G, y v es un elemento arbitrario de V. Claramente V es simple. Además dadas dos raíces e–ésimas distintas λ_1 y λ_2 , y sus respectivos simples asociados V_1 y V_2, se sigue que estos no son isomorfos como kG–módulos. Hemos construido una lista completa de kG–módulos simples no isomorfos.

A continuación vamos a describir los kG-módulos indescomponibles.

Primero vamos a observar que todo kG–módulo indescomponible es un bloque de Jordan. Sea V un kG–módulo, y sea T el endomorfismo de V asociado a g. Entonces tenemos que $T^n = I$ en tanto que $g^n = 1$. En consecuencia, los autovalores de T han de ser raíces n–ésimas de la unidad en k. Por la forma canónica de Jordan V ha de admitir una descomposición en bloques de Jordan

$$V = U_1 + \cdots + U_r$$

En donde cada U_i admite una base $u_1, \ldots, u_r$ de tal forma que

$$T(u_1) = \lambda u_1 + u_2, \quad \ldots \quad T(u_{r-1}) = \lambda u_{r-1} + u_r, \quad T(u_r) = \lambda u_r$$

en donde λ es un autovalor de T. Cada uno de estos bloques es indescomponible como kG–módulo. Por tanto, todo kG–módulo indescomponible aparece como bloque de Jordan.

Ahora vamos a precisar como son estos bloques. Para empezar si U es un kG–módulo indescomponible de dimensión r y autovalor asociado λ, entonces λ es una raíz e–ésima de la unidad, y $r \leq p^a$.

Efectivamente, $1 = \lambda^n = (\lambda^e)^{p^a}$. Como elevar a p es una biyección en k se sigue que $\lambda^e = 1$, y por tanto que λ es raíz e–ésima de la unidad.

Sean λ_1, ... , λ_e las e raíces e–ésimas distintas de la unidad en k y observamos que

$$T'e - I = (T - \lambda_1 I)...(T - \lambda_e I) = (T - \lambda I)S.$$

En donde S es una matriz no singular que conmuta con T. Por tanto,

$$0 = T^n - I = (T^e - I)^{p^a} = (T - \lambda I)^{p^a} S^{p^a}.$$

En consecuencia $(T - \lambda I)^{p^a} = 0$ de donde $r \leq p^a$ (T es una matriz de Jordan).

El recíproco también es cierto. Si suponemos U un bloque de Jordan de dimensión $r \leq p^a$, con endomorfismo asociado T, y autovalor una raíz e–ésima de la unidad λ, entonces es un kG–módulo indescomponible. Efectivamente, $(T - \lambda I)^r = 0$, luego $(T - \lambda I)^{p^a} = 0$ y $(T^e - I)^{p^a} = 0$, todo esto nos da que $T^n = I$, y por tanto tiene una estructura de kG–módulo natural, y es claramente indescomponible.

Finalmente, puesto que dos bloques de Jordan distintos no son isomorfos, en tanto que se caracterizan por su dimensión r, y por su autovalor λ. Hemos obtenido una lista completa de los kG–módulos indescomponibles.

Lo siguiente que hacemos es describir la estructura de estos. Para ello tomamos un kG–módulo indescomponible U, y pretendemos calcular su serie de radicales. Comenzamos investigando el radical de kG.

En kG tenemos que $(g^e - 1)^{p^a} = g^n - 1 = 0$. Por tanto el elemento $g^e - 1$ es nilpotente y está contenido en $rad(kG)$ por ser kG conmutativo.

Ahora $(g^e - 1)U$ es el subespacio W generado por $u_2, \ldots, u_r$. Por tanto, W está contenido en $rad(U) = rad(kG)U$, no le queda otra que ser $W = rad(U)$ por tener codimensión 1. En conclusión, $rad(U)$ es un bloque de Jordan para λ de dimensión $r - 1$. Este razonamiento lo podemos iterar, de tal forma que la serie desciende una dimensión en cada iteración. Hemos conseguido una serie de composición de U, en la que los factores de composición son los bloques de Jordan de dimensión 1 asociados al autovalor λ.

Este ejemplo es un caso particular de un fenómeno más general.

Proposición 3.5 (Módulos uniseriales). *Si A es una K–álgebra finito dimensional con K un cuerpo algebraicamente cerrado, y U es un A–módulo finitamente generado. Entonces equivalen:*

(i) U admite una única serie de composición

(ii) Los sucesivos cocientes de la serie de radicales de U son simples

(iii) Los sucesivos cocientes de la serie de zócalos de U son simples

A un módulo que verifique cualquiera de estas propiedades se le llama uniserial.

<u>Prueba</u>. Supongamos que (i) se verifica y que

$$U = U_0 \supset U_1 \supset \ldots \supset U_n = 0$$

es la única serie de composición de U. En particular U_1 es el único submódulo maximal de U, pues cada submódulo de U es término de la serie de composición. Por tanto, $U_1 = rad(U)$.

U_1 por su parte también ha de de tener una única serie de composición, de donde, con un razonamiento análogo deducimos que $U_2 = rad^2(U)$. Siguiendo este razonamiento vemos que la única serie de composición es la serie radical.

Ahora supongamos (ii). Como $U/rad(U)$ es simple, esto significa que $rad(U)$ es el único submódulo maximal de U, y por tanto cualquier serie de composición de U ha de comenzar como $U \supset rad(U)$. Podemos razonar análogamente para $rad(U)$, de donde concluimos que la serie habría de continuar como $U \supset rad(U) \supset rad^2(U)$. En definitiva, observamos, que hay una única serie de composición que es precisamente la que viene dada por la serie radical.

La equivalencia (i), (iii) se prueba análogamente. □

En vista de que los kG-módulos indescomponibles son uniseriales, tenemos control sobre la estructura de estos. A modo de ejemplo podemos describir la teoría de representación del grupo cíclico G de orden 6 sobre k con característica 3.

Sean λ_1, y λ_2 las raíces cuadradas de la unidad en k. Entonces tenemos dos kG-módulos simples V_1, y V_2, que son bloques de Jordan 1-dimensionales con autovalor asociado λ_1, y λ_2 respectivamente.

Ahora describimos los indescomponibles. Estos van a ser los bloques de Jordan U_{ij} de dimensión $i = 2, 3$ y autovalor asociado λ_j con $j = 1, 2$. Los indescomponibles tienen la siguiente estructura:

$$\begin{tikzcd}
U_{21} \arrow[d, dash, "V_1"] \\
rad(U_{21}) = V_1 \arrow[d, dash, "V_1"] \\
0
\end{tikzcd}$$

$$\begin{tikzcd}
U_{22} \arrow[d, dash, "V_2"] \\
rad(U_{22}) = V_2 \arrow[d, dash, "V_2"] \\
0
\end{tikzcd}$$

$$\begin{tikzcd} U_{31} \arrow[d, dash, "V_1"] \\ rad(U_{31}) = U_{21} \arrow[d, dash, "V_1"] \\ rad(U_{21}) = V_1 \arrow[d, dash, "V_1"] \\ 0 \end{tikzcd}$$

$$\begin{tikzcd} U_{32} \arrow[d, dash, "V_2"] \\ rad(U_{32}) = U_{22} \arrow[d, dash, "V_2"] \\ rad(U_{22}) = V_2 \arrow[d, dash, "V_2"] \\ 0 \end{tikzcd}$$

3.2.5. Ejemplo: $SL(2, p)$

El siguiente grupo que vamos a estudiar en profundidad es $SL(2, p)$.

Probamos antes un lema sencillo:

Lema 3.6 (kG–Módulos simples de p–grupos)**.** *Si G es un p–grupo el único kG–módulo simple es el trivial.*

Prueba. Simplemente hay que observar que el kG–módulo trivial siempre es simple, y que en un p–grupo el único elemento p–regular es la identidad, por tanto aplicando el teorema de Brauer, se tiene que solo hay un kG–módulo simple. □

Comenzamos estudiando los kG–módulos simples para $G = SL(2, p)$. Como dato grupo teórico partimos del conocimiento de que G tiene p clases de conjugación p–regulares. Por tanto, por el teorema de Brauer, hemos de construir p kG–módulos simples no isomorfos.

Sea V_2 el k–espacio vectorial de columnas de longitud 2. Entonces el producto de matrices nos da una acción de G sobre V_2 que lo dota de estructura de kG–módulo. Efectivamente, si tomamos

$$X = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad e \quad Y = \begin{pmatrix} 0 \\ 1 \end{pmatrix},$$

como base de V_2, y tomamos $g \in G$ con

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

Se sigue que $gX = aX + cY$, y que $gY = bX + dY$. Si consideramos ahora el álgebra $k[X, Y]$, la acción de g antes definida nos da un automorfismo del álgebra. Teniendo esto en cuenta definimos el espacio V_n de polinomios homogéneos de grado $n - 1$ en $K[X, Y]$. Este es un k–espacio de dimensión n, que admite estructura de kG–módulo con la acción recién definida. Vamos a probar que los kG–módulos $V_1, \ldots, V_p$ son una lista completa de simples.

Primero observamos que V_1 es el trivial y por tanto es simple, ahora trabajamos el resto, para ello sea $1 \leq n < p$, y sea también el kG–módulo V_{n+1}. Ahora escogemos dos elementos de G

$$g = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad h = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

y tomamos V_{n+1} con estructura de $k\langle g\rangle$-módulo y $k\langle h\rangle$–módulo respectivamente. Probaremos entonces que X^n es un generador de V_{n+1} como $k\langle g\rangle$–módulo y que tiene por zócalo kY^n. Análogamente, se tendrá que V_{n+1} como $k\langle h\rangle$–módulo está generado por Y^n y que su zócalo es kX^n.

Con esta información razonamos de la siguiente forma. Sea W un kG–submódulo de V_{n+1} no nulo. Entonces W es un $k\langle g\rangle$–submódulo y contiene un simple. Como solo hay una opción, a saber kY^n, se sigue que Y^n está contenido en W, y por tanto, por ser kG–submódulo, $W = V_{n+1}$. Hemos probado que V_{n+1} es simple.

Para probar la afirmación que hemos hecho sobre la estructura de V_{n+1} como $k\langle g\rangle$-módulo, vamos a probar un resultado más fuerte. Así pues para $0 \leq i \leq n$, sea W_{i+1} el subespacio de V_{n+1} de dimensión $i + 1$ con base $X^iY^{n-i}, X^{i-1}Y^{n-i+1}, \ldots, XY^{n-1}, Y^n$, y pongamos $W_0 = 0$ de tal manera que tenemos

$$V_{n+1} = W_{n+1} \supset W_n \supset \ldots \supset W_1 \supset W_0$$

donde cada subespacio tiene codimensión 1 con el que le precede.

Para cada $0 \leq i \leq n$ probamos:

- W_i es $k\langle g\rangle$-módulo.
- W_i/W_{i-1} es un $k\langle g\rangle$-módulo trivial.
- Cada elemento de $W_i - W_{i-1}$ genera W_i como $k\langle g\rangle$-módulo.

Vamos a demostrar el resultado haciendo inducción sobre i:

Observamos que $gX = X + Y$, $gY = Y$, y que $gY^n = Y^n$, luego nuestro enunciado es cierto para $i = 1$.

Supongamos verdadero el enunciado para i, y veamos que lo es para W_{i+1}. Utilizando la expansión binomial

$$gX^iY^{n-i} = (X+Y)^iY^{n-i} = X^iY^{n-i} + \binom{i}{1}X^{i-1}Y^{n-i+1} + u$$

en donde u representa una combinación lineal de $X^{i-2}Y^{n-i+2}, XY^{n-1}, \ldots, Y^n$ y está por tanto en W_{i-1}. Ahora como W_{i+1} está generado por X^iY^{n-i} y W_i, y este último es un $k\langle g\rangle$–módulo, se sigue que W_{i+1} también lo es.

Además, como W_{i+1}/W_i es 1-dimensional y $gX^iY^{n-i} - X^iY^{n-i}$ está en W_i, tenemos que W_{i+1}/W_i es un $k\langle g\rangle$–módulo trivial.

Finalmente, como $i < p$ tenemos que $\binom{i}{1} \neq 0$, por lo que $(g-1)X^iY^{n-i}$ es un elemento de $W_i - W_{i-1}$. Por tanto, si $v \in W_{i+1} - W_i$ entonces $v = \alpha X^iY^{n-i} + w$, en donde $\alpha \neq 0$, y $w \in W_i$. En consecuencia,

$$(g-1)v = \alpha(g-1)X^iY^{n-i} + (g-1)w$$

para $(g-1)w \in W_{i-1}$, por ser W_i/W_{i-1} un $k\langle g\rangle$–módulo trivial. Entonces $(g-1)v \in W_i - W_{i-1}$.

Se sigue pues que el $k\langle g\rangle$–módulo generado por v contiene a W_i por contener a un elemento de $W_i - W_{i-1}$, y contiene a v, luego es exactamente W_{i+1}.

Ahora aplicamos estos resultados al caso que veníamos desarrollando.

En particular, el elemento X^n genera V_{n+1} como $k\langle g\rangle$-módulo, pues $X^n \in W_{n+1} - W_n$. Nos queda examinar el zócalo de V_{n+1} como $k\langle g\rangle$–módulo.

Observamos que $g^p = 1$, luego $\langle g\rangle$ es un p–grupo, por lo que el $k\langle g\rangle$–módulo trivial es el único simple, y el subespacio de V_{n+1} de vectores fijados por g es el zócalo. Pero si $v \in V_{n+1} - W_1$, entonces el $k\langle g\rangle$–módulo generado por v no es 1-dimensional, luego $gv \neq v$. Por tanto, $W_1 = kY^n$ es el zócalo.

Ahora vamos a estudiar los indescomponibles proyectivos.

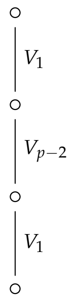
Comenzamos probando que V_p es proyectivo. Para ello comprobamos que como módulo para un p–subgrupo de Sylow es proyectivo. Sabemos que G tiene orden $p(p^2-1)$ y la matriz

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

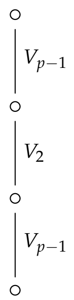
es un elemento de orden p en G, luego genera un p–subgrupo de Sylow. Como ya hemos establecido que V_p es uniserial para este subgrupo, como es p–dimensional, es el indescomponible proyectivo para este grupo cíclico.

Hecha esta observación, sean $P_1, \ldots, P_p$ los indescomponibles proyectivos asociados a los simples $V_1, \ldots, V_p$, de tal forma que $P_p \simeq V_p$. Vamos a establecer la estructura de estos módulos.

Primero P_1 es uniserial, con tres factores de composición salvo que $p = 2$, en cuyo caso hay 2, a saber V_1 y V_1.



Si $p > 2$, entonces P_{p-1} también es uniserial de longitud tres:



Finalmente, si $1 < n < p-1$, entonces $rad(P_n)/soc(P_n) \simeq V_{p+1-n} \oplus V_{p-1-n}$. También tenemos que $P_n/rad(P_n) \simeq soc(P_n) \simeq V_n$ por lo que tenemos P_n en ´´tres capas ", a saber $V_n, V_{p+1-n} \oplus V_{p-1-n}, V_n$. Como $rad(P_n)$ es el único ideal maximal de P_n, y $soc(P_n)$ es único minimal de P_n, el retículo queda tal que así:

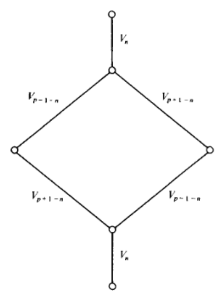


Figura 3.1.:

Para establecer estas estructuras lo que hacemos es investigar la estructura de ciertos productos de módulos simples. Este es el contenido del siguiente lema:

Lema 3.7. *Si* $2 \leq n < p$ *entonces* $V_2 \otimes V_n \simeq V_{n-1} \oplus V_{n+1}$.

<u>Prueba</u>. Comenzamos observando que la aplicación de $V_2 \otimes V_n$ a V_{n+1} dada por el producto

de polinomios, constituye un homomorfismo de módulos sobreyectivo, en tanto que todo monomio de V_{n+1} contiene a X o a Y como factor. Por tanto, para mostrar que el núcleo de este homomorfismo es isomorfo a V_{n-1}, basta definir un homomorfismo inyectivo de V_{n-1} a $V_2 \otimes V_n$ cuya imagen esté contenida en el núcleo del homomorfismo de multiplicación, en tanto que el núcleo tiene dimensión $2n - (n+1) = n - 1$. Así pues, definimos una transformación lineal ϕ de V_{n-1} a $V_2 \otimes V_n$ por la regla $\phi(f) = X \otimes Yf - Y \otimes Xf$, de tal manera que la imagen esté contenida en el núcleo. Comprobemos que además es homomorfismo de módulos.

Supongamos

$$s = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

en donde $ad - bc = 1$, entonces

$$\begin{aligned} s(\phi(f)) &= s(X \otimes Yf - T \otimes Xf) \\ &= s(X) \otimes s(Y)s(f) - s(Y) \otimes s(X)s(f) \\ &= (aX + cY) \otimes (bX + dY)s(f) - (bX + dY) \otimes (aX + cY)s(f) \\ &= (ad - bc)(X \otimes Ys(f) - Y \otimes Xs(f)) \\ &= \phi(s(f)). \end{aligned}$$

Además, ϕ es inyectiva. Los elementos X^iY^{n-2-i}, con $0 \leq i \leq n-2$, forman una base de V_{n-1} y

$$\phi(X^iY^{n-2-i}) = X \otimes X^iY^{n-1-i} - Y \otimes X^{i+1}Y^{n-2-i},$$

y los $2(n-1)$ tensores, cuyas diferencias son las $n-1$ imágenes, forma un subconjunto de dos bases de $V_2 \otimes V_n$, luego son linealmente independientes.

Para probar el lema, es necesario probar que $V_2 \otimes V_n$ contiene un submódulo isomorfo a V_{n+1}. Probamos esto haciendo inducción sobre n. Si $n = p - 1$ entonces $V_2 \otimes V_n$ tiene al módulo proyectivo V_p como imagen homomórfica, luego ha de contener un submódulo isomorfo a V_p. Ahora supongamos que $n + 1 < p$ y $V_2 \otimes V_{n+1}$ es de la forma citada. Basta ver entonces, como V_{n+1} es un módulo simple, que $Hom_{kG}(V_{n+1}, V_2 \otimes V_n) \neq 0$. Observamos que

$$\begin{aligned} Hom_{kG}(V_{n+1}, V_2 \otimes V_n) &\simeq Hom_{kG}(V_{n+1} \otimes V_2*, V_n) \\ &\simeq Hom_{kG}(V_{n+1} \otimes V_2, V_n) \\ &\simeq Hom_{kG}(V_n \oplus V_{n+2}, V_n) \\ &\neq 0. \end{aligned}$$

Probado esto, estamos preparados para establecer la estructura de los módulos proyectivos. El módulo $V_2 \otimes V_p$ es proyectivo, en tanto que V_p es proyectivo, y podemos aplicar l primera parte de la demostración del lema anterior: $V_2 \otimes V_p$ contiene un submódulo isomorfo a V_{p-1} , y el cociente de este submódulo es isomorfo a V_{p+1}. Por tanto, $V_2 \otimes V_p$ tiene un sumando isomorfo a P_{p-1}. Efectivamente, pues $V_2 \otimes V_p$ tiene un sumando indescomponible y su zócalo contiene un submódulo isomorfo a V_{p-1}. Ahora $P_{p-1} \supsetneqq soc(P_{p-1})$, pues V_{p-1} no puede ser proyectivo, en tanto que su dimensión no es divisible por p, luego $P_{p-1} \supset rad(P_{p-1}) \supset soc(P_{p-1})$, y P_{p-1} tiene dimensión al menos $2(p-1)$. Como p divide la dimensión de P_{p-1} y $V_2 \otimes V_p$ es $2p$-dimensional, se sigue que $V_2 \otimes V_p \simeq P_{p-1}$, si $p > 2$ (Si p = 2, $P_{p-1} = P_1$. $6 = dimP_1 + 2dimP_2$, P_1 es 2-dimensional, y su estructura es inmediata). Tenemos entonces que el submódulo $V = soc(V_2 \otimes V_p) \simeq V_{p-1}$, y $V_2 \otimes V_p/U \simeq V_{p-1}$ donde $U = rad(V_2 \otimes V_p)$. Tenemos entonces el siguiente diagrama

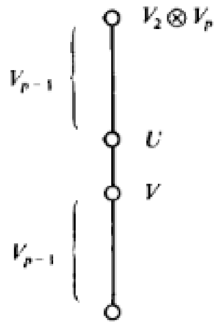


Figura 3.2.:

Vemos que U/V es 2-dimensional. Como U es el único submódulo maximal de $V_2 \otimes V_p$ y V es el único minimal, hemos de mostrar que $U/V \simeq V_2$ para probar que P_{p-1} es uniserial. Observamos que $V_2 \otimes V_p/V \simeq V_{p+1}$, y U/V es el único submódulo maximal de este cociente, luego solo hemos de demostrar que V_{p+1} contiene un submódulo isomorfo a V_2. Teniendo en cuenta que tomar potencia p-ésima nos da un automorfismo de $k[X, Y]$, y que este envía V_2 a V_{p+1}, hemos acabado.

Ahora procedemos a estudiar P_{p-2}, y para ello examinamos $V_2 \otimes P_{p-1}$. Este módulo es proyectivo, y tiene una sucesión de submódulos cuyos sucesivos cocientes son isomorfos a $V_2 \otimes V_{p-1}$, $V_2 \otimes V_2$, y $V_2 \otimes V_2 \otimes V_{p-1}$, esto es, $V_{p-2} \oplus V_p$, $V_1 \oplus V_3$, y $V_{p-2} \oplus V_p$. Como V_p es proyectivo y V_{p-2} es imagen homomórfica, tenemos que $V_2 \otimes P_{p-1}$ tiene un sumando directo isomorfo a $P_{p-2} \oplus V_p \oplus V_p$ ($P_1 \oplus V_3 \oplus V_3$ si $p = 3$). P_{p-2} tiene dos factores de composición isomorfos a V_{p-2}, su dimensión es divisible por p, y sus otros factores de composición solo pueden ser V_3 o V_1 (Solo V_1 si $p = 3$). Por tanto, deducimos que $rad(P_{p-2})/soc(P_{p-2})$ tiene como factores de composición a V_1 y a V_3 (Solo V_1 si $p = 3$).

Hemos de ver que este cociente es isomorfo a $V_1 \oplus V_3$. Si este no fuera semisimple, entonces habría de ser uniserial, por solo tener dos factores de composición, y no sería isomorfo a su dual, que sería uniserial, pero con los factores de composición al revés, sin embargo, P_{p-2} es isomorfo a su dual (en tanto que P_{p-2}^* es el indescomponible proyectivo con $soc(P_{p-2})^* \simeq V_{p-2}^* \simeq V_{p-2}$). Se sigue entonces que $rad(P_{p-2})/soc(P_{p-2})$ es isomorfo a su dual, y hemos establecido la estructura de P_{p-2}.

Ahora supongamos que P_n, con $2 < n < p-1$ es tal y como hemos afirmado. Entonces $V_2 \otimes P_n$ tiene una serie de submódulos con cocientes sucesivos $V_2 \otimes V_n$, $V_2 \otimes (V_{p+1-n} \oplus V_{p-1-n})$, $V_2 \otimes V_n$, esto es, $V_{n-1} \oplus V_{n+1}$, $V_{p+2-n} \oplus V_{p-n} \oplus V_{p-n} \oplus V_{p-n-2}$, $V_{n-1} \oplus V_{n+1}$, donde en el caso de $n = p-2$ el término V_{p-n-2} debe ser eliminado. Como ya hemos tratado los casos P_{p-1}, y P_{p-2}, podemos razonar inductivamente. Suponemos entonces que P_{n+1} también es como hemos afirmado. Como $V_2 \otimes P_n$ es proyectivo, y tiene a $V_{n+1} \oplus V_{n-1}$ como imagen homomórfica, se sigue que $V_2 \otimes P_n \simeq P_{n+1} \oplus U$, en donde U es proyectivo, tiene V_{n-1} como imagen homomórfica, y tiene 4 factores de composición, a saber V_{n-1}, V_{p+2-n}, V_{p-n}, y V_{n-1}. Procediendo exactamente como antes obtenemos que $U \simeq P_{n-1}$, y P_{n-1} es tal y como hemos dicho.

Finalmente nos queda estudiar P_1 examinando $V_2 \otimes P_2$. Obtenemos de nuevo una serie de submódulos pero con V_p como factor. Utilizando la proyectividad y el argumento de antes se concluye que $V_2 \otimes P_2 \simeq P_3 \oplus V_p \oplus U$, donde U es proyectivo, V_1 es imagen homomórfica suyo, y tiene a V_1,V_{p-2}, y V_1 como factores de composición. Por tanto, tenemos ya la estructura deseada.

Estos resultados también pueden deducirse utilizando la correspondencia estudiada en la sección anterior. cf. [Alp86] p75-79.

3.2.6. Correspondencia de Green

La correspondencia establecida en la sección de intersección trivial es tan solo un caso particular de la correspondencia de Green. Esta se aplica a cualquier grupo sin ninguna referencia a la posición de los p–subgrupos de Sylow en el grupo.

Dado que la correspondencia es bastante técnica, vamos a introducir otro caso particular. Sea Q un p–subgrupo de G, y $L = N_G(Q)$. La correspondencia de Green implica entonces que tenemos una correspondencia biyectiva entre las clases de isomorfía de kG–módulos indescomponibles con vértice Q, y las clases de isomorfía de kL–módulos indescomponibles con vértice Q . Además esta correspondencia se comporta muy bien en tanto que si U es un kG–módulo indescomponible con vértice Q, se sigue que $U_L \simeq V \oplus Y$, en donde V es un kL–módulo indescomponible con vértice Q, e Y no contiene sumando indescomponible con vértice Q. Debido al teorema de Krull-Schmidt, la clase de isomorfía de V está determinada. Análogamente se tiene que $V^G \simeq U \oplus X$, en donde U es un kG–módulo indescomponible con vértice Q, y X no contiene sumando indescomponible con vértice Q. Ambas correspondencias son inversas la una de la otra.

En la última sección, trabajamos con un p–subgrupo de Sylow y los kG–módulos indescomponibles no proyectivos, y los propios para el normalizador del p–subgrupo de Sylow en G. La correspondencia de Green nos permitirá relacionar módulos que además no tengan porqué compartir el vértice.

Fijamos algo de notación: Sea Q un p–subgrupo de G, y L un subgrupo de G que contenga a su normalizador. Si P, y R son subgrupos de G, escribimos $P \subset_G R$ para decir que un conjugado de P está contenido en R. Si $\mathcal{H}$ es una colección de subgrupos de G, diremos que $P \subset_G \mathcal{H}$ cuando $P \subset_G H$ para algún $H \in \mathcal{H}$. Ahora fijamos algunas colecciones de p–subgrupos de G:

$$\mathcal{X} = \{sQs^{-1} \cap Q : s \in G, s \notin L\},$$
$$\mathcal{N} = \{sQs^{-1} \cap L : s \in G, s \notin L\},$$

$$\mathcal{E} = \{R : R \subset Q, R \not\subset_G \mathcal{X}\}.$$

Uno debería pensar en $\mathcal{X}$ y $\mathcal{N}$ como subgrupos "pequeños", con respecto a Q; y en $\mathcal{E}$ constituido por Q y sus subgrupos "grandes".

Notamos que cada subgrupo de $\mathcal{X}$ es un subgrupo propio de Q. Finalmente si $\mathcal{H}$ es cualquier colección de subgrupos de G diremos que el kG–módulo U es $\mathcal{H}$–proyectivo si U es suma directa de módulos, de tal forma que cada uno de ellos sea proyectivo relativo a algún subgrupo en $\mathcal{H}$, Enunciamos el teorema:

Teorema 3.14 (Correspondencia de Green)**.** *Existe una correspondencia entre clases de isomorfía de kG–módulos indescomponibles con vértice en $\mathcal{E}$, y clases de indescomponibles de kL–módulos con vértice en $\mathcal{E}$. Si U y V son tales módulos, para G y L respectivamente, entonces U y V tienen el mismo vértice y se tiene que*

- $U_L \simeq V \oplus Y$.
- $V^G \simeq U \oplus X$.

Donde Y es relativamente $\mathcal{N}$-proyectivo, y X es relativamente $\mathcal{X}$–proyectivo.

Veamos que efectivamente generaliza al caso de intersección trivial.

Supongamos que Q es un subgrupo de intersección trivial, entonces $gQg^{-1} \cap Q = 1$ si $g \notin N_G(Q)$. Por tanto, si $s \notin L$, $sQs^{-1} \cap Q = 1$ por lo que $\mathcal{X} = \{1\}$, y $\mathcal{E}$ está compuesto por todos los subgrupos no triviales de Q. Además, si Q es un p–subgrupo de Sylow, entonces $sQs^{-1} \cap L = 1$ si $s^{-1} \notin L$, de no ser así $sQs^{-1} \cap L$ sería un p–subgrupo de L, luego existiría $x \in L$ tal que $x(sQs^{-1} \cap L)x^{-1} \subset Q$, de donde $xsQs^{-1}x^{-1} \cap Q \neq 1$ y $xs \notin L$ lo cual es una contradicción. En consecuencia, $\mathcal{N} = \{1\}$ y tanto X como Y son proyectivos.

La demostración de la correspondencia de Green es muy técnica, se puede encontrar la demostración en [Alp86, p. 84].

3.2.7. Bloques y el grupo de defecto

Vamos ahora a introducir la noción de bloque. Esta nos permitirá partir el conjunto de clases de isomorfía de indescomponibles del álgebra kG de una manera que será muy útil. De hecho los tres grandes teoremas se enuncian sobre bloques y no sobre el álgebra kG.

Comenzamos probando que dado un álgebra finito dimensional, esta admite una descomposición esencialmente única en álgebras indescomponibles:

Teorema 3.15. *Sea A una álgebra finito dimensional, entonces esta admite una única descomposición en suma directa de subálgebras indescomponibles.*

Si $A = A_1 + \cdots + A_r$ es una descomposición como la descrita, decimos que los sumandos A_i son los bloques del álgebra A. Observamos que los bloques son ideales, y que si toma uno $a_i \in A_i$, $a_j \in A_j$ con $i \neq j$, entonces $a_ia_j = 0$, pues $a_ia_j \in A_i \cap A_j$.

Prueba. Expresamos $A = A_1 + \cdots + A_r$ como suma directa de álgebras A_i cada una de ellas indescomponible como álgebra. Consideramos ahora B un sumando en otra descomposición de este tipo. Hemos de probar que $B = A_i$ para algún $1 \leq i \leq r$.

Sea $b \in B$ y lo expresamos como $b = a_1 + \cdots + a_r$, donde cada $a_i \in A_i$. Como cada A_i tiene unidad, a saber, la componente del 1 de A en A_i; y B es un ideal, se sigue que $a_i \in B$ para cada i. Por tanto, $B = (B \cap A_1) + \cdots + (B \cap A_r)$. Esta es una descomposición de B. Por nuestra hipótesis sobre B, todos los sumandos han de ser 0, salvo uno de ellos. Luego $B \subset A_i$ para algún A_i. Haciendo el razonamiento idéntico cambiando los papeles, se sigue la doble inclusión. □

Si M es un A-módulo verificando que , $A_iM = M$, y $A_jM = 0$ para $i \neq j$, decimos que M pertenece al bloque A_i. Dado un A_i-módulo N, podemos convertirlo en un A-módulo perteneciente al bloque A_i sin más que exigir que todo A_j con $i \neq j$ anule a N. De hecho todo A-módulo perteneciente a un bloque surge así.

Hay otra manera de expresar esto más anillo-teórica. Sea $1 = e_1 + \cdots + e_r$ una descomposición de la unidad, de tal forma que e_i sea la identidad de A_i. Si M pertenece a A_i, entonces e_i actúa como la identidad sobre M y e_j con $j \neq i$ anula a M. Por otro lado si esto le ocurre a un A-módulo M, tenemos que $AM = Ae_iM = A_iM$, y $A_jM = Ae_jM = 0$.

Tenemos que la relación de pertenencia a un bloque es cerrada por sumas, submódulos y cocientes. Además, si M_i, y M_j son módulos pertenecientes a los bloques A_i, y A_j respectivamente, para $i \neq j$, se sigue que $Hom_A(M_i, M_j) = 0$.

Lo interesante de la relación de pertenencia a un bloque es que nos da descomposiciones de A–módulos

Proposición 3.6 (Descomposición de un A–módulo a través de los bloques)**.** *Si M es un A–módulo, este admite una descomposición única*

$$M = M_1 + \cdots + M_r$$

donde M_i pertenece al bloque A_i.

Prueba. Llamemos $M_i = A_iM$, de tal manera que M_i es un A-módulo perteneciente a A_i. Además $M = 1M = M_1 + \cdots + M_r$ y esta suma es directa. Efectivamente, supongamos que $m_1 + \cdots + m_r = 0$, con $m_i \in M_i$. Si aplicamos a esta suma la unidad de A_j, obtenemos que $m_j = 0$ con $1 \leq j \leq r$.

Por otro lado, supongamos que $M = N_1 + \cdots + N_r$ es otra descomposición del tipo estudiado. Entonces, $N_i = A_iN_i \subset A_iM = M_i$, cambiando los papeles se obtiene que $N_i = M_i$. □

De esta forma, el estudio de los A–módulos en general, queda reducido al estudio de los A_i–módulos.

Lo siguiente que hacemos es establecer un criterio útil para determinar los bloques (Este es muy cercano a la definición original de Brauer cf[RB37, RB]). La estrategia se basa en el estudio de los simples que puede haber en un bloque. Si M es un A–módulo perteneciente a A_i, entonces todo factor de composición suyo, en tanto que cociente de M y sus submódulos, pertenecerá también al bloque. Recíprocamente, si cada factor de composición de M pertenece a A_i, la unidad de A_i actúa como la identidad sobre estos, y las de A_j los anula, de donde M también estará sometido a este comportamiento, luego M pertenece a A_i.

Proposición 3.7 (Determinación de los bloques a través de simples)**.** *Si S y T son A-módulos simples, entonces equivalen:*

(i) S y T pertenecen al mismo bloque.

(ii) Existen A–módulos simples
$$S = S_1, \dots, S_m = T$$
tal que S_i, S_{i+1}, $1 \leq i < m$, son factores de composición de un A–módulo proyectivo indescomponible.

(iii) Existen A–módulos simples
$$S = T_1, \dots, T_n = T$$
tal que T_i, T_{i+1}, $1 \leq i < n$, son iguales o existe una extensión que no escinde de uno para el otro.

Prueba. Las tres condiciones describen tres relaciones sobre el conjunto de A–módulos simples y hemos de ver que son la misma.

Si T y T' son A–módulos simples y existe una extensión M de T por T' que no escinde, entonces M es un módulo uniserial, luego es imagen homomórfica del indescomponible proyectivo asociado a T. Por tanto, (iii) implica (ii). Además por la proposición 3.6, cualquier módulo indescomponible pertenece a un bloque luego (ii) implica (i).

Sean S y T A–módulos simples que pertenecen a B bloque de A, y suponemos que no son como en (ii). En particular podemos escribir
$$B = P_1 + \cdots P_s + Q_1 + \cdots + Q_t,$$
como suma de indescomponibles proyectivos, donde cada P_i está relacionado con S según (ii) y ningún factor de composición de Q_j está relacionado con S según (ii). Esto se verifica porque S y T son imágenes homomórficas de B-módulos proyectivos indescomponibles en tanto que son B–módulos simples. Esto implica que $Hom_B(P_i, Q_j) = 0$ y $Hom_B(Q_j, P_i) = 0$, pues ningún factor de composición de Q_j puede serlo de P_i. Por tanto, $P_1 + \cdots + P_s$ y $Q_1 + \cdots + Q_t$ son invariantes bajo todos los endomorfismos de B, luego son ideales, lo cual es una contradicción.

Finalmente veamos que (ii) implica (iii). Para ello es suficiente demostrar que si V es un A–módulo simple, y P es su proyectivo indescomponible asociado, entonces V está relacionado con cada uno de los factores de composición de P a través de la relación (iii). De hecho, si S y T están relacionados según (ii), entonces uno puede expandir la sucesión dada añadiendo entre S_i y S_{i+1} el módulo simple correspondiente al indescomponible proyectivo que tiene a

S_i y S_{i+1} como factores de composición, de tal manera que se sigue teniendo una sucesión al modo de (ii).

Por tanto, para finalizar la demostración, probamos que si W es factor de composición de $rad^{i+1}(P)/rad^{i+2}(P)$, entonces existe un factor de composición U de $rad^{i}(P)/rad^{i+1}(P)$ y una extensión que no escinde de W por U. Para ello, probamos un enunciado más general: Si X es un A–módulo y $rad(X)$ es semisimple, entonces para cualquier factor de composición W de $rad(X)$, hay un factor de composición U de $X/rad(X)$ y una extensión que no escinde de W por U.

Podemos suponer que $rad(X) = W \oplus W'$, en tanto que $rad(X)$ es semisimple. El módulo X/W' satisface las mismas condiciones, así que sin perdida de generalidad suponemos que $rad(X) = W$.

Existen submódulos $Y_1, \cdots Y_n$ de X conteniendo a W tales que X/W es suma directa de simples Y_i/W. Ahora $rad(X) = rad(A)X$, por lo que $rad(X)$ es la suma de los $rad(A)Y_i = rad(Y_i)$. Por tanto, existe j con $1 \leq j \leq n$, tal que $rad(Y_j) \neq 0$. Como $W = rad(X)$ es simple, tenemos que $rad(Y_j) = W$, y entonces Y_j es una extensión que no escinde de W por Y_j/W. $\square$

La segunda condición nos dice cómo determinar la descomposición de A en bloques, si tenemos una descomposición en indescomponibles proyectivos de A. Supongamos que $A = P_1 + \cdots + P_k$ es tal descomposición. Supongamos que $P_1, \ldots, P_j$ pertenecen al mismo bloque , y ningún otro sumando pertenece a este bloque. Entonces, el bloque es $P_1 + \ldots + P_j$. De hecho si B es tal bloque, entonces $B = BA$, y $BP_i = P_i$, para $1 \leq i \leq j$, y $BP_i = 0$ para $i > j$.

Llegados a este punto, particularizamos la discusión sobre álgebras de grupo. La aproximación módulo-teórica al estudio de los bloques pasa por ver a kG como un $k[G \times G]$–módulo con la acción

$$(g_1, g_2)a = g_1 a g_2^{-1}, \quad a \in kG, \quad g_1, g_2 \in G.$$

De esta forma, los submódulos son los ideales de kG. En particular, kG admite una expresión como suma de $k[G \times G]$–módulos indescomponibles que son precisamente los bloques de kG. Estos bloques como $k[G \times G]$–módulos son dos a dos no isomorfos, esto se debe a que sus anuladores en $k[G \times 1]$ son distintos.

Ahora nos gustaría aplicar la teoría que hemos construido sobre módulos indescomponibles al estudio de los bloques.

Vamos a definir un homomorfismo que nos será de gran utilidad. $\delta : G \to G \times G$ el cual actúa según $(g) \mapsto (g, g)$.

Teorema 3.16. *Si B es un bloque de kG entonces B tiene un vértice, como $k[G \times G]$–módulo, de la forma $\delta(D)$, en donde D es un p–subgrupo de G.*

Si H y K son subgrupos de G con $\delta(H)$ y $\delta(K)$ conjugados en $G \times G$, entonces es sencillo ver que H y K son conjugados en G. Por tanto, los subgrupos D de G tal que $\delta(D)$ es vértice del $k[G \times G]$–módulo B, son una clase de conjugación de p–subgrupos de G. Estos son los grupos de defecto de B. El término defecto se debe a que el tamaño de D (Esto es el defecto como cantidad aritmética cf. [Bra44]), es una medida de la desviación del álgebra B de ser semisimple. Si D es de orden p^d, entonces decimos que B tiene defecto d.

Prueba.Basta probar que el $k[G \times G]$–módulo B es $\delta(G)$–proyectivo pues de ser así, $\delta(G)$ contendría un vértice de B. Como B es sumando directo del $k[G \times G]$–módulo kG, solo hemos de demostrar que kG es $\delta(G)$–proyectivo.

Observamos que kG contiene al subespacio $k1$, que es un $k[\delta(G)]$–módulo trivial. Además:

$$dim_k(kG) = |G|dim_k(k1) = |G \times G : \delta(G)|dim_k(k1)$$

Como es claro que $k1$ genera al $k[G \times G]$–módulo kG, se sigue que $kG \simeq (k1)^{G \times G}$, luego kG es claramente $\delta(G)$–proyectivo. □

El grupo de defecto de un bloque está relacionado con los módulos en el bloque de la siguiente forma:

Teorema 3.17. *Si B es un bloque de G y D es un grupo de defecto de B, entonces cualquier kG–módulo indescomponible perteneciente a B tiene vértice contenido en D.*

De hecho uno puede caracterizar el grupo de defecto de un bloque como uno de los vértices más grandes entre los asociados a un bloque.

Prueba. Vamos a considerar B como un kG–módulo usando la conjugación: si $g \in G$, $\beta \in B$, entonces $g\beta = g\beta g^{-1}$. Si U es cualquier kG–módulo entonces existe una transformación lineal ϕ del kG–módulo $B \otimes U$ (con la acción diagonal) al kG–módulo U que envía $\beta \otimes u$ al producto βu (por ser bilineal).

Además esta transformación es un kG–homomorfismo:

$$\begin{aligned} \phi(g(\beta \otimes u)) &= \phi(g\beta g^{-1} \otimes gu) \\ &= g\beta g^{-1} gu \\ &= g(\beta u) \\ &= g\phi(\beta \otimes u). \end{aligned}$$

También hay un kG–homomorfismo de U a $B \otimes U$. Sea e la unidad de B. Hay una transformación lineal ψ de U a $B \otimes U$ que envía $u \in U$ a $e \otimes u$. Veamos que es un kG–homomorfismo:

$$\begin{aligned} \psi(gu) &= e \otimes gu \\ &= g(e \otimes u) \\ &= g\psi(u). \end{aligned}$$

Si U pertenece al bloque B, entonces $eu = u$ para cada $u \in U$, por lo que la composición de estos homomorfismos nos da la identidad. Por tanto, $U|B \otimes U$, y es suficiente probar que $B \otimes U$ es D–proyectivo, pues de ser así, U también lo es.

Sin embargo, por el lema 3.3 (v), es suficiente probar que el kG–módulo B es D proyectivo, pues entonces $B \otimes U$ también lo es.

El isomorfismo $G \simeq \delta(G)$ nos permite, por transporte de estructura, considerar B como $k\delta(G)$–módulo. Por tanto, solo tenemos que probar que B como $k\delta(G)$–módulo es $\delta(D)$–proyectivo.

Sabemos que B, como $k[G \times G]$–módulo es inducido desde un $k\delta(G)$, luego por el teorema de Mackey, B como $k\delta(G)$–módulo es proyectivo respecto a la colección de subgrupos

$$\delta(G) \cap (g_1, g_2)\delta(D)(g_1, g_2)^{-1}$$

en donde $g_1, g_2 \in G$. Es suficiente probar que cada uno de estos subgrupos está conjugado en $\delta(G)$ con $\delta(D)$. Observemos que para $d \in D$, $g_1, g_2 \in G$ y $(g_1, g_2)\delta(d)(g_1, g_2)^{-1} \in \delta(G)$, se tiene que

$$\begin{aligned}(g_1, g_2)\delta(d)(g_1, g_2)^{-1} &= (g_1 d g_1^{-1}, g_2 d g_2^{-1})\\ &= (g_1 d g_1^{-1}, g_1 d g_1^{-1})\\ &= \delta(g_1)\delta(d)\delta(g_1)^{-1}\end{aligned}$$

está contenido en $\delta(g_1)\delta(D)\delta(g_1)^{-1}$, un conjugado de $\delta(D)$ en $\delta(G)$, tal y como queríamos.□

Por último vamos a probar algunas propiedades de los grupos de defecto:

Teorema 3.18 (Los grupos de defecto están lejos de ser arbitrarios)**.** *Sea B un bloque de G, y sea D su grupo de defecto, entonces:*

(i) Si S es un p–subgrupo de Sylow de G que contiene a D, entonces hay un elemento $c \in C_G(D)$ tal que $D = S \cap cSc^{-1}$.

(ii) D contiene todo subgrupo normal de G.

(iii) D es el mayor p–subgrupo normal de $N_G(D)$

Prueba. (i) implica los otros dos. Supongamos (i) y sea N un p–subgrupo normal de G. Por el teorema de Sylow, N está contenido en todos los p–subgrupos de Sylow de G, luego $N \subset S$ y $N \subset cSc^{-1}$. Por tanto, $N \subset D$. Sea ahora T un p–subgrupo de Sylow de $N_G(D)$ y sea S tal que contiene a T. Entonces

$$D \subset T \cap cTc{-1} \subset S \cap cSc^{-1} = D$$

pero cTc^{-1} también es un p–subgrupo de Sylow de $N_G(D)$, luego D es la intersección delos p–subgrupos de Sylow de $N_G(D)$. Como todo p–subgrupo normal de $N_G(D)$ está contenido en algún p–subgrupo de Sylow de $N_G(D)$ hemos probado (iii).

Para probar (i) , estudiamos kG como $k[S \times S]$–módulo. Para ello, necesitamos algunas propiedades de tal restricción que agrupamos en el siguiente lema.

Lema 3.8. *Sea H un subgrupo de G y t un elemento de G.*

(i) El $k[H \times H]$–submódulo $kHtH$ de kG es inducido desde el módulo trivial de

$$(1,t)^{-1}\delta(H \cap tHt^{-1})(1,t)$$

(ii) Si H es un p–subgrupo de G, entonces $kHtH$ es indescomponible como $k[H \times H]$–módulo y su vértice es

$$(1,t)^{-1}\delta(H \cap tHt^{-1})(1,t)$$

(iii) Si Q es un p–subgrupo de H, $C_G(Q) \subset H$ y $t \notin H$, entonces ningún sumando indescomponible de $kHtH$ tiene un vértice que contenga a $\delta(Q)$.

Para probar el lema, consideramos el subgrupo de $H \times H$ formado por los elementos que dejan t fijado. Si $h_1, h_2 \in H$, entonces $(h_1, h_2)t = t$ si y solo si $h_1 t h_2^{-1} = t$, esto es si, $h_2 = t^{-1}h_1 t$. Por tanto, este subgrupo está compuesto por los pares $(h, t^{-1}ht)$ tal que $h \in H$, y $t^{-1}ht \in H$, esto significa que $h \in H \cap tHt^{-1}$. Es decir, el subgrupo está formado por todos los elementos

$$(1,t)^{-1}(h,h)(1,t)$$

en donde $h \in H \cap tHt^{-1}$, lo cual es el subgrupo

$$(1,t)^{-1}\delta(H \cap tHt^{-1})(1,t)$$

La dimensión de $kHtH$ es el producto de $|H|$ y el número de coclases dobles HtH, luego

$$\begin{aligned} dim(kHtH) &= |H||H : H \cap tHt^{-1} \\ &= |H \times H : (1,t)^{-1}\delta(H \cap tHt^{-1})(1,t)| \end{aligned}$$

Además, es claro que t genera $kHtH$ como $k[H \times H]$–módulo, luego por la caracterización de módulo inducido, hemos probado (i).

El segundo enunciado es ahora inmediato, pues $kHtH$ es el módulo inducido desde el módulo trivial de subgrupos de un p–subgrupo, luego es indescomponible con el subgrupo como vértice.

Ahora estudiamos (iii). Del primer enunciado se sigue que cada sumando indescomponible de $kHtH$ tiene un vértice contenido en $(1,t)^{-1}\delta(H \cap tHt^{-1})(1,t)$. Por tanto, si (iii) es falso entonces hay un conjugado en $H \times H$ de $\delta(Q)$, el cual está contenido en $(1,t)^{-1}\delta(H \cap tHt^{-1})(1,t)$. en particular, existen $h_1, h_2 \in H$ tales que

$$(h_1,h_2)^{-1}\delta(Q)(h_1,h_2) \subset (1,t)^{-1}\delta(G)(1,t)$$

esto es,

$$(1,t)(h_1,h_2)^{-1}\delta(Q)(h_1,h_2)(1,t)^{-1} \subset \delta(G)$$

Esto significa que si $x \in Q$, entonces

$$h_1^{-1}xh_1 = th_2^{-1}xh_2t^{-1}$$

luego $h_! th_2^{-1} \in C(Q)$ y $t \in h_1^{-1}C(Q)h_2 \subset H$, lo cual es una contradicción.

Una vez hemos probado el lema, retomamos la demostración.

Como $\delta(D) \subset S \times S$ y B, visto como $k[G \times G]$–módulo, tiene a $\delta(D)$ como vértice, se sigue del lema 3.3 que la restricción de B a $S \times S$ admite un sumando indescomponible con vértice $\delta(D)$. Observamos que B es sumando de kG y

$$(kG)_{S\times S} \simeq \bigoplus_{t\in S\backslash G/S} kStS,$$

por ser G una unión disjunta de todos los S, S–coclases dobles. El lema nos dice que cada $k[S \times S]$-módulo $kStS$ es indescomponible y tiene a $(1,t)^{-1}\delta(S \cap tSt^{-1})(1,t)$ como vértice. Por tanto, existe $t \in G$ tal que $\delta(D)$ está conjugado en $S \times S$ con $(1,t)^{-1}\delta(S \cap tSt^{-1})(1,t)$. Esto es , que existe $r, s \in S$ con

$$\delta(D) = (r,s)(1,t)^{-1}\delta(S \cap tSt^{-1})(1,t)(r,s)^{-1}$$

En particular, $|D| = |S \cap tSt^{-1}|$. Además esto implica que

$$(1,t)(r,s)^{-1}\delta(D)(r,s)(1,t)^{-1} \subset \delta(G)$$

luego para cualquier $d \in D$,

$$r^{-1}dr = ts^{-1}dst^{-1},$$

esto significa que $rts^{-1} \in C(D)$. Pongamos entonces $c = rts^{-1}$. Queremos probar que $D = S \cap cSc^{-1}$.

Ciertamente D está contenido en esta intersección, en tanto que $D \subset S$, y $c \in C(D)$, luego solo hemos de demostrar que Dy $S \cap cSc^{-1}$ tienen el mismo orden. Efectivamente

$$\begin{aligned} |S \cap cSc^{-1}| &= |S \cap rts^{-1}Sst^{-1}r^{-1}| \\ &= |r^{-1}Sr \cap tSt^{-1}| \\ &= |S \cap tSt^{-1}| \\ &= |D|. \end{aligned}$$

□

3.2.8. Los tres grandes teoremas

Vamos a estudiar como determinar los bloques localmente, y a relacionar esto con la correspondencia de Green. La idea fundamental es construir una forma de asignar bloques de subgrupos de G a bloques de G. Supongamos $H < G$, b es un bloque de H, y B es un bloque de G. Diremos que B corresponde a b, si:

- b es un sumando directo de $B_{H\times H}$ como $k[H \times H]$–módulo.
- B es el único bloque de G con esa propiedad.

Si b es tal que existe un bloque B de G con esa propiedad, ponemos que $B = b^G$, y decimos que b^G está definido.

De esta forma hemos construido una correspondencia entre bloques de H, y bloques de G. Estudiamos sus propiedades básicas.

Proposición 3.8 (Propiedades básicas de la correspondencia)**.** *Sea b un bloque de H subgrupo de G, y sea D el grupo de defecto de b.*

(i) Si b^G está definido, entonces D está contenido en un grupo de defecto de b^G.

(ii) Si H está contenido en el subgrupo K de G, con b^K, $(b^K)^G$, y b^G definidos, se tiene que $b^G = (b^K)^G$.

(iii) Si $C_G(D) \subset H$, entonces b^G está definido.

Prueba. Sea E un grupo de defecto de $B = b^G$ de tal manera que el $k[G \times G]$–módulo B tiene como vértice a $\delta(E)$. Como $b | B_{H \times H}$ se sigue del teorema de Mackey que el vértice $\delta(D)$ de b es conjugado en $G \times G$ de un subgrupo de $\delta(E)$. Si $(g_1, g_2) \in G \times G$ conjuga $\delta(D)$ en $\delta(E)$, en particular g_1 conjuga D en E. Esto demuestra (i).

(ii) se sigue de la definición en tanto que $b|(b^G)_{H\times H}$, y $b|((b^K)^G)_{H\times H}$, esto último porque $b|(b^K)_{H\times H}$, y $b^K|((b^K)^G)_{K\times K}$.

Para probar (iii) hemos de comprobar que la hipótesis implica que b ocurre exactamente una vez en la descomposición de $(kG)_{H\times H}$ en indescomponibles. Como kH es suma directa de bloques de H, todos no isomorfos dos a dos como $k[H \times H]$-módulos, es suficiente probar que $b \nmid kHtH$ para $t \notin H$. Puesto que b tiene como vértice a $\delta(D)$, aplicando el lema de la sección anterior se sigue que ningún sumando indescomponible de $kHtH$ tiene un vértice que contenga a $\delta(D)$. □

Estamos en condiciones de probar el Primer gran teorema.

Nos preguntamos, cuál es el correspondiente de Green del $k[G \times G]$–módulo indescomponible B, en donde B es un bloque de G. Si D es un grupo de defecto de B, entonces $N_G(D) \times N_G(D)$ contiene al normalizador de $\delta(D)$ en $G \times G$, un vértice de B, por tanto hay un $k[N_G(D) \times N_G(D)]$–módulo correspondiente. El primer gran teorema nos dice que este es un bloque.

Teorema 3.19 (Primer gran teorema de Brauer)**.** *Si D es un p–subgrupo de G y H es un subgrupo de G que contiene a $N_G(D)$, entonces hay una biyección entre los bloques de H con defecto D, y los bloques de G con defecto D, a través de $b \mapsto b^G$.*

Para el caso más importante, $H = N_G(D)$, diremos que b es el correspondiente de Brauer de b^G.

Prueba. Como el centralizador de D está contenido en H, b^G está definido.

Sea b un bloque de H con defecto D y pongamos $B = b^G$. Ahora $H \times H$ contiene al normalizador de $\delta(D)$ en $G \times G$, en tanto que $N_G(D) \times N_G(D) \subset H \times H$. b es un $k[H \times H]$–módulo indescomponible con vértice $\delta(D)$, y $b|B_{H\times H}$, por el teorema 12.2 de [Alp86] tal B también tiene como vértice a $\delta(D)$, esto significa que B tiene como grupo de defecto a D.

Además, por el mismo teorema B y b están en correspondencia de Green con respecto a $H \times H$. Por tanto, la aplicación $b \mapsto b^G$ es una biyección de bloques de H con defecto D y bloques de G con defecto D. Nos queda ver que si B es un bloque de G con defecto D, entonces surge de esta manera. Por el lema 3.3 , $B_{H\times H}$ tiene un sumando indescomponible con vértice $\delta(D)$, pero $B|kG$ y los únicos sumandos indescomponibles de $(kG)_{H\times H}$ que contienen a $\delta(D)$ son los sumandos de kH por el lema 3.8, y estos son precisamente los bloques de H. Por tanto, hay un bloque b de H con grupo de defecto D tal que $b|B_{H\times H}$. □

Ahora vamos a probar la versión módulo-teórica del segundo gran teorema. Su objeto es la relación entre la correspondencia de Green y la de Brauer. En realidad vamos a probar un resultado más general.

Teorema 3.20 (Segundo gran teorema de Brauer). *Sea U un kG–módulo indescomponible perteneciente al bloque B de G. Sea V un kH–módulo indescomponible, para un subgrupo H de G, el cual pertenece a un bloque b de H con vértice Q tal que $C_G(Q) \subset H$. Si $V|U_H$, entonces b_G está definido y $b^G = B$.*

Prueba.Primero observamos que existe un grupo de defecto de b que contiene a Q por el teorema 3.17 , luego su centralizador está contenido en H y se sigue que b^G está definido. Ahora razonamos por reducción al absurdo, concretamente suponemos que $B \neq b^G$.

Sea e la unidad de b, y sea $kG = kH + M$, en donde M es la suma de todos los espacios $kHtH$ para $t \notin H$. De esta forma $ekG = ekH + eM = b + eM$ es una suma directa de kH–módulos. Como $H \times 1 \subset H \times H$, b y M son $k[H \times H]$–módulos, y e conmuta con todos los elementos de $k[H]$, se sigue que además es suma directa de $k[H \times H]$–módulos. Para $k[H \times H]$–módulos tenemos también que $eB|ekG$, luego $eB|e + eM$, y $eM|M$. Como b es un $k[H \times H]$–módulo indescomponible y no es sumando de $B_{H\times H}$ por hipótesis, se tiene que $eB|eM$ y $eB|M$. Por tanto el lema 3.8 nos dice que ningún sumando indescomponible del $k[H \times H]$–módulo eB tiene un vértice que contenga a $\delta(Q)$.

Se sigue de esto que ningún sumando indescomponible del $k[\delta(H)]$–módulo $eB_{\delta(H)}$ tiene un vértice que contenga a $\delta(Q)$. De hecho, el teorema de Mackey implica que $eB_{\delta(H)}$ es relativamente proyectivo para el conjunto de subgrupos formado por los vértices de los sumandos indescomponibles de eB intersecados con $\delta(H)$. Ahora utilizando el isomorfismo $\delta(H) \simeq H$, y el transporte de estructura, para deducir que eB, como kH–módulo con los elementos de H actuando por conjugación, no posee sumando indescomponible con vértice conteniendo a Q. Lo mismo se verifica para $eB \otimes eU$.

Ahora $eV = V$, pues V pertenece a b. Entonces, $V|U_H$ implica que $V|eU$. Para alcanzar una contradicción bastará demostrar, en tanto que V tiene vértice Q, que $eU|eB \otimes eU$.

Comenzamos definiendo un homomorfismo ϕ de eU a $eB \otimes eU$ por

$$\phi(w) = eE \otimes w.$$

En donde E es la unidad de B. Esta es claramente una aplicación lineal, y además es un kH–homomorfismo:

$$\begin{aligned}\phi(hw) &= eE \otimes hw\\ &= heEh^{-1} \otimes hw\\ &= h(eE \otimes w)\\ &= h(\phi(w)).\end{aligned}$$

Ahora definimos otra transformación lineal ψ, esta vez de $eB \otimes eU$ a eU a través de

$$\psi(a \otimes w) = aw.$$

Esta aplicación también es un kH–homomorfismo:

$$\begin{aligned}\psi(h(a \otimes w)) &= \psi(hah^{-1} \otimes hw)\\ &= hah^{-1}hw\\ &= h(aw)\\ &= h\psi(a \otimes w).\end{aligned}$$

Finalmente, si $w \in eU$, entonces $ew = w$ y $Ew = w$, en tanto que $w \in U$ que está en B. Por tanto,

$$\begin{aligned}\psi(\phi(w)) &= \psi(eE \otimes w)\\ &= eEw\\ &= w.\end{aligned}$$

Luego $eU|eB \otimes eU$ $\square$

Algunas consecuencias importantes son:

Corolario 3.4 (Módulos en correspondencia de Green tienen sus bloques en correspondencia de Brauer)**.** *Si U es un kG–módulo indescomponible perteneciente al bloque B con vértice Q, y V es $kN_G(Q)$–módulo indescomponible correspondiente que pertenece al bloque b, entonces b^G está definido y $b^G = B$*

Corolario 3.5. *Si B es un bloque de G con grupo de defecto D, entonces hay un kG–módulo indescomponible perteneciente a B con vértice D.*

Prueba. Sea b el bloque de $N(D)$ en correspondencia con B. Sea S un $kN(D)$–módulo simple perteneciente a b tal que S es un $k[N(D)/D]$–módulo.

Sea V un indescomponible proyectivo para $N(D)/D$ en correspondencia con S de tal manera que, como S es factor de composición de V, y V es indescomponible, tenemos que V también pertenece a b.

Ahora V es sumando del módulo libre $k[N(D)/D]$ que es isomorfo a $(k_D)^{N(D)}$, luego V es D–proyectivo y V_D es suma directa de kD–módulos triviales. Como D es normal, lo mismo se sigue para $(k_D)^{N(D)}$.

Por el Lema 3.3, V_D tiene un sumando con el mismo vértice que V, luego V ha de tener vértice D.

Sea U el kG–módulo indescomponible en correspondencia de Green con V, entonces U también tiene vértice D y U pertenece a B por el corolario 3.4.□

Corolario 3.6 (Caracterización de los bloques con defecto 0)**.** *El bloque B de G es un álgebra simple, si y solo si, tiene defecto* 0*.*

Prueba. Si B tiene defecto 1, entonces todo B–módulo indescomponible tiene vértice 1 en virtud del teorema 3.17, esto significa que todo B–módulo es proyectivo. Por tanto, todos los submódulos de B-módulos son sumandos, y B es semisimple. Como B es indescomponible como álgebra, B ha de ser simple.

Por otro lado, si B es simple todos los B–módulos son proyectivos, y el corolario 3.5 implica que B tiene defecto 1.□

Para probar el tercer gran teorema hemos de introducir un teorema previo que no vamos a demostrar. Para ello hemos de introducir la noción de recubridor.

Sea N un subgrupo normal de G, B un bloque de G, y b un bloque de N. Diremos que B recubre a a b si hay un kG–módulo perteneciente a B cuya restricción a N tenga un sumando perteneciente a b.

Enunciamos el teorema:

Teorema 3.21. *Con la notación establecida:*

(i) *Los bloques de N recubiertos por B forman una única clase de conjugación de bloques de N bajo conjugación en G.*

(ii) *Cada grupo de defecto de b es la intersección de un grupo de defecto de B con N.*

(iii) *Hay un grupo de defecto de B contenido en $Stab(b)$.*

(iv) *Hay un bloque B' de G que recubre b tal que B' tiene grupo de defecto D', y este contiene un conjugado del grupo de defecto de todo bloque de G que recubre a b. Además,*

$$|D' : D' \cap N| = |Stab(b) : N|_p$$

(v) *Si el centralizador de G de un grupo de defecto de b está contenido en N, entonces $B = b^G$ y B el único bloque recubriendo a B.*

A continuación probamos un lema que vamos a necesitar en la demostración.

Lema 3.9. *Existe una correspondencia entre los bloques de G con defecto D y las clases de conjugación en $N_G(D)$ de bloques β de $DC_G(D)$ con defecto D tales que $|Stab(\beta) : DC_G(D)|$ no es divisible por p.*

Prueba. Sea B un bloque de G con grupo de defecto D y b su bloque correspondiente de $N_G(D)$. Sea también un bloque de $DC_G(D)$ recubierto por b.

Como D es normal en $DC_G(D)$, está contenido en un grupo de defecto de β, luego el centralizador de tal grupo de defecto está contenido en $DC_G(D)$. Por tanto, $\beta^{N_G(D)}$ está definido, es igual a b, y b es el único bloque de $N_G(D)$ que recubre a β.

Además β tiene grupo de defecto D: Como $\beta^{N_G(D)} = b$, un grupo de defecto de β que debe contener a D está contenido en el grupo de defecto de b, por el lema 3.8. Como b tiene grupo de defecto D, también tenemos por la parte (iv) del teorema 3.21, que p no divide a $|Stab(\beta) : DC_G(D)|$. Por tanto, existe una correspondencia entre bloques de G con grupos de defecto D, y clases de conjugación de bloques de $DC_G(D)$ con las propiedades requeridas.

Supongamos ahora que β es un bloque de $DC_G(D)$ con grupo de defecto D tal que $|Stab(\beta) : DC_G(D)|$ no es divisible por p. Entonces β^G es el único bloque $N_G/(D)$ que recubre a β, y por los puntos (ii) y (iv) del teorema 3.21, un grupo de defecto de β^G, , que debe contener el grupo de defecto D de β, tiene orden $|Stab(\beta) : DC_G(D)|_p|D|$. Por tanto, b tiene grupo de defecto D, y por el Primer Gran teorema, es el bloque de $N_G(D)$ en correspondencia con el bloque de G con defecto D. □

Ya estamos en condiciones de probar el tercer gran teorema. Este trata sobre el correspondiente de Brauer del bloque principal $b_0(G)$, que es el bloque que contiene al kG–módulo trivial.

Teorema 3.22 (Tercer gran teorema)**.** *Si b es un bloque de un subgrupo H de G, D es el grupo de defecto de b, y $C_G(D) \subset H$ entonces $b^G = b_0(G)$ si y solo si $b = b_0(H)$.*

Prueba. primero suponemos que $b = b_0(H)$ Vamos a aplicar el Segundo Gran Teorema para determinar b^G.

El kG–módulo k pertenece a $b_0(G)$, su restricción k_H pertenece B, Y su vértice es un p–subgrupo de Sylow de H. Pero b tiene los p–subgrupos de Sylow como grupos de defecto,luego el centralizador en G de un vértice de k_H pertenece a H. Por tanto, por el Segundo Gran Teorema, $b^G = b_0(G)$.

Ahora asumimos que $b \neq b_0(H)$, y que $b^G = b_0(G)$. Hemos de llegar a contradicción.

Sea b' el bloque de $N_H(D)$ en correspondencia de Brauer con b, aplicada al grupo H, de tal forma que b' tiene grupo de defecto D y $(b')^H = b$. Como $C(D) \subset H$, $(b')^G$ está definido, y por tanto $(b')^G = b^G = b_0(G)$ por el lema 3.8. Si $b' = b_0(N_H(D))$ entonces $b = b_0(H)$ por lo dicho, luego $b' \neq b_0(N_H(D))$.

Sea β un bloque de $DC_H(D)$ recubierto por b', luego β tiene grupo de defecto D ,y $\beta^{N_H(D)} = b'$. Entonces $\beta \neq b_0(DC(D))$.

Además, β^G está definido y $\beta^G = (b')^G = b_0(G)$. Por tanto, tenemos que D es un p–subgrupo de de G, β es un bloque de $DC(D)$ con defecto D, $\beta \neq b_0(DC(D))$, y $\beta^G = b_0(G)$.

Procedemos por inducción sobre el orden de D para llegar a contradicción.

Supongamos que D es un p–subgrupo de Sylow de G. En particular, $b_0(G) = \beta^G = (\beta^{N(D)})^G$. $b_0(N(D))^G = b_0(G)$, luego el Primer Gran Teorema implica que $\beta^{N(D)} = b_0(N(D))$. Pero por el teorema 3.21, $\beta^{N(D)}$ es el único bloque de $N(D)$ que recubre a β, sin embargo $b_0(N(D))$ solo recubre a $b_0(DC(D))$, luego $\beta_0 = b_0(DC(D))$, lo cual es una contradicción.

Por tanto, podemos asumir que si E es un p–subgrupo de G que contiene propiamente a D, γ un bloque de $EC(E)$ con defecto E, y $\gamma^G = b_0(G)$, entonces $\gamma = b_0(EC(E))$.

Por el lema 3.8, $\beta^{N(D)}$ tiene grupo de defecto E que contiene a D. Afirmamos que este lo contiene propiamente: Si $D = E$, entonces $(\beta N(D))^G = \beta^G = b_0(G)$, entonces D es un p–subgrupo de Sylow por el Primer Gran Teorema. Por el lema 3.9 aplicado al grupo $N(D)$, tenemos que hay un bloque γ de $EC_{N(D)(E)} = EC(E)$ con grupo de defecto E y $\gamma^{N(D)} = \beta^{N(D)}$. Por tanto, $\gamma^G = (\gamma N(D))^G = (\beta^{N(D)})^G = \beta^G = b_0(G)$. Luego, por la hipótesis de inducción, $\gamma = b_0(EC(E))$. Finalmente , $\gamma^{N(D)} = b_0(N(D))$, pero $\beta^N(D) = \gamma^{N(D)}$ lo cual nos da una contradicción. $\square$

Bibliografía

[Alp86] J.L. Alperin. *Local representation theory*. Cambridge University Press, 1986.

[Bra35] R. Brauer. Über die darstellung von gruppen in galoisschen feldern. *Actualités Sci. Indust.*, (195):15pp, 1935.

[Bra39] R. Brauer. On the representation of groups of finite order. *Proc. Nat. Acad. Sci. USA.*, 25:290–295, 1939.

[Bra41a] R. Brauer. Investigations on group characters. *Ann. of Math*, 42:936–958, 1941.

[Bra41b] R. Brauer. On the cartan invariants of groups of finite order. *Ann. of Math.*, 42:53–61, 1941.

[Bra42a] R. Brauer. On groups whose order contains a prime number to the first power i. *Amer. J. Math*, 64(1):401–420, 1942.

[Bra42b] R. Brauer. On groups whose order contains a prime number to the first power ii. *Amer. J. Math*, 64(1):421–440, 1942.

[Bra44] R. Brauer. On the arithmetic in a group ring. *Proc. Nat. Acad. Sci. USA*, 30:109–114, 1944.

[Bra46a] R. Brauer. On blocks of characters of groups of finite order, i. *Proc. Nat. Acad. Sci. USA*, 32:182–186, 1946.

[Bra46b] R. Brauer. On blocks of characters of groups of finite order, ii. *Proc. Nat. Acad. Sci. USA*, 32:215–219, 1946.

[Bra53] R. Brauer. A characterization of the characters of groups of finite order. *Ann. of Math.*, 57:357–377, 1953.

[Bra56] R. Brauer. Zur darstellungstheorie der gruppen endlicher ordnung. *Math. Z.*, 63:406–444, 1956.

[Bra59] R. Brauer. Zur darstellungstheorie der gruppen endlicher ordnung ii. *Math. Z.*, 72:25–46, 1959.

[Bra71a] R. Brauer. Some applications of the theory of blocks of characters of finite groups i. *J. Algebra*, 1:152–167, 1971.

[Bra71b] R. Brauer. Some applications of the theory of blocks of characters of finite groups iv. *J. Algebra*, 17:489–521, 1971.

[Bur04] William Burnside. On the reduction of a group of homogeneous linear substitutions of finite order. *Acta Mathematica*, 28:p369, 1904.

[CC81] I. Reiner C.W. Curtis. *Methods of representation theory with applications to finite groups and orders*, volumen 1. John Wiley and Sons, 1981.

[Ded63] R. Dedekind. *Vorlesungen über Zahlentheorie*. 1863.

[Dic03] Leonard E. Dickson. On the group defined for any given field by the multiplication table of any given finite group. *Transactions of the American Mathematical Society*, 3(3):285–301, 1903.

[Dic07a] Leonard E. Dickson. Modular theory of group characters. *Bulletin of the American Mathematical Society*, 13:477–488, 1907.

[Dic07b] Leonard E. Dickson. Modular theory of group matrices. *Transactions of the American Mathematical Society*, 8(3):389–398, 1907.

[Fei79] W. Feit. Richard d. brauer. *Bulletin of the AMS*, 1(1), 1979.

[Fro96a] Ferdinand G. Frobenius. Über die primfactoren der gruppendeterminante. *Sitzungsberichte de Königlich Preussischen Akademie der Wissenchaften zu Berlin*, páginas 1343–1382, 1896.

[Fro96b] Ferdinand G. Frobenius. Über gruppencharaktere. *Sitzungsberichte de Königlich Preussischen Akademie der Wissenchaften zu Berlin*, páginas 985–1021, 1896.

[Fro97] Ferdinand G. Frobenius. Über die darstellung der endlichen gruppen durch lineare substitutionen. *Sitzungsberichte de Königlich Preussischen Akademie der Wissenchaften zu Berlin*, páginas 994–1015, 1897.

[Fro99] Ferdinand G. Frobenius. Über die darstellung der endlichen gruppen durch lineare substitutionen ii. *Sitzungsberichte de Königlich Preussischen Akademie der Wissenchaften zu Berlin*, páginas 482–500, 1899.

[Fro03] Ferdinand G. Frobenius. Über die primfactoren der gruppendeterminante ii. *Sitzungsberichte de Königlich Preussischen Akademie der Wissenchaften zu Berlin*, páginas 401–409, 1903.

[Gau63] K. F. Gauss. *Disquisitiones Arithmeticae*. 1863.

[Gol80] D. M. Goldschmidt. *Lectures on character theory*. Publish or Perish, 1980.

[Gre59] J. A. Green. On the indecomposable representations of a finite group. *Math. Z.*, 70:430–445, 1959.

[Gre62] J. A. Green. Blocks of modular representations. *Math Z.*, 79:100–115, 1962.

[Gre72] J.A. Green. Relative module categories for finite groups. *J. Pure Appl. Algebra*, 2:371–393, 1972.

[Haw71] T. Hawkins. The origins of the theory of group characters. *Archive for History of Exact Sciences*, 7(2):142–170, 1971.

[Hig54] D.G. Higman. Modules with a group of operators. *Duke Math. J.*, 21:369–376, 1954.

[Noe29] Emmy Noether. Hyperkomplexe größen und darstellungstheorie. *Matematische Zeitschrift*, 30:641–692, 1929.

[Osi55] Osima. Notes on blocks of group characters. *Math J. Okuyama Univ.*, 4:175–188, 1955.

[RB] C. Nesbitt R. Brauer. On the modular characters of groups. *Ann. of Math.*, 42.

[RB37] C. Nesbitt R. Brauer. On the modular representations of groups of finite order i. *Univ. Toronto Studies*, (4):21pp, 1937.

[Ros61] A. Rosenberg. Blocks and centres of group algebras. *Math. Z.*, 76:209–216, 1961.

[Sch05] Issai Schur. Neue begründung der theorie der gruppencharaktere. *Sitzungsberichte de Königlich Preussischen Akademie der Wissenchaften zu Berlin*, páginas 406–432, 1905.

[Ser77] J.P. Serre. *Linear representations of finite groups*. Springer-Verlag, New York Inc., 1977.

[Swa60] R. Swan. Induced representations and projective modules. *Ann. of Math.*, 71:552–578, 1960.

[Swa63] R. Swan. The grothendieck group of a finite group. *Topology*, páginas 85–110, 1963.

[Web95] H. Weber. *Lehrbuch von Algebra*. 1895.