Carlos Ivorra Castillo

REPRESENTACIONES DE GRUPOS FINITOS

Necesitamos unas supermatemáticas en las que las operaciones sean tan desconocidas como las cantidades sobre las que operan, y un supermatemático que no sepa qué está haciendo cuando realiza esas operaciones. Esas supermatemáticas son la teoría de grupos.

Sir Arthur Stanley Eddington

Índice General

Prefacio

Este libro es el resultado de extender lo que originalmente era un capítulo de preliminares para definir el conductor de una curva elíptica en la parte de aplicaciones de mi libro de *Superficies aritméticas.* El lector interesado específicamente en este objetivo puede leer las secciones 1.1 y 1.2 y el capítulo II (saltándose, si lo desea, las secciones 2.3 y 2.7) y desde ahí pasar directamente al apéndice A, del que podrá seguir las secciones A.1 y A.2, con lo cual alcanzará los requisitos necesarios para entender el estudio del conductor de una curva elíptica. Ahora bien, si quiere entender realmente la teoría que hay de fondo en el uso de los caracteres de Artin y Swan construidos en A.2 deberá leer también las secciones A.3 y A.4, para lo cual necesitará estudiarse casi la totalidad del presente libro.

El lector interesado en la teoría de representaciones propiamente dicha debe observar que hemos duplicado la exposición de la teoría en el caso de las representaciones de grupos finitos sobre el cuerpo de los números complejos. En el capítulo II presentamos la teoría mediante razonamientos "rápidos" y "elementales", en el sentido de que evitan el uso de la mayor parte del aparato algebraico subyacente a la teoría de representaciones, y en el capítulo III desarrollamos dicho aparato algebraico sin apoyarnos en el capítulo precedente, con lo que obtenemos pruebas alternativas de los mismos resultados, sólo que en un contexto mucho más general. Lo hemos hecho así para permitir el acceso rápido a las primeras secciones del apéndice A que hemos indicado antes y también porque, de este modo, el lector interesado en la teoría de caracteres propiamente dicha tiene la oportunidad de apreciar su interés y utilidad antes de adentrarse en sus aspectos más técnicos. Conviene tener presente a este respecto que el capítulo II no requiere las secciones 1.3 y 1.4, por lo que su lectura puede posponerse. Como complemento al capítulo II, el lector puede estudiar también la construcción de las tablas de caracteres ordinarios de los grupos Σ_4 y A_5 expuestas respectivamente en las secciones 4.8 y B.3.

Por otra parte, el lector que desee evitar exposición duplicada puede optar por pasar del capítulo I al capítulo III y después volver sobre el capítulo II para ver los ejemplos, aplicaciones, y algunos resultados adicionales, saltándose las pruebas de los hechos ya probados en el capítulo III. En cualquier caso, quien siga este camino deberá volver al capítulo II para estudiar —como mínimo— el teorema de Brauer sobre caracteres inducidos, que será necesario posteriormente

en numerosas ocasiones.

El capítulo IV es una introducción a la teoría de representaciones modulares. El lector que no esté interesado en esta parte puede saltarse la sección 1.4 y el final de la sección 1.3 (desde el apartado correspondiente a módulos proyectivos). De hecho, puede saltarse toda alusión a módulos proyectivos que encuentre en los capítulos precedentes.

Dada la naturaleza técnica de la teoría que nos ocupa, al lector interesado en formarse una primera idea de su naturaleza y contenido lo remitimos a la sección 1.1, en la que se exponen los conceptos e ideas básicas.

En cuanto a los requisitos para seguir este libro, no son muchos. Para los tres primeros capítulos no se requiere más que el álgebra básica (algo de teoría de grupos, de anillos, de extensiones de cuerpos y álgebra lineal, a un nivel no superior al de mi libro de *Álgebra,* salvo que también se requiere el conocimiento del producto tensorial de módulos, que puede estudiarse en mi libro de *Teoría de cuerpos de clases* o en el de *Topología algebraica.*) En la sección 1.2 se recogen (con pruebas) los requisitos sobre teoría de grupos que no aparecen en mi libro de *Álgebra* y la sección 1.3 incluye (también con pruebas) algunos preliminares de teoría de anillos, muchos de los cuales son generalizaciones inmediatas al caso de anillos no conmutativos de resultados expuestos en mi libro de *Álgebra* o en el de *Álgebra conmutativa.* El capítulo IV requiere, además de algunos hechos adicionales de teoría de anillos recogidos en las secciones 1.3 y 1.4, un mínimo conocimiento de la teoría de cuerpos locales, expuesta, por ejemplo, en mi libro de *Geometría algebraica.*

Por último, el apéndice A requiere un conocimiento mucho más profundo de la aritmética de los cuerpos métricos discretos completos, especialmente de la teoría de la ramificación. La sección A.1 contiene un resumen de los principales hechos necesarios, en muchos casos enunciados sin prueba, pero todos los resultados citados sin prueba (tanto en esta sección como en las posteriores) están demostrados en mi libro de *Teoría de cuerpos de clases,* y se indican las referencias oportunas.

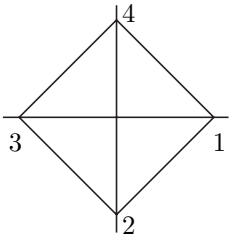
Capítulo I

Introducción y preliminares

Una cosa es tener definido un grupo (por ejemplo, un grupo de unidades de un anillo, un grupo de Galois de una extensión de cuerpos, etc.) y otra muy distinta tener una representación clara de su estructura. A la hora de "comprender un grupo", resulta útil encontrar un grupo isomorfo lo más "concreto" posible. Un recurso clásico es tratar de expresar un grupo dado como grupo de permutaciones:

Ejemplo Si definimos el grupo diédrico de orden 8 como el grupo D_4 de las simetrías de un cuadrado, tendremos una representación más clara y manejable —que podemos incluso tomar como definición— si observamos que es isomorfo al subgrupo siguiente del grupo Σ_4 de las permutaciones de 4 elementos (que podemos identificar con los cuatro vértices del cuadrado):

$$D_4 = \{1, (1,2,3,4), (1,3)(2,4), (4,3,2,1), (1,3), (2,4), (1,2)(3,4), (1,4)(2,3)\}.$$



Las tres primeras (sin contar a 1) se corresponden con los giros de 90°, 180° y 270°, las dos siguientes son las simetrías respecto de las diagonales y las dos últimas son las simetrías respecto de las mediatrices de los lados. Por ejemplo, a partir de esta representación de D_4 es fácil ver que, si llamamos $\sigma = (1,2,3,4)$ y $\tau = (1,3)$, entonces

$$D_4 = \{1, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\} = \langle \sigma, \tau \rangle .$$

Además, el producto en D_4 puede calcularse a partir de estas expresiones sin más que tener en cuenta que $\sigma^4 = \tau^2 = 1$ y que $\tau\sigma = \sigma^{-1}\tau$. ∎

Sin embargo, la interpretación de D_4 como el grupo de las simetrías de un cuadrado nos proporciona otra representación concreta del mismo, como un grupo de matrices. En efecto, podemos identificar cada simetría del cuadrado con una aplicación lineal en $\mathbb{R}^2$ y ésta a su vez con su matriz en la base canónica:

Ejemplo El giro de 90° en $\mathbb{R}^2$ y la simetría respecto al eje Y son, respectivamente, las aplicaciones lineales determinadas por las matrices

$$\sigma = \begin{pmatrix} \cos\frac{2\pi}{4} & \operatorname{sen}\frac{2\pi}{4} \\ -\operatorname{sen}\frac{2\pi}{4} & \cos\frac{2\pi}{4} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \tau = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Se comprueba fácilmente que las matrices $1, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau$ son distintas dos a dos, así como que satisfacen las relaciones $\sigma^4 = \tau^2 = 1$, $\tau\sigma = \sigma^{-1}\tau$, de donde se sigue que las ocho matrices son el subgrupo generado por σ y τ, y que sus elementos son todas las simetrías del cuadrado (la identidad, los tres giros y las cuatro simetrías propiamente dichas). Esto nos da una representación (o una definición) alternativa de D_4 como grupo de matrices (como el subgrupo generado por las matrices σ y τ).

Una forma sencilla de comprobar que D_4 como grupo de permutaciones es isomorfo a D_4 como grupo de matrices es observar que si identificamos el conjunto $\{1,2,3,4\}$ con los puntos de $X = \{(1,0),(0,-1),(-1,0),(0,1)\}$ (de acuerdo con la numeración de la figura), entonces, las permutaciones σ y τ son las restricciones a X de los automorfismos de $\mathbb{R}^2$ determinados por σ y τ, por lo que, en general, si identificamos cada matriz de D_4 con el automorfismo que determina en $\mathbb{R}^2$ (respecto de la base canónica), un isomorfismo entre D_4 como grupo de automorfismos y D_4 como grupo de permutaciones viene dado por la restricción $\phi \mapsto \phi|_X$. ∎

Ejemplo Si cambiamos $n = 4$ por $n = 3$ en el ejemplo anterior, obtenemos una representación matricial del grupo de simetrías de un triángulo, que tiene seis elementos y es, por consiguiente, isomorfo al grupo Σ_3 de permutaciones de tres elementos. Los generadores son

$$\sigma = \begin{pmatrix} \cos\frac{2\pi}{3} & \operatorname{sen}\frac{2\pi}{3} \\ -\operatorname{sen}\frac{2\pi}{3} & \cos\frac{2\pi}{3} \end{pmatrix} = \begin{pmatrix} -1/2 & \sqrt{3}/2 \\ -\sqrt{3}/2 & -1/2 \end{pmatrix}, \quad \tau = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Se comprueba fácilmente que las seis matrices $1, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau$ son distintas dos a dos, así como que $\sigma^3 = \tau^2 = 1$, $\tau\sigma = \sigma^{-1}\tau$, de donde se sigue que el grupo $\langle\sigma,\tau\rangle$ tiene orden 6. ∎

A primera vista, podría dudarse de si es más útil representar un grupo finito como grupo de permutaciones o como grupo de matrices, pero sucede que las representaciones matriciales dan lugar a una potente herramienta cuyas posibilidades superan con creces a las que ofrecen las representaciones por grupos de permutaciones.

1.1 Representaciones lineales de grupos

Aunque los grupos D_4 y Σ_3 que hemos considerado en los ejemplos precedentes tenían una interpretación geométrica —como grupos de simetrías— que nos llevaba de forma natural a una representación matricial, podemos plantearnos

la posibilidad de representar cualquier grupo abstracto (aunque aquí sólo consideraremos grupos finitos) en forma de grupo de matrices. Esta idea se plasma en la definición siguiente:

Definición 1.1 Una *representación matricial* de *grado* $n \geq 1$ de un grupo finito G sobre un anillo conmutativo[1] A es un homomorfismo de grupos

$$\rho : G \longrightarrow \mathrm{LG}(n, A),$$

donde el grupo *lineal general* $\mathrm{LG}(n, A)$ es el grupo de las matrices inversibles de orden $n \times n$ con coeficientes en A. Diremos que A es el *anillo de coeficientes* de la representación.

Notemos que la definición no exige que ρ sea inyectivo. (En tal caso se dice que la representación es *fiel*.) En general, si N es el núcleo de ρ, tenemos que ρ induce una representación fiel del grupo cociente G/N.

En los ejemplos precedentes hemos calculado una representación fiel de grado 2 del grupo D_4 sobre $\mathbb{Q}$ y otra de Σ_3 sobre $\mathbb{R}$.

A la hora de estudiar las representaciones matriciales, es útil tener en cuenta que las matrices pueden identificarse con automorfismos de espacios vectoriales. Ello nos lleva a la definición siguiente:

Definición 1.2 Una *representación lineal* de *grado* $n \geq 1$ de un grupo finito G sobre un *anillo de coeficientes* (conmutativo) A es un homomorfismo de grupos $\rho : G \longrightarrow \mathrm{Aut}_A(V)$, donde V es un A-módulo libre de rango n.

Si $\rho : G \longrightarrow \mathrm{Aut}(V)$ es una representación lineal de un grupo G, escribiremos a menudo $v\sigma = \rho(\sigma)(v)$. En estos términos, el hecho de que $\rho(\sigma)$ sea un automorfismo de V y que ρ sea un homomorfismo de grupos equivale a las relaciones

$$(v + w)\sigma = v\sigma + w\sigma, \qquad (\alpha v)\sigma = \alpha(v\sigma), \qquad (v\sigma)\tau = v(\sigma\tau),$$

donde v, $w \in V$, σ, $\tau \in G$, $\alpha \in K$.

La relación entre las representaciones matriciales y las representaciones lineales es evidente: toda representación matricial ρ de grado n sobre un anillo A determina una representación lineal sobre cualquier A-módulo libre V de rango n respecto a una base B de V prefijada, sin más que asignar a cada $\sigma \in G$ el automorfismo de V que tiene matriz $\rho(\sigma)$ en la base B.

Recíprocamente, toda representación lineal ρ en un A-módulo libre V de rango n determina una representación matricial de grado n para cada base B de V, sin más que asignar a cada $\sigma \in G$ la matriz de $\rho(\sigma)$ en la base B.

Ahora damos una definición de isomorfismo de representaciones que vuelve irrelevante la arbitrariedad en la elección de las bases:

[1] Todos los anillos que vamos a considerar serán unitarios, pero no serán conmutativos salvo que lo especifiquemos explícitamente.

Definición 1.3 Diremos que dos representaciones lineales $\rho_i : G \longrightarrow \mathrm{Aut}(V_i)$, para $i = 1, 2$ (sobre un mismo anillo de coeficientes A) son *isomorfas* si existe un isomorfismo de A-módulos $\phi : V_1 \longrightarrow V_2$ que cumpla $\rho_2 = \rho_1 \circ \bar{\phi}$, donde $\bar{\phi} : \mathrm{Aut}(V_1) \longrightarrow \mathrm{Aut}(V_2)$ es el isomorfismo de grupos dado por $\bar{\phi}(f) = \phi^{-1} f \phi$. Observemos que la condición $\rho_2 = \rho_1 \circ \bar{\phi}$ es equivalente a que

$$\phi(v\sigma) = \phi(v)\sigma$$

para todo $v \in V_1$ y todo $\sigma \in G$.

Dos representaciones matriciales $\rho_i : G \longrightarrow \mathrm{LG}(n, A)$ son *isomorfas* si existe una matriz $M \in \mathrm{LG}(n, A)$ tal que, para todo $\sigma \in G$, se cumple la relación $\rho_2(\sigma) = M^{-1}\rho_1(\sigma)M$.

Es inmediato que dos representaciones matriciales isomorfas dan lugar a representaciones lineales isomorfas independientemente de los módulos y las bases elegidas, así como que dos representaciones lineales isomorfas dan lugar a representaciones matriciales isomorfas independientemente de las bases elegidas.

A continuación vamos a mostrar una tercera estructura equivalente a la de representación matricial y a la de representación lineal. Se basa en la definición siguiente:

Definición 1.4 Si G es un grupo finito y A es un anillo conmutativo, llamaremos $A[G]$ al A-módulo libre de base G, en el que consideraremos la estructura de A-álgebra[2] determinada por el producto siguiente:

$$(\sum_{\sigma\in G} \alpha_\sigma \sigma)(\sum_{\tau\in G} \beta_\tau \tau) = \sum_{\sigma,\tau\in G} \alpha_\sigma \beta_\tau \sigma\tau.$$

Es evidente que el producto así definido es bilineal y que extiende al producto de G. Teniendo esto en cuenta, se comprueba sin dificultad que cumple todas las propiedades necesarias para que $A[G]$ sea ciertamente una A-álgebra, cuya unidad es el elemento neutro de G.

Si $\rho : G \longrightarrow \mathrm{Aut}(V)$ es una representación lineal, podemos dotar a V de estructura de $A[G]$-módulo (por la derecha) mediante el producto dado por

$$v(\sum_{\sigma\in G} \alpha_\sigma \sigma) = \sum_{\sigma\in G} \alpha_\sigma \rho(\sigma)(v).$$

Notemos que el producto $v\sigma$ según esta definición coincide con el producto $v\sigma = \rho(\sigma)(v)$ que habíamos definido. Recíprocamente, si V es un $A[G]$-módulo que como A-módulo es libre de rango finito n, podemos definir una representación $\rho : G \longrightarrow \mathrm{Aut}(V)$ mediante $\rho(\sigma)(v) = v\sigma$.

De este modo, tenemos una correspondencia entre las representaciones lineales de grado n de G y los $A[G]$-módulos (por la derecha) que son A-módulos

[2]En álgebra conmutativa, una A-álgebra B se define como un anillo (conmutativo) B con una estructura de A-módulo compatible, en el sentido de que $a(b_1b_2) = (ab_1)b_2$. Si no exigimos que B sea conmutativo, hemos de añadir que $a(b_1b_2) = (ab_1)b_2 = b_1(ab_2)$. En particular, si $A \subset B$, tenemos que los elementos de A conmutan con todos los de B.

libres de rango n. Es inmediato que dos representaciones son isomorfas si y sólo si los $A[G]$-módulos correspondientes son isomorfos. Más concretamente, un isomorfismo $f : V_1 \longrightarrow V_2$ entre dos A-módulos libres es un isomorfismo entre dos representaciones lineales de G si y sólo si es un isomorfismo entre los $A[G]$-módulos asociados.

Con esto tenemos ya determinado el objeto de estudio de este libro: vamos a ocuparnos de las representaciones lineales de grupos finitos, las cuales pueden estudiarse a través de las representaciones lineales propiamente dichas, a través de las representaciones matriciales o a través de los $A[G]$-módulos asociados.

Observemos que, aunque A sea un anillo conmutativo, el anillo $A[G]$ no lo es salvo que el grupo G sea abeliano (una hipótesis que no podemos permitirnos), y ésta es la razón por la que hemos advertido que no supondremos que los anillos con los que trabajemos sean conmutativos. Sólo vamos a considerar representaciones sobre anillos de coeficientes conmutativos, pero los $A[G]$-módulos asociados serán módulos sobre anillos no necesariamente conmutativos.

En realidad nos va a interesar principalmente el caso en que el anillo de coeficientes A es un cuerpo K, pero hemos dado las definiciones para anillos conmutativos arbitrarios porque este caso general nos permitirá más adelante relacionar las representaciones sobre cuerpos de característica 0 con las representaciones sobre cuerpos de característica prima.

Conviene precisar cuál es el centro de $A[G]$. En general el *centro* de un anillo A se define como el subanillo

$$Z(A) = \{a \in A \mid ab = ba \text{ para todo } b \in A\}.$$

Recordamos que dos elementos $\tau_1, \tau_2 \in G$ se dicen *conjugados* si existe un $\sigma \in G$ tal que $\tau_2 = \sigma^{-1}\tau_1\sigma$. La conjugación es una relación de equivalencia en G. Representaremos por $\mathrm{cl}_G(\tau)$ a la clase de conjugación de τ en G y por $\mathrm{cl}(G)$ al conjunto de todas las clases de conjugación de G.

Si A es un anillo conmutativo, es obvio que un elemento

$$x = \sum_{\sigma\in G} \alpha_\sigma \sigma \in A[G]$$

está en el centro de $A[G]$ si y sólo si conmuta con todos los elementos $\tau \in G$, es decir, si cumple que $\tau x = x\tau$ o, equivalentemente, $\tau x \tau^{-1} = x$. Explícitamente:

$$\sum_{\sigma\in G} \alpha_\sigma \tau\sigma\tau^{-1} = \sum_{\sigma\in G} \alpha_\sigma \sigma.$$

Teniendo en cuenta que $\sigma \mapsto \tau\sigma\tau^{-1}$ es biyectiva con inversa $\sigma \mapsto \tau^{-1}\sigma\tau$, esto equivale a que

$$\sum_{\sigma\in G} \alpha_{\tau^{-1}\sigma\tau} \sigma = \sum_{\sigma\in G} \alpha_\sigma \sigma,$$

lo cual equivale a que la función $\sigma \mapsto \alpha_\sigma$ sea constante sobre las clases de conjugación de G. Por consiguiente:

Teorema 1.5 *Si G es un grupo finito y A un anillo conmutativo el centro de $A[G]$ está formado por los elementos de la forma*

$$\sum_{c\in \mathrm{cl}(G)} \alpha_c e_c, \qquad \alpha_c \in A,$$

donde, para cada clase de conjugación $c \in \mathrm{cl}(G)$, llamamos

$$e_c = \sum_{\sigma\in c} \sigma.$$

Equivalentemente, $Z(A[G])$ es el submódulo de $A[G]$ que tiene por base los elementos e_c.

Observemos ahora que si A es un subanillo de un anillo conmutativo B, entonces $\mathrm{LG}(n, A)$ es un subgrupo de $\mathrm{LG}(n, B)$, por lo que toda representación matricial de un grupo G sobre A puede considerarse también como representación sobre B. Esto tiene un equivalente en términos de representaciones lineales:

Definición 1.6 Sea A un subanillo de un anillo conmutativo B, sea V un A-módulo libre de rango finito y sea $\rho : G \longrightarrow \mathrm{Aut}(V)$ una representación lineal de un grupo finito G. El producto tensorial[3] $V_B = B \otimes_A V$ es un B-módulo libre del mismo rango que V, y podemos considerar el monomorfismo de grupos $\mathrm{Aut}(V) \longrightarrow \mathrm{Aut}(V_B)$ dado por $\alpha \mapsto 1 \otimes \alpha$, donde $1 : B \longrightarrow B$ es la identidad. Definimos la *extensión de coeficientes* $\rho^B : G \longrightarrow \mathrm{Aut}(V_B)$ como la composición de ρ con este monomorfismo, que claramente es una representación lineal de G sobre B del mismo grado que ρ.

Concretamente, si $v_1, \ldots, v_n$ es una A-base de V, entonces $1 \otimes v_1, \ldots, 1 \otimes v_n$ es una B-base de V_B, y la representación matricial de ρ en la primera base es la misma que la de ρ^B en la segunda.

En términos de módulos tenemos un isomorfismo natural $B[G] \cong B \otimes_A A[G]$, y ρ^B está asociada a la estructura natural de $B[G]$-módulo en V_B dada por

$$(b \otimes v)(b' \otimes \sigma) = (bb') \otimes v\sigma.$$

Recíprocamente, si una representación de G con coeficientes en B es de la forma ρ^B, para cierta representación ρ con coeficientes en A, se dice que es *realizable* sobre A. Equivalentemente, una representación lineal es realizable sobre un anillo A si está inducida por una representación matricial con coeficientes en A.

Veamos un par de ejemplos generales de representaciones:

Definición 1.7 Si G es un grupo finito, la *representación trivial* de grado n de G sobre el anillo conmutativo A es la representación matricial $\rho : G \longrightarrow \mathrm{LG}(n, A)$ dada por $\rho(\sigma) = I_n$ para todo $\sigma \in G$. Sus representaciones lineales asociadas son las representaciones en A-módulos libres V de rango n que cumplen $v\sigma = v$ para todo $v \in V$ y todo $\sigma \in G$.

[3]Para las propiedades básicas del producto tensorial de módulos (sobre anillos no necesariamente conmutativos) véase la sección 14.1 de mi *Teoría de cuerpos de clases,* que es independiente de los capítulos anteriores.

Definición 1.8 Si G es un grupo finito, llamaremos *representación regular* de G a la representación asociada a la estructura de $A[G]$-módulo de $A[G]$. Claramente es fiel y su grado es el orden de G.

Ahora veamos cómo podemos construir nuevas representaciones a partir de unas dadas:

Definición 1.9 Si $\rho_i : G \longrightarrow \mathrm{Aut}(V_i)$, para $i = 1, 2$, son dos representaciones lineales de G, definimos su *suma directa* como la representación

$$\rho_1 \oplus \rho_2 : G \longrightarrow \mathrm{Aut}(V_1 \oplus V_2)$$

asociada a la suma directa de los $A[G]$-módulos $V_1 \oplus V_2$. Obviamente, se trata de la representación dada por $(v_1 + v_2)\sigma = v_1\sigma + v_2\sigma$, donde $v_1\sigma$ se calcula con ρ_1 y $v_2\sigma$ con ρ_2.

Es claro que podemos definir igualmente la suma directa de cualquier número finito de representaciones de G. El grado de la suma directa es la suma de los grados.

Definición 1.10 Si $\rho_i : G \longrightarrow \mathrm{Aut}(V_i)$, para $i = 1, 2$, son dos representaciones lineales de G, definimos su *producto tensorial* como la representación

$$\rho_1 \otimes \rho_2 : G \longrightarrow \mathrm{Aut}(V_1 \otimes_A V_2)$$

asociada al A-módulo libre $V_1 \otimes_A V_2$ con la estructura de $A[G]$-módulo dada por

$$(v_1 \otimes v_2)\sigma = (v_1\sigma) \otimes (v_2\sigma).$$

El grado del producto tensorial es el producto de los grados.

A partir de aquí nos centraremos en las representaciones lineales sobre cuerpos. Observemos que, si K es un cuerpo, todo $K[G]$-módulo V es libre sobre K, aunque, para que determine una representación de G sobre K, hemos de exigir que su dimensión sobre K sea finita.

A la hora de estudiar las representaciones lineales de un grupo finito, es fundamental estudiar la posibilidad de expresar una representación dada como suma de otras más sencillas. Tales sumandos han de ser subrepresentaciones, en el sentido siguiente:

Definición 1.11 Si $\rho : G \longrightarrow \mathrm{Aut}(V)$ es una representación de G con coeficientes en un cuerpo K, llamaremos *subrepresentaciones* de ρ a las representaciones $G \longrightarrow \mathrm{Aut}(W)$ asociadas a los $K[G]$-submódulos W de V.

Notemos que, para que un subespacio vectorial $W \subset V$ sea un $K[G]$-submódulo, es suficiente con que $W\sigma \subset W$, para todo $\sigma \in G$.

Según decíamos, si $\rho = \rho_1 \oplus \rho_2 : G \longrightarrow \mathrm{Aut}(V_1 \oplus V_2)$ es la suma de dos representaciones ρ_1 y ρ_2, entonces éstas son subrepresentaciones de ρ, pues están asociadas a V_1 y V_2, que son $K[G]$-submódulos de $V_1 \oplus V_2$.

Veamos ahora el primer resultado no trivial sobre representaciones lineales:

Teorema 1.12 *Sea $\rho : G \longrightarrow \mathrm{Aut}(V)$ una representación de un grupo finito G sobre un cuerpo K cuya característica no divida al orden de G, y sea W un $K[G]$-submódulo de V. Entonces existe otro $K[G]$-submódulo W^0 tal que $V = W \oplus W^0$.*

Demostración: Sea W' cualquier subespacio vectorial de V que cumpla $V = W \oplus W'$, sea $p : V \longrightarrow W$ la proyección y sea $p^0 : V \longrightarrow W$ la aplicación lineal dada por[4]

$$p^0(v) = \frac{1}{|G|} \sum_{\sigma \in G} p(v\sigma^{-1})\sigma.$$

Si $w \in W$, entonces $p(w\sigma^{-1})\sigma = (w\sigma^{-1})\sigma = w$, luego $p^0(w) = w$. Si llamamos W^0 al núcleo de p^0, es claro que $V = W \oplus W^0$. Por otra parte,

$$p^0(v\tau^{-1})\tau = \frac{1}{|G|} \sum_{\sigma \in G} p(v\tau^{-1}\sigma^{-1})\sigma\tau = p^0(v).$$

Esto implica que W^0 es un $K[G]$-submódulo, pues si $p^0(v) = 0$, entonces

$$p^0(v\tau)\tau^{-1} = p^0(v) = 0,$$

luego $p^0(v\tau) = 0$ y, por lo tanto, $v\tau \in W^0$. ∎

Definición 1.13 Diremos que una representación $\rho : G \longrightarrow \mathrm{Aut}(V)$ es *irreducible* si V no tiene más $K[G]$-submódulos que los triviales: 0 y V.

Por el teorema anterior, si una representación no es irreducible, se descompone en suma directa de dos subrepresentaciones no triviales. Es claro entonces que toda representación puede descomponerse en suma directa de representaciones irreducibles $V = W_1 \oplus \cdots \oplus W_n$. La descomposición no es única, en el sentido de que podemos elegir los submódulos W_i de formas distintas, pero más adelante veremos que la descomposición es única salvo isomorfismo, en el sentido de que dos descomposiciones cualesquiera de un mismo $K[G]$-módulo V han de tener el mismo número de sumandos y que, debidamente ordenados, cada sumando de una descomposición es isomorfo al sumando correspondiente de la otra.

Ahora bien, es crucial tener presente que todo esto sólo es cierto bajo la hipótesis del teorema anterior, a saber, que $\mathrm{car}\, K \nmid |G|$. (En particular, esto sucede si $\mathrm{car}\, K = 0$.) Veamos un ejemplo de lo que puede suceder en caso contrario:

Teorema 1.14 *Sea p un número primo, sea K un cuerpo de característica p y sea G un grupo de orden potencia de p. Entonces todo $K[G]$-módulo no nulo contiene un submódulo no nulo trivial (es decir, tal que G deja invariantes a todos sus elementos). Por consiguiente, todo $K[G]$-módulo irreducible es isomorfo a K con la estructura de $K[G]$-módulo trivial.*

[4]Al dividir entre $|G|$ estamos usando la hipótesis sobre la característica de K.

DEMOSTRACIÓN: Sea V un $K[G]$-módulo no nulo y sea $k = \mathbb{Z}/p\mathbb{Z} \subset K$. Podemos considerar a V como k-espacio vectorial (tal vez de dimensión infinita). Tomemos $v_0 \in V$ no nulo y sea V_0 el k-espacio vectorial (de dimensión finita) generado por $\{v_0\sigma \mid \sigma \in G\}$.

Como V_0 se descompone en suma directa de copias de k, tenemos que su cardinal es potencia de p. Claramente, si $v \in V_0$, se cumple que $v\sigma \in V_0$, y esto determina una acción[5] de G sobre V_0, respecto a la cual, la órbita de 0 se reduce a $\{0\}$. No puede ser la única órbita con un solo elemento, ya que, en tal caso, todas las demás órbitas tendrían[6] orden múltiplo de p, y concluiríamos que $|V_0| \equiv 1$ (mód p), lo cual es imposible. Así pues, existe un $v \in V_0$ no nulo tal que $v\sigma = v$ para todo $\sigma \in G$.

Por lo tanto, el K-espacio vectorial W generado por v es un $K[G]$-submódulo trivial de V. Si V es irreducible, entonces ha de ser $V = W$. ∎

De este modo, si G tiene orden potencia de p y K es un cuerpo de característica p, los únicos $K[G]$-módulos que se descomponen en suma directa de $K[G]$-módulos irreducibles son los triviales, ya que las componentes irreducibles han de ser triviales y la suma de $K[G]$-módulos triviales es trivial.

Ejemplo Sea p un número primo, $K = \mathbb{Z}/p\mathbb{Z}$ y consideremos la matriz

$$\sigma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{LG}(2, K).$$

Se comprueba fácilmente que

$$\sigma^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix},$$

por lo que $G = \langle\sigma\rangle$ es un grupo de orden p. La inclusión $\rho : G \longrightarrow \mathrm{LG}(2, K)$ es una representación matricial de p de grado 2. Consideremos la representación lineal $\rho : G \longrightarrow \mathrm{Aut}(K^2)$ asociada a la base canónica de K^2, de modo que

$$(1, 0)\sigma = (1, 1), \qquad (0, 1)\sigma = (0, 1).$$

Vemos que $V = K^2$ es un $K[G]$-módulo no trivial, que, de acuerdo con el teorema anterior, contiene como submódulo trivial al subespacio vectorial generado por $(0, 1)$, el cual no puede tener un submódulo complementario por las observaciones previas a este ejemplo. ∎

El teorema 1.12 hace que las representaciones de grupos sobre cuerpos de característica cero tengan un comportamiento mucho más simple que sobre cuerpos de característica prima. Por ello se distingue entre la *teoría de representaciones ordinarias* (sobre cuerpos de característica 0) y la teoría de *representaciones modulares* (sobre cuerpos de característica prima, que es esencialmente análoga a la primera cuando la característica no divide al orden del grupo).

[5] Véase el primer apartado de la sección 1.2, más abajo.

[6] Véase el teorema 1.18, más abajo, concretamente la observación posterior.

La característica más destacada de la teoría de representaciones ordinarias es que éstas quedan completamente determinadas por sus caracteres, en el sentido que definimos a continuación.

Recordemos que la traza[7] de una matriz cuadrada $A = (a_{ij})$ se define como

$$\mathrm{Tr}(A) = \sum_i a_{ii}.$$

La traza es invariante por semejanza, es decir, que, si M es una matriz regular, se cumple que $\mathrm{Tr}(M^{-1}AM) = \mathrm{Tr}(A)$. En particular, si V es un espacio vectorial y $f \in \mathrm{Aut}(V)$, podemos definir la traza $\mathrm{Tr}(f)$ como la traza de la matriz de f en cualquier base.

Definición 1.15 Sea $\rho : G \longrightarrow \mathrm{Aut}(V)$ una representación de un grupo finito G en un K-espacio vectorial V. Llamaremos *carácter* asociado a ρ a la función $\chi_\rho : G \longrightarrow K$ dada por $\chi_\rho(\sigma) = \mathrm{Tr}(\rho(\sigma))$. Los caracteres de las representaciones de G se llaman también caracteres de G. Un carácter es *irreducible* si está asociado a una representación irreducible.

Claramente, dos representaciones isomorfas determinan el mismo carácter. Observemos que, si ρ tiene grado n, entonces $\rho(1)$ es la identidad en V y su matriz asociada en cualquier base es I_n, luego $\chi_\rho(1) = n$.

Otro hecho obvio es que

$$\chi_\rho(\sigma^{-1}\tau\sigma) = \mathrm{Tr}(\rho(\sigma)^{-1}\rho(\tau)\rho(\sigma)) = \mathrm{Tr}(\rho(\tau)) = \chi_\rho(\tau).$$

En otras palabras: los caracteres son constantes sobre las clases de conjugación de G.

Ejemplo Sea r_G el carácter de la representación regular de un grupo G. Entonces

$$r_G(\sigma) = \begin{cases} |G| & \text{si } \sigma = 1, \\ 0 & \text{si } \sigma \neq 1. \end{cases}$$

En efecto, fijemos $\tau \in G$. Si $\tau \neq 1$ la matriz de $\rho(\tau)$ respecto de la base G tiene en la fila correspondiente a σ un único 1 situado en la columna correspondiente a $\sigma\tau \neq \sigma$, y ceros en los demás lugares, luego la diagonal es nula y, por consiguiente $r_G(\tau) = 0$. ∎

Ejemplo El grupo D_4 tiene 5 clases de conjugación:

$$\mathrm{cl}(D_4) = \{\{1\}, \{\sigma, \sigma^3\}, \{\sigma^2\}, \{\tau, \sigma^2\tau\}, \{\sigma\tau, \sigma^3\tau\}\},$$

y se comprueba sin dificultad que el carácter χ asociado a la representación lineal que hemos construido en la página 2 es el determinado por la tabla:

	1	σ	σ^2	τ	$\sigma\tau$
χ	2	0	-2	0	0

∎

[7] Definición 8.38 de mi libro de *Álgebra*.

Ejercicio: Calcular el carácter asociado a la representación de Σ_3 construida en la página 2.

El teorema siguiente muestra que la suma y el producto de caracteres es de nuevo un carácter.

Teorema 1.16 *Sean $\rho_i : G \longrightarrow \mathrm{Aut}(V_i)$, para $i = 1, 2$, dos representaciones de un grupo G y sean $\chi_i : G \longrightarrow K$ sus caracteres correspondientes. Entonces el carácter de $\rho_1 \oplus \rho_2$ es $\chi_1 + \chi_2$, y el carácter de $\rho_1 \otimes \rho_2$ es $\chi_1\chi_2$.*

Demostración: Si fijamos bases B_i de V_i y llamamos $\bar{\rho}_i(\sigma)$ a la matriz de $\rho_i(\sigma)$ en la base B_i, es claro que la matriz de $(\rho_1 \oplus \rho_2)(\sigma)$ en la base $B_1 \cup B_2$ de $V_1 \oplus V_2$ es

$$\begin{pmatrix} \bar{\rho}_1(\sigma) & 0 \\ 0 & \bar{\rho}_2(\sigma) \end{pmatrix},$$

y la traza de esta matriz es $\chi_1(\sigma) + \chi_2(\sigma)$.

Si $B_1 = \{v_i\}$, $B_2 = \{w_j\}$, $\bar{\rho}_1(\sigma) = (a_{ij})$, $\bar{\rho}_2(\sigma) = (b_{ij})$, entonces

$$(\rho_1 \otimes \rho_2)(\sigma)(v_i \otimes w_j) = \rho_1(\sigma)(v_i) \otimes \rho_2(\sigma)(v_j)$$

$$= \sum_k a_{ki} v_k \otimes \sum_l b_{lj} w_l = \sum_{k,l} a_{ki} b_{lj} v_k \otimes w_l.$$

La matriz $(\overline{\rho_1 \otimes \rho_2})(\sigma)$ en la base $B_1 \otimes B_2$ tiene una fila y una columna para cada elemento $v_k \otimes w_l$. Según el cálculo que acabamos de hacer, el elemento que está en la fila y en la columna correspondientes a $v_i \otimes w_j$ es $a_{ii}b_{jj}$, por lo que la traza es

$$\sum_{i,j} a_{ii} b_{jj} = \chi_1(\sigma)\chi_2(\sigma).$$

■

Terminamos esta sección con una observación adicional ilustrada por el ejemplo siguiente:

Ejemplo Consideremos la matriz

$$\sigma = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in \mathrm{LG}(2, \mathbb{Q}).$$

El grupo $G = \langle \sigma \rangle$ tiene orden 4 y la inclusión $\rho : G \longrightarrow \mathrm{LG}(2, \mathbb{Q})$ determina una representación matricial de G con coeficientes en $\mathbb{Q}$. Tomemos $V = \mathbb{Q}^2$ y consideremos la representación lineal inducida por ρ respecto de la base canónica. Resulta que es irreducible, pues un $\mathbb{Q}[G]$-submódulo propio de V debería ser un subespacio vectorial $W = \langle w \rangle$ de dimensión 1, luego habría de ser $w\sigma = rw$, para cierto $r \in \mathbb{Q}$ no nulo. Ahora bien, entonces r debería ser un valor propio de σ, es decir, una raíz del polinomio característico

$$|xI - \sigma| = x^2 + 1.$$

Como este polinomio no tiene raíces racionales, concluimos que, en efecto, la representación es irreducible. Ahora bien, si consideramos $V_{\mathbb{C}} = \mathbb{C}^2$, el mismo razonamiento prueba que $V_{\mathbb{C}}$ sí que tiene $\mathbb{C}[G]$-submódulos propios. Explícitamente:

$$V_{\mathbb{C}} = \langle (i,1) \rangle \oplus \langle (-i,1) \rangle$$

Así pues, vemos que una representación irreducible puede volverse reducible tras una extensión de constantes. ∎

Aunque no podemos justificarlo todavía, lo que marca la diferencia entre $\mathbb{Q}$ y $\mathbb{C}$ en lo tocante al ejemplo anterior es que $\mathbb{C}$ es algebraicamente cerrado. Como en muchos otros contextos algebraicos, sucede que "las cosas funcionan mejor cuando el cuerpo es algebraicamente cerrado" y, en efecto, sucede que la teoría de representaciones más sencilla es la teoría sobre cuerpos algebraicamente cerrados de característica 0, de la que nos ocuparemos en el capítulo siguiente.

1.2 Preliminares sobre grupos finitos

Recordamos ahora algunos hechos de la teoría de grupos finitos que nos serán necesarios más adelante. Suponemos que el lector está familiarizado con los hechos más elementales.[8]

Acciones de grupos El concepto de acción de un grupo sobre un conjunto permite tratar de forma unificada una situación (y, especialmente, un argumento) que aparece en contextos diversos.

Definición 1.17 Una *acción* de un grupo G sobre un conjunto X es un homomorfismo $\rho : G \longrightarrow \Sigma_X$ de G en el grupo Σ_X de las permutaciones de X (es decir, de las aplicaciones biyectivas de X en X, con el producto dado por la composición).

Si $x \in X$ y $\sigma \in G$, escribiremos a menudo $x\sigma = \rho(\sigma)(x)$. De este modo, para todo $x \in X$ y $\sigma, \tau \in G$, se cumple que

$$x1 = x, \qquad (x\sigma)\tau = x(\sigma\tau).$$

Una acción de G sobre un conjunto X define una relación de equivalencia en X, a saber, la dada por

$$x \sim y \text{ si y sólo si existe un } \sigma \in G \text{ tal que } x\sigma = y.$$

Llamaremos *órbita* de x a su clase de equivalencia, y la representaremos por $\Omega_x \subset X$. Por otro lado, el *estabilizador* de un $x \in X$ es el subgrupo

$$G_x = \{\sigma \in G \mid x\sigma = x\}.$$

El resultado fundamental sobre acciones de grupos es el siguiente:

[8] Véase, por ejemplo, mi libro de *Álgebra*.

Teorema 1.18 *Sea G un grupo finito que actúa sobre un conjunto finito X. Para cada $x \in X$, se cumple que*

$$|\Omega_x| = |G : G_x|.$$

DEMOSTRACIÓN: Observemos que $x\sigma = x\tau$ si y sólo si $x\sigma\tau^{-1} = x$, si y sólo si $\sigma\tau^{-1} \in G_x$, si y sólo si $G_x\sigma = G_x\tau$. Por lo tanto, la aplicación $f : G/G_x \longrightarrow \Omega_x$ dada por $f(G_x\sigma) = x\sigma$ está bien definida, es inyectiva y, por definición de órbita, es suprayectiva. ∎

En particular vemos que los cardinales de las órbitas han de dividir al orden del grupo.

Clases de conjugación Recordemos que si G es un grupo y $\sigma \in G$ la conjugación por σ es la aplicación $\alpha_\sigma : G \longrightarrow G$ dada por $\alpha_\sigma(\tau) = \tau^\sigma = \sigma^{-1}\tau\sigma$. Se comprueba inmediatamente que α_σ es un automorfismo de G. Más aún, la aplicación $G \longrightarrow \mathrm{Aut}(G)$ dada por $\sigma \mapsto \alpha_\sigma$ es un homomorfismo de grupos.

Observemos que un grupo G actúa sobre sí mismo por conjugación. La relación de equivalencia asociada a esta acción es la relación de conjugación que ya hemos considerado anteriormente, y la órbita de un $\sigma \in G$ respecto de la conjugación es lo que hemos llamado su clase de conjugación, y que representamos por $\mathrm{cl}_G(\sigma)$. El estabilizador de un $\sigma \in G$ recibe el nombre de *centralizador* de σ, y se representa por

$$C_G(\sigma) = \{\tau \in G \mid \sigma^\tau = \sigma\} = \{\tau \in G \mid \tau\sigma = \sigma\tau\}.$$

Vemos que es el subgrupo formado por los elementos que conmutan con σ. El teorema 1.18 se particulariza al teorema siguiente:

Teorema 1.19 *Si G es un grupo finito y $\sigma \in G$, se cumple que*

$$|\mathrm{cl}_G(\sigma)| = |G : C_G(\sigma)|.$$

Definimos el *centro* de G como el subgrupo formado por los elementos que conmutan con todos los elementos de G, es decir:

$$Z(G) = \{\sigma \in G \mid \sigma\tau = \tau\sigma \text{ para todo } \tau \in G\}.$$

Observemos que $\sigma \in Z(G)$ si y sólo si $\mathrm{cl}_G(\sigma) = \{\sigma\}$. Es evidente que $Z(G)$ es un subgrupo normal abeliano de G. Más aún, todo subgrupo de $Z(G)$ es normal en G.

Sabemos que un grupo finito G tiene $|Z(G)|$ clases de conjugación con un elemento y, digamos, n clases con más de un elemento. Sean $\sigma_1, \ldots, \sigma_n$ representantes de estas clases. El orden de G es la suma de los órdenes de sus clases de conjugación luego, teniendo en cuenta el teorema anterior, concluimos:

Teorema 1.20 (Ecuación de clases) *Si G es un grupo finito, existen elementos $\sigma_1, \ldots, \sigma_n \in G$ tales que $C_G(\sigma_i) < G$ y*

$$|G| = |Z(G)| + \sum_{i=1}^{n} |G : C_G(\sigma_i)|.$$

Recordemos que, si p es un número primo, un *p-grupo* es un grupo de orden potencia de p. Una consecuencia de la ecuación de clases es el hecho siguiente:

Teorema 1.21 *Si p es un número primo y G es un p-grupo, entonces $Z(G) \neq 1$.*

Demostración: Con la notación del teorema anterior, como $C_G(\sigma_i) < G$, tenemos que $p \mid |G : C_G(\sigma_i)|$, luego la ecuación de clases nos da que $p \mid |Z(G)|$, luego $Z(G) \neq 1$. ∎

De aquí deducimos a su vez:

Teorema 1.22 *Si p es un número primo y G es un p-grupo no trivial, entonces G tiene un subgrupo normal de índice p.*

Demostración: Lo probamos por inducción sobre el orden de G. Si $|G| = p$ el subgrupo trivial es un subgrupo normal de índice p. Supongamos que el teorema es cierto para p-grupos de orden menor que $|G|$. Como $Z(G)$ es un subgrupo abeliano no trivial, podemos tomar un $\sigma \in Z(G)$ de orden p. El subgrupo $H = \langle \sigma \rangle$ tiene orden p y es normal, por estar contenido en $Z(G)$. Podemos suponer que $H < G$, pues ya hemos tratado el caso en que $|G| = p$. El grupo cociente G/H tiene orden menor que $|G|$, luego por hipótesis de inducción tiene un subgrupo normal N/H de índice p. Es claro que N es un subgrupo normal en G de índice p. ∎

A su vez, esto implica que los p-grupos tienen subgrupos de todos los órdenes que dividen al orden del grupo.

Subgrupos de Sylow Si G es un grupo finito y p es un número primo, podemos descomponer $|G| = p^n m$, con $p \nmid m$. Un *p-subgrupo de Sylow* de G es un subgrupo de orden p^n.

Teorema 1.23 (Teorema de Sylow) *Sea G un grupo finito y p un número primo.*

a) G tiene p-subgrupos de Sylow.

b) Todo p-subgrupo de G está contenido en un p-subgrupo de Sylow.

c) Dos p-subgrupos de Sylow cualesquiera de G son conjugados.

Demostración: Demostraremos a) por inducción sobre el orden de G. Si G tiene orden 1 es obvio. Supongamos que todos los grupos de orden menor que $|G|$ tienen p-subgrupos de Sylow y demostremos que G también los tiene.

Si $p \nmid |G|$, entonces el subgrupo trivial es un p-subgrupo de Sylow de G. Supongamos, pues, que $p \mid |G|$. Sea $|G| = p^n \cdot m$, con $(p, m) = 1$.

Distinguimos dos casos:

Caso 1 Existe un subgrupo $H < G$ tal que $p \nmid |G : H|$.

Entonces $p^n \mid |H|$ y por hipótesis de inducción H tiene un p-subgrupo de Sylow P de orden p^n, y así, P es también un p-subgrupo de Sylow de G.

Caso 2 Para todo subgrupo $H < G$, se cumple que $p \mid |G : H|$.

Entonces la ecuación de clases nos da que $p \mid |Z(G)|$. Como se trata de un grupo abeliano,[9] tiene un elemento de orden p o, lo que es lo mismo, G tiene un subgrupo $H \leq Z(G)$ de orden p. Como los elementos de H conmutan con todos los elementos de G, es evidente que H es normal en G.

Se cumple que $|G/H| = p^{n-1}m$ y, por hipótesis de inducción, tiene un subgrupo de Sylow P/H que cumplirá $|P/H| = p^{n-1}$, luego $|P| = p^n$, es decir, P es un subgrupo de Sylow de G.

Consideremos ahora Q un p-subgrupo de G. Entonces Q actúa sobre el conjunto cociente G/P por multiplicación por la derecha (es decir, consideramos la acción ρ dada por $\rho(\sigma)(P\tau) = P\tau\sigma$).

El teorema 1.18 nos da que las órbitas de los elementos de G/P tienen cardinal potencia de p, sin excluir la posibilidad de que alguna tenga cardinal $p^0 = 1$. De hecho, concluimos que alguna órbita ha de tener cardinal igual a 1, pues, de lo contrario, el cardinal de G/P, que es m, sería suma de potencias (no triviales) de p, luego sería múltiplo de p.

Así pues, existe un $\sigma \in G$ tal que la clase $x = P\sigma$ cumple $|\Omega_x| = 1$, de modo que $P\sigma\tau = P\sigma$ para todo $\tau \in Q$. En particular $\sigma\tau \in P\sigma$, luego $\tau \in P^\sigma$, para todo $\tau \in Q$. Concluimos que $Q \leq P^\sigma$ y P^σ es también un subgrupo de Sylow de G. Esto prueba b).

Si Q es también un p-subgrupo de Sylow de G, entonces ha de darse la igualdad $Q = P^\sigma$, pues tenemos una inclusión y ambos grupos tienen el mismo orden. Esto prueba c). ∎

En particular vemos que un p-subgrupo de Sylow es normal si y sólo si es el único p-subgrupo de Sylow de G.

La existencia de p-subgrupos de Sylow junto con 1.22, implica que un grupo G tiene p-subgrupos de todos los órdenes que dividen a $|G|$. En particular:

Teorema 1.24 *Si G es un grupo finito y p es un primo tal que $p \mid |G|$, entonces G tiene un elemento de orden p.*

[9] Aquí usamos que todo grupo abeliano es producto de grupos cíclicos, y que un grupo cíclico tiene elementos de todos los órdenes que dividen a su orden.

Grupos resolubles, superresolubles y nilpotentes Recordemos que un grupo finito G se dice *resoluble* si existe una serie de subgrupos

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

con factores G_i/G_{i-1} abelianos.

Diremos que G es *superresoluble* si además se cumple que $G_i \trianglelefteq G$ y los factores G_i/G_{i-1} son cíclicos.

Diremos que G es *nilpotente* si los factores son centrales, es decir, si

$$G_i/G_{i-1} \leq Z(G/G_{i-1}),$$

(lo cual implica que $G_i/G_{i-1} \trianglelefteq G/G_{i-1}$ y a su vez que $G_i \trianglelefteq G$).

Teorema 1.25 *Todo subgrupo y todo cociente de un grupo resoluble (resp. superresoluble o nilpotente) es también resoluble (resp. superresoluble o nilpotente).*

Demostración: Supongamos que G es resoluble, superresoluble o nilpotente y consideremos una serie de subgrupos según la definición correspondiente. Si $N \trianglelefteq G$, podemos considerar la serie

$$1 = G_0N/N \trianglelefteq G_1N/N \trianglelefteq \cdots \trianglelefteq G_nN/N = G/N.$$

Si G es superresoluble, es claro que $G_iN/N \trianglelefteq G/N$ y si G es nilpotente, también es claro que

$$\frac{G_iN/N}{G_{i-1}N/N} \leq Z\left(\frac{G/N}{G_{i-1}N/N}\right),$$

pues si $\sigma \in G_i$ y $\tau \in G$, entonces $\sigma\tau = \tau\sigma\sigma'$, para cierto $\sigma' \in G_{i-1}$, de donde se sigue que las clases de σ y τ en el grupo de la izquierda conmutan entre sí. Por otra parte, tenemos un epimorfismo

$$G_i/G_{i-1} \longrightarrow (G_iN/N) \,/\, (G_{i-1}N/N),$$

luego los factores son también abelianos o cíclicos si lo son G_i/G_{i-1}.

Similarmente, si $H \leq G$, razonamos análogamente con la serie

$$1 = G_0 \cap H \trianglelefteq G_1 \cap H \trianglelefteq \cdots \trianglelefteq G_n \cap H = H,$$

donde ahora tenemos monomorfismos

$$(G_i \cap H)/(G_{i-1} \cap H) \longrightarrow G_i/G_{i-1}.$$

■

Ejercicio: Probar que si $N \trianglelefteq G$ cumple que N y G/N son resolubles, entonces G es resoluble.

Teorema 1.26 *Si G es un grupo finito tal que $G/Z(G)$ es superresoluble o nilpotente, entonces G también lo es.*

DEMOSTRACIÓN: Sea

$$1 = G_0/Z(G) \trianglelefteq G_1/Z(G) \trianglelefteq \cdots \trianglelefteq G_n/Z(G) = G/Z(G)$$

una serie según la definición de grupo superresoluble o nilpotente. Es claro que la serie

$$Z(G) = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

cumple también la definición para G salvo que quizá $Z(G) \neq 1$. Ahora bien, como $Z(G)$ es abeliano, se descompone en producto de grupos cíclicos, y esta descomposición da lugar claramente a una serie

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_m = Z(G)$$

con factores N_i/N_{i-1} cíclicos. Más aún, es claro que $N_i/N_{i-1} \leq Z(G/N_{i-1})$, luego al enlazar las dos series anteriores obtenemos una serie para G que cumple la definición de grupo superresoluble o nilpotente. ∎

Como consecuencia:

Teorema 1.27 *Todo grupo nilpotente es superresoluble y todo grupo superresoluble es resoluble.*

DEMOSTRACIÓN: Es evidente que todo grupo superresoluble es resoluble. Sea G nilpotente y veamos que es superresoluble por inducción sobre el orden de G. Como para $G = 1$ es trivial, podemos suponer que todo grupo nilpotente de orden menor que $|G|$ es superresoluble. Tomemos una serie según la definición de grupo nilpotente. Podemos suponer que $1 = G_0 < G_1$. Como $G_1 \leq Z(G)$, tenemos que $Z(G) \neq 1$. Por consiguiente, $G/Z(G)$ es un grupo nilpotente de orden menor que G, luego es superresoluble por hipótesis de inducción, luego G es superresoluble por el teorema anterior. ∎

Teorema 1.28 *Todo p-grupo es nilpotente.*

DEMOSTRACIÓN: Aplicamos el mismo razonamiento inductivo del teorema anterior: sabemos que $Z(G) \neq 1$ (por el teorema 1.21), luego $G/Z(G)$ es nilpotente por hipótesis de inducción y esto implica a su vez que G lo es. ∎

También es obvio que todo grupo abeliano es nilpotente.

Teorema 1.29 *El producto directo de grupos resolubles (resp. superresolubles o nilpotentes) es resoluble (resp. superresoluble o nilpotente).*

DEMOSTRACIÓN: Para grupos resolubles basta observar que si $G = H \times K$, entonces H y G/H son resolubles. Para grupos nilpotentes basta observar que $Z(G) = Z(H) \times Z(K) \neq 1$ y razonar por inducción: como

$$G/Z(G) = (H/Z(H)) \times (K/Z(K))$$

es nilpotente, lo mismo le sucede a G. Para grupos superresolubles razonamos como en 1.26, teniendo en cuenta que los subgrupos normales de H son también subgrupos normales de G. ∎

Aunque no nos va a hacer falta, vamos a probar que los grupos nilpotentes son precisamente los productos de p-grupos. Para ello necesitamos un resultado previo. Se define el *normalizador* de un subgrupo H en un grupo G como el subgrupo

$$N_G(H) = \{\sigma \in G \mid H^\sigma = H\}.$$

Teorema 1.30 *Si G es un grupo nilpotente y $H < G$, entonces $H < N_G(H)$.*

Demostración: Sea $1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$ una serie según la definición de grupo nilpotente. Existe un i tal que $G_{i-1} \leq H$ pero $G_i \not\leq H$. Tomemos $\sigma \in G_i \setminus H$. Como $G_i/G_{i-1} \leq Z(G/G_{i-1})$, para cada $h \in H$ se cumple que $h^\sigma G_{i-1} = hG_{i-1}$, luego $h^\sigma \in H$. Esto implica que $H^\sigma \leq H$ y, como ambos grupos tienen el mismo orden, $H^\sigma = H$. Por lo tanto, $\sigma \in N_G(H) \setminus H$. ∎

Teorema 1.31 *Un grupo finito es nilpotente si y sólo si es producto directo de p-grupos (para distintos primos p).*

Demostración: Sea G un grupo nilpotente. Basta probar que tiene un único subgrupo de Sylow para cada primo p que divida a $|G|$ y que G es el producto directo de todos ellos. Sea $P \leq G$ un p-subgrupo de Sylow. Como los p-subgrupos de Sylow son conjugados, la unicidad equivale a que $P \trianglelefteq G$, y esto a su vez implica ya que el producto de los p-subgrupos de Sylow para todos los divisores primos de $|G|$ es directo (pues el producto de todos ellos tiene orden igual a $|G|$ y la intersección de uno con el producto de los demás es necesariamente trivial, teniendo en cuenta sus órdenes).

Así pues, sólo hemos de probar que $P \trianglelefteq G$. Esto equivale a que $N_G(P) = G$. En caso contrario, el teorema anterior nos da que $N_G(P) < N_G(N_G(P))$. Vamos a ver que esto es imposible. Para ello tomamos $\sigma \in N_G(N_G(P))$, lo que significa que $N_G(P)^\sigma = N_G(P)$. Entonces $P^\sigma \leq N_G(P)$, pero, como $P \trianglelefteq N_G(P)$, sucede que P es el único p-subgrupo de Sylow de $N_G(P)$, luego ha de ser $P^\sigma = P$, lo que implica que $\sigma \in N_G(P)$. ∎

Como consecuencia, un grupo nilpotente tiene subgrupos de todos los órdenes que dividen al orden del grupo.

Más adelante necesitaremos este hecho elemental:

Teorema 1.32 *Si G es un grupo finito superresoluble no abeliano, entonces existe un subgrupo normal abeliano N que cumple $Z(G) \lhd N \lhd G$.*

Demostración: El cociente $G/Z(G) \neq 1$ es superresoluble, luego podemos considerar el primer término no trivial $N/Z(G) \trianglelefteq G/Z(G)$ de una serie según la definición de grupo superresoluble. Así, se cumple que $Z(G) \lhd N \trianglelefteq G$ y $N/Z(G)$ es cíclico. Es claro entonces que N es abeliano, luego $N \neq G$. ∎

1.3 Preliminares sobre anillos

Los resultados de esta sección no serán necesarios en el capítulo siguiente, por lo que tal vez el lector prefiera saltársela de momento y volver después sobre ella cuando ya esté familiarizado con la teoría de caracteres.

Módulos e ideales Tal y como hemos advertido en la sección precedente, el estudio de las representaciones de grupos nos obligará a trabajar con módulos sobre anillos no conmutativos. Recordemos que, si A es un anillo no necesariamente conmutativo, debemos distinguir entre A-módulos por la izquierda y A-módulos por la derecha, según si los escalares de A multiplican por la izquierda o por la derecha a los elementos del módulo M. La diferencia sería meramente un convenio de escritura si no fuera por la propiedad asociativa del producto, que es

$$(ab)m = a(bm) \quad \text{por la izquierda, y} \quad m(ab) = (ma)b \quad \text{por la derecha.}$$

Si tratamos de escribir la propiedad asociativa para A-módulos derechos con los escalares a la izquierda obtenemos $(ab)m = b(am)$, que no es lo mismo que la propiedad asociativa para A-módulos izquierdos (salvo que el anillo A sea conmutativo).

Si A y B son dos anillos, un *A-B-bimódulo* es un conjunto M con estructura de A-módulo por la izquierda, de B-módulo por la derecha y que cumple la propiedad asociativa mixta $(am)b = a(mb)$, para $a \in A$, $m \in M$ y $b \in B$.

En particular, un anillo A puede considerarse de forma natural como A-módulo por la izquierda y como A-módulo por la derecha (lo que lo convierte en un A-A-bimódulo) y, en general, ambas estructuras son distintas y no debemos confundirlas. (Véanse los ejemplos de las páginas 21 y 22.) Por ejemplo, un *ideal izquierdo* (resp. derecho) I de A es un submódulo respecto de la estructura de A-módulo por la izquierda (resp. por la derecha) de A. Explícitamente, es un subconjunto $I \subset A$ no vacío que cumple las propiedades siguientes:

a) $a + b \in I$ para todo a, $b \in I$,

b) $ab \in I$ para todo $a \in A$ y todo $b \in I$ (resp. para todo $a \in I$ y todo $b \in A$).

Un *ideal bilátero* es un subconjunto de A que es a la vez un ideal izquierdo y derecho.

Si I es un ideal izquierdo (resp. derecho), el grupo cociente A/I tiene una estructura natural de A-módulo por la izquierda (resp. por la derecha), pero para que herede la estructura de anillo de A es necesario y suficiente que I sea un ideal bilátero.[10]

Aunque ya lo hemos señalado al definir las álgebras $A[G]$, repetimos aquí por conveniencia la definición de álgebra no (necesariamente) conmutativa:

[10] Veamos la necesidad: si $a \in A$ y $b \in I$, entonces $[ab] = [a][b] = [a][0] = 0$, luego $ab \in I$. Esto prueba que I es un ideal derecho, e igualmente se comprueba que es un ideal izquierdo.

Definición 1.33 Si A es un anillo conmutativo, una *A-álgebra* B es un anillo dotado de estructura de A-módulo de forma que $a(b_1b_2) = (ab_1)b_2 = b_1(ab_2)$, para todo $a \in A$, $b_1, b_2 \in B$.

En particular, si B es un anillo y A es un subanillo contenido en su centro, entonces B tiene una estructura natural de A-álgebra.

Para terminar este primer epígrafe, recordamos la definición de sucesión exacta de homomorfismos de grupos (en particular, de módulos):

Definición 1.34 Una cadena de homomorfismos de grupos

$$\cdots \longrightarrow M \xrightarrow{\alpha} N \xrightarrow{\beta} R \longrightarrow \cdots$$

es *exacta* en N si cumple $\operatorname{Im}\alpha = \operatorname{N}(\beta)$. La sucesión completa es *exacta* si lo es en todos sus módulos.

En particular, una sucesión $0 \longrightarrow M \xrightarrow{\alpha} N$ es exacta en M si y sólo si α es inyectiva, mientras que una sucesión $M \xrightarrow{\beta} N \longrightarrow 0$ es exacta en N si y sólo si α es suprayectiva.

Una *sucesión exacta corta* es una sucesión exacta de la forma

$$0 \longrightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \longrightarrow 0,$$

de modo que M' puede identificarse con un submódulo de M y $M'' \cong M/M'$.

Si $M = M' \oplus M''$, podemos formar obviamente una sucesión exacta corta con $\alpha(m') = m'$ y $\beta(m' + m'') = m''$. Cuando una sucesión exacta corta es de esta forma se dice que se escinde. Más concretamente, se dice que una sucesión exacta corta *se escinde* si cumple cualquiera de las condiciones del teorema siguiente:

Teorema 1.35 *Sea $0 \longrightarrow M' \xrightarrow{i_1} M \xrightarrow{p_2} M'' \longrightarrow 0$ una sucesión exacta corta de módulos. Las afirmaciones siguientes son equivalentes:*

a) Si $M_1 = i_1[M']$, existe un submódulo $M_2 \subset M$ tal que $M = M_1 \oplus M_2$. (Obviamente, entonces, $M_2 \cong M''$).

b) Existe un homomorfismo $i_2 : M'' \longrightarrow M$ tal que $i_2 \circ p_2 = 1$.

c) Existe un homomorfismo $p_1 : M \longrightarrow M'$ tal que $i_1 \circ p_1 = 1$.

Demostración: a) $\Rightarrow$ b) Observemos que $p_2|_{M_2} : M_2 \longrightarrow M''$ es un isomorfismo. En efecto, si $p_2(m_2) = 0$, entonces $m_2 \in M_1 \cap M_2 = 0$. Basta tomar $i_2 = (p_2|_{M_2})^{-1}$.

b) $\Rightarrow$ a) Tomamos $M_2 = i_2[M'']$. Si $m \in M$, entonces $m - i_2(p_2(m)) \in M_1$, pues

$$p_2(m - i_2(p_2(m))) = p_2(m) - p_2(i_2(p_2(m))) = p_2(m) - p_2(m) = 0.$$

Por consiguiente, $m \in M_1 + M_2$ y $M = M_1 + M_2$. Un punto de $M_1 \cap M_2$ es de la forma $m = i_1(m') = i_2(m'')$, luego aplicando p_2 vemos que $m'' = 0$, luego $m = 0$. Esto prueba que la suma es directa.

a) $\Rightarrow$ c) Tomamos como p_1 la proyección asociada a la descomposición en suma directa.

c) $\Rightarrow$ a) Tomamos como M_2 el núcleo de p_1. Si $m \in M$, se comprueba fácilmente que $m - i_1(p_1(m)) \in M_2$, luego $M = M_1 + M_2$, y si $m \in M_1 \cap M_2$, entonces $m = i_1(m')$ y $0 = p_1(m) = m'$, luego $m = 0$. Esto prueba que la suma es directa. ∎

Anillos y módulos noetherianos Estudiamos ahora dos importantes condiciones de finitud sobre un anillo.

Definición 1.36 Sea A un anillo y M un A-módulo (por la izquierda o por la derecha). Se dice que M es *noetheriano* (resp. *artiniano*) si no contiene cadenas estrictamente crecientes (resp. decrecientes) de submódulos. Un anillo A es *artiniano* (resp. *noetheriano*) por la izquierda (o por la derecha) si lo es como A-módulo por la izquierda (o por la derecha).

Es claro que un A-módulo M es noetheriano (resp. artiniano) si cualquier familia no vacía de submódulos tiene un elemento maximal (resp. minimal) respecto de la inclusión.

Teorema 1.37 *Un A-módulo M es noetheriano si y sólo si todos sus submódulos son finitamente generados.*

Demostración: Si M es un A-módulo y tiene un submódulo N no finitamente generado, tomamos $n_1 \in N$, de modo que $\langle n_1 \rangle \subsetneq N$, luego existe un $n_2 \in N \setminus \langle n_1 \rangle$, de modo que $\langle n_1 \rangle \subsetneq \langle n_1, n_2 \rangle \subsetneq N$, y de este modo podemos construir una cadena estrictamente creciente de submódulos, luego M no es noetheriano.

Recíprocamente, si todo submódulo de M es finitamente generado y tenemos una cadena de submódulos

$$M_1 \subset M_2 \subset M_3 \subset \cdots,$$

tenemos que la unión de todos ellos, llamémosla N, es también un submódulo de M. Por hipótesis tiene un generador finito, que estará contenido en algún M_i, y es claro entonces que $M_i = M$, luego la cadena no es estrictamente creciente. ∎

Ejemplo *El anillo A formado por las matrices*

$$\begin{pmatrix} m & r \\ 0 & s \end{pmatrix},$$

donde $m \in \mathbb{Z}$, r, $s \in \mathbb{Q}$, es noetheriano por la derecha, pero no por la izquierda.

En efecto, observemos en primer lugar que

$$\begin{pmatrix} m_1 & r_1 \\ 0 & s_1 \end{pmatrix}\begin{pmatrix} m_2 & r_2 \\ 0 & s_2 \end{pmatrix} = \begin{pmatrix} m_1m_2 & m_1r_2 + r_1s_2 \\ 0 & s_1s_2 \end{pmatrix},$$

por lo que A es ciertamente un anillo (unitario). En particular,

$$\begin{pmatrix} m & r \\ 0 & s \end{pmatrix}\begin{pmatrix} 0 & t \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & mt \\ 0 & 0 \end{pmatrix},$$

por lo que, si llamamos a_t al segundo factor, tenemos que

$$Aa_1 \subsetneq Aa_{1/2} \subsetneq Aa_{1/4} \subsetneq Aa_{1/8} \subsetneq \cdots$$

lo que prueba que A no es noetheriano por la izquierda. Sea ahora I un ideal derecho de A y llamemos $I_0 \subset I$ al ideal formado por las matrices de I que cumplen $m = 0$. Como

$$\begin{pmatrix} 0 & r_1 \\ 0 & s_1 \end{pmatrix}\begin{pmatrix} m_2 & r_2 \\ 0 & s_2 \end{pmatrix} = \begin{pmatrix} 0 & r_1s_2 \\ 0 & s_1s_2 \end{pmatrix},$$

es claro que I_0 es ciertamente un ideal derecho, así como que la aplicación $I_0 \longrightarrow \mathbb{Q}^2$ que a cada matriz le asigna su par de coordenadas (r, s) es un monomorfismo de grupos cuya imagen es un subespacio vectorial de $\mathbb{Q}^2$. Por consiguiente, dicha imagen admite un sistema generador con dos elementos (no necesariamente independientes). Si llamamos $a_1, a_2 \in I_0$ a sus antiimágenes en I_0, es fácil ver que $I_0 = \langle a_1, a_2\rangle$.

Si $I = I_0$, entonces ya tenemos que I es finitamente generado. En caso contrario, sea $a_3 \in I$ una matriz cuyo valor $m = m_0 \neq 0$ sea el menor posible en valor absoluto. Multiplicando a_3 por $-\mathrm{Id}$ si fuera necesario (donde Id es la matriz identidad), podemos suponer que $m_0 > 0$. Si $a \in I$, dividimos su coeficiente m entre m_0, de modo que $m = cm_0 + r$, con $0 \leq r < m_0$. Entonces $a - a_3(c\,\mathrm{Id}) \in I$ tiene $m = r$, luego, por la minimalidad de m_0, ha de ser $m = r = 0$, luego $a - a_3(c\,\mathrm{Id}) \in I_0$. Esto prueba que $I = \langle a_1, a_2, a_3\rangle$, luego A es noetheriano por la derecha. ∎

Ejemplo *El anillo A formado por las matrices*

$$\begin{pmatrix} r & \alpha \\ 0 & \beta \end{pmatrix},$$

donde $r \in \mathbb{Q}$, $\alpha, \beta \in \mathbb{R}$, es artiniano por la derecha, pero no por la izquierda.

En efecto, si $V \subset \mathbb{R}$ es un $\mathbb{Q}$-espacio vectorial, se comprueba inmediatamente que el conjunto $I(V) \subset A$ de las matrices con $r = \beta = 0$, $\alpha \in V$ es un ideal izquierdo de A. Como $\mathbb{R}$ tiene dimensión infinita sobre $\mathbb{Q}$, podemos tomar una familia de subespacios vectoriales

$$\cdots \subsetneq V_3 \subsetneq V_2 \subsetneq V_1 \subsetneq V_0 \subset \mathbb{R},$$

que da lugar a una cadena de ideales

$$\cdots \subsetneq I(V_3) \subsetneq I(V_2) \subsetneq I(V_1) \subsetneq I(V_0) \subset A,$$

lo que prueba que A no es artiniano por la izquierda. Supongamos ahora que

$$\cdots \subset I_3 \subset I_2 \subset I_1 \subset I_0 \subset A$$

es una cadena de ideales derechos. Llamemos I_n^0 al ideal formado por los elementos de I_n que cumplen $r = 0$. Se comprueba fácilmente que la aplicación $I_n^0 \longrightarrow \mathbb{R}^2$ que a cada matriz le asigna su par (α, β) es un monomorfismo de grupos cuya imagen es un $\mathbb{R}$-espacio vectorial. Por consiguiente, la sucesión $I_0^0 \supset I_1^0 \supset I_2^0 \supset \cdots$ ha de estabilizarse, es decir, existe un ideal derecho I^0 tal que $I_n^0 = I^0$ para todo n suficientemente grande. No perdemos generalidad si suponemos que esto sucede para todo n.

Si algún n cumple $I_n = I^0$, entonces $I_m = I^0$ para todo $m \geq n$, con lo que la cadena se estabiliza. En caso contrario $I_n \neq I^0$ para todo n. Tomemos $a_0 \in I_0 \setminus I_0^0$. No perdemos generalidad si suponemos que a_0 tiene $r = 1$.

Si $a \in I_n$ tiene primer coeficiente igual a r, entonces $a - a_0(r\,\mathrm{Id}) \in I^0$, lo que prueba que $I_n = I^0 + \langle a_0 \rangle$, luego la sucesión es constante. Esto prueba que A no contiene cadenas estrictamente decrecientes de ideales derechos, luego A es artiniano por la derecha. ∎

Teorema 1.38 *Si $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ es una sucesión exacta de homomorfismos de A-módulos, entonces M es noetheriano (resp. artiniano) si y sólo si lo son M' y M''.*

Demostración: Supongamos que M es artiniano. Obviamente, una cadena descendente de submódulos de M' lo es también de M, luego si M es artiniano M' también lo es. Similarmente, una cadena descendente de submódulos de M'' ha de ser de la forma

$$M_0/M'' \supset M_1/M'' \supset M_2/M'' \supset \cdots$$

La cadena de los "numeradores" se ha de estabilizar, luego lo mismo le sucede a la cadena dada.

Si M' y M'' son artinianos y tenemos una cadena descendente de submódulos de M, digamos

$$M_0 \supset M_1 \supset M_2 \supset \cdots$$

entonces las cadenas $\{M_n \cap M'\}_n$ y $\{(M_n + M')/M'\}_n$ se han de estabilizar para n suficientemente grande. Si

$$M_n \cap M' = M_{n+1} \cap M', \qquad (M_n + M')/M' = (M_{n+1} + M')/M',$$

entonces $M_n = M_{n+1}$, pues si $m \in M_n$ entonces $m + M' = m'' + M'$, para un $m'' \in M_{n+1}$, luego existe un $m' \in M'$ tal que $m = m' + m''$. Entonces $m' \in M' \cap M_n$, luego $m' \in M_{n+1}$, luego $m \in M_{n+1}$. Esto prueba que la cadena de partida se estabiliza.

La demostración para módulos noetherianos es análoga. ∎

De aquí se sigue inmediatamente que la suma directa de dos (y, por consiguiente, de un número finito de) módulos noetherianos (resp. artinianos) es noetheriana (resp. artiniana). A su vez, de aquí se sigue el teorema siguiente:

Teorema 1.39 *Si A es un anillo noetheriano (resp. artiniano) (por la izquierda o por la derecha), entonces, todo A-módulo finitamente generado (por la izquierda o por la derecha) es noetheriano (resp. artiniano).*

Demostración: Esto se debe a que M se puede expresar como cociente de una suma directa de un número finito de copias de A (considerado como A-módulo por la izquierda o por la derecha). ∎

Módulos de longitud finita Vamos a estudiar los módulos que son simultáneamente noetherianos y artinianos.

Definición 1.40 Si A es un anillo, un A-módulo M es *simple* o *irreducible* si $M \neq 0$ y no contiene más submódulos que los submódulos impropios: 0 y M.

En estos términos, una representación lineal $\rho : G \longrightarrow \mathrm{Aut}(V)$ es irreducible si y sólo si V es un $K[G]$-módulo irreducible.

Definición 1.41 Una *serie de composición* de un A-módulo M es una sucesión de submódulos

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_l = M$$

tal que cada factor M_i/M_{i-1} es simple. El número l se llama *longitud* de la serie. Se dice que M es un A-módulo de *longitud finita* si tiene una serie de composición. Diremos que un anillo A tiene *longitud finita* (por la izquierda o por la derecha) si tiene longitud finita como A-módulo.

Luego veremos que, tal y como hemos anunciado, estos módulos no son sino los módulos noetherianos y artinianos al mismo tiempo. Antes hemos de probar otros resultados, entre ellos el que justifica el nombre de "módulos de longitud finita". Necesitamos algunos resultados previos:

Teorema 1.42 (Zassenhaus) *Sea A un anillo, sea M un A-módulo y sean $N' \subset N$, y $R' \subset R$ submódulos de M. Entonces*

$$\frac{N' + (N \cap R)}{N' + (N \cap R')} \cong \frac{R' + (N \cap R)}{R' + (N' \cap R)}.$$

Demostración: Basta probar que

$$\frac{N' + (N \cap R)}{N' + (N \cap R')} \cong \frac{N \cap R}{(N \cap R') + (N' \cap R)}$$

pues intercambiando N y R obtenemos un isomorfismo análogo donde el miembro izquierdo es el miembro derecho del enunciado y el miembro derecho es el mismo. Para ello definimos

$$f : N' + (N \cap R) \longrightarrow (N \cap R)/((N \cap R') + (N' \cap R))$$

mediante $f(n'+m) = [m]$. La definición es correcta, pues si $n'_1 + m_1 = n'_2 + m_2$, con $n'_i \in N'$, $m_i \in N \cap R$, entonces

$$m_1 - m_2 = n'_2 - n'_1 \in (N \cap R) \cap N' = N' \cap R \subset (N \cap R') + (N' \cap R).$$

Es claro que f es un epimorfismo de módulos y se cumple que $f(n'+m) = 0$ si y sólo si $m \in (N \cap R') + (N' \cap R)$, si y sólo si

$$n' + m \in N' + (N \cap R') + (N' \cap R) = N' + (N \cap R').$$

Así pues, el núcleo de f es $n' + (N \cap R')$ y el teorema queda probado. ∎

Se dice que una serie de submódulos

$$0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$$

es un *refinamiento* de otra serie dada si resulta de intercalar submódulos entre los de dicha otra serie.

Teorema 1.43 (Schreier) *Si A es un anillo y M es un A-módulo, dos series cualesquiera de submódulos de M admiten refinamientos equivalentes, en el sentido de que cada factor de un refinamiento se corresponde biunívocamente con un factor isomorfo del otro refinamiento.*

Demostración: Consideremos dos series de submódulos:

$$0 = N_0 \subset N_1 \subset \cdots \subset N_k = M, \quad 0 = R_0 \subset R_1 \subset \cdots \subset R_l = M.$$

Entre N_{i-1} y N_i intercalamos los submódulos

$$N_{i-1} = N_{i-1} + (N_i \cap R_0) \subset N_{i-1} + (N_i \cap R_1) \subset \cdots \subset N_{i-1} + (N_i \cap R_l) = N_i$$

y, del mismo modo, entre R_{j-1} y R_j insertamos

$$R_{j-1} = R_{j-1} + (R_j \cap N_0) \subset R_{j-1} + (R_j \cap N_1) \subset \cdots \subset R_{j-1} + (R_j \cap N_k) = R_j.$$

De este modo hemos obtenido refinamientos de longitud kl y el teorema anterior nos da que

$$\frac{N_{i-1} + (N_i \cap R_j)}{N_{i-1} + (N_i \cap R_{j-1})} \cong \frac{R_{j-1} + (N_i \cap R_j)}{R_{j-1} + (N_{i-1} \cap R_j)},$$

es decir, que el j-ésimo factor insertado entre N_{i-1} y N_i es isomorfo al i-ésimo factor insertado entre R_{j-1} y R_j. ∎

Teorema 1.44 (Jordan-Hölder) *Si A es un anillo y M es un A-módulo de longitud finita, dos series de composición cualesquiera de M tienen la misma longitud, y cada factor de una se corresponde biunívocamente con un factor isomorfo de la otra.*

DEMOSTRACIÓN: Dadas dos series de composición de M, les aplicamos el teorema anterior para obtener dos refinamientos equivalentes. Las series de partida, por definición, no tienen factores triviales, pero los refinamientos construidos en el teorema anterior pueden tenerlos. Ahora bien, cada factor trivial de un refinamiento se corresponde biunívocamente con otro factor trivial del otro, luego si eliminamos los módulos repetidos de ambos refinamientos, seguimos teniendo refinamientos equivalentes, pero ahora sin factores triviales. Esto significa que, en cada serie de composición, hemos intercalado módulos estrictamente comprendidos entre sus términos, pero, como los factores son simples, no existen tales módulos. Esto sólo es posible si las series dadas eran ya equivalentes, lo que, en particular, supone que tienen la misma longitud. ∎

Así pues, si M es un A-módulo de longitud finita, podemos definir su *longitud*, que representaremos por $l(M)$, como la longitud de cualquiera de sus series de composición. Más aún, podemos hablar de sus *factores de composición*, definidos (salvo isomorfismo) como los A-módulos simples que aparecen como factores en cualquier serie de composición de M. Más aún, para cada factor de composición de M podemos definir su *multiplicidad* como el número de veces que aparece en una serie de composición de M. En series distintas, los factores de composición pueden aparecer en un orden distinto, pero el teorema anterior prueba que cada uno de ellos aparecerá siempre el mismo número de veces, es decir, que la multiplicidad en M de un factor de composición está bien definida.

El mismo argumento que hemos usado en la prueba del teorema 1.44 (aplicado ahora a una serie de composición y una serie arbitraria) nos da el teorema siguiente:

Teorema 1.45 *Si M es un módulo de longitud finita, toda serie en M (con factores no triviales) puede refinarse hasta una serie de composición.*

Ahora ya podemos demostrar lo que habíamos anticipado:

Teorema 1.46 *Un módulo tiene longitud finita si y sólo si es noetheriano y artiniano.*

DEMOSTRACIÓN: Si un A-módulo M tiene longitud finita, entonces ha de ser noetheriano y artiniano, pues cualquier cadena estrictamente creciente o decreciente de submódulos ha de tener longitud menor que $l(M)$. Si M es noetheriano y artiniano a la vez, podemos construir como sigue una serie de composición:

Sea $M_0 = 0$. Si $M_0 \neq M$, tomamos como M_1 un submódulo minimal entre los submódulos que contienen estrictamente a M_0. (Existe porque M es artiniano). Así M_1/M_0 es simple. Si $M_1 \neq M$, tomamos como M_2 un submódulo minimal entre los submódulos que contienen estrictamente a M_1, con lo que M_2/M_1 es simple. Como M es noetheriano, la serie

$$M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots$$

no puede prolongarse indefinidamente, luego, tras un número finito de pasos, hemos de llegar a $M_n = M$ y así tenemos una serie de composición. ∎

El teorema 1.39 nos da ahora la consecuencia siguiente:

Teorema 1.47 *Si A es un anillo de longitud finita (por la izquierda o por la derecha), entonces todo A-módulo (izquierdo o derecho) finitamente generado tiene longitud finita.*

La conexión con la teoría de representaciones consiste en que si K es un cuerpo y G es un grupo finito, entonces la K-álgebra $K[G]$ tiene longitud finita (por la izquierda y por la derecha), pues sus ideales izquierdos y derechos son K-espacios vectoriales, luego una cadena estrictamente creciente o decreciente de ideales no puede tener longitud mayor que $|G|$.

Teorema 1.48 *Sea A un anillo y M un A-módulo (por la izquierda o por la derecha). Entonces M es simple si y sólo si es isomorfo a A/I, donde I es un ideal maximal (izquierdo o derecho) de A.*

Demostración: Consideremos el caso en que M es un A-módulo derecho. Por definición, I es un ideal maximal derecho si $I \subsetneq A$ y no existen ideales derechos $I \subsetneq J \subsetneq A$, lo que implica inmediatamente que A/I es un A-módulo simple. Recíprocamente, si M es un A-módulo simple, existe $m \in M$ no nulo. El homomorfismo $A \longrightarrow M$ dado por $a \mapsto ma$ tiene imagen no trivial, luego ha de ser suprayectivo, y su núcleo I (que es un submódulo derecho de A, es decir, un ideal derecho) ha de ser un ideal maximal derecho, pues el isomorfismo $A/I \cong M$ transformaría un ideal $I \subsetneq J \subsetneq A$ en un submódulo propio de M. ∎

Si A tiene longitud finita, la serie $0 \subset I \subsetneq A$ puede refinarse hasta una serie de composición de A, lo que muestra que A/I es un factor de composición de A. En definitiva, vemos que si A es un anillo de longitud finita, entonces todo A-módulo simple es isomorfo a un factor de composición de A. En particular, sólo hay un número finito de clases de isomorfismo de A-módulos simples.

Para terminar probamos que la longitud de los módulos de longitud finita es aditiva respecto a sucesiones exactas:

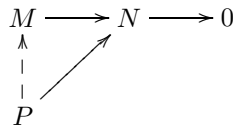
Teorema 1.49 *Si $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ es una sucesión exacta de módulos, entonces M tiene longitud finita si y sólo si la tienen M' y M'', en cuyo caso $l(M) = l(M') + l(M'')$.*

Demostración: Si M tiene longitud finita, la serie $0 \subset M' \subset M$ puede refinarse hasta una serie de composición (aquí suponemos que $0 \neq M' \neq M$, pues en caso contrario el teorema es obvio). Los términos intercalados entre 0 y M' forman una serie de composición de M', mientras que los intercalados entre M' y M determinan una serie de composición de M''. La relación entre las longitudes es obvia.

Recíprocamente, si M' y M'' tienen longitud finita, una serie de composición de M'' determina una serie con factores simples entre M' y M, que, unida a una serie de composición de M', da lugar a una serie de composición de M. ∎

Módulos proyectivos Los módulos proyectivos son —como veremos enseguida— una generalización de los módulos libres.

Definición 1.50 Sea A un anillo y P un A-módulo. Diremos que P es *proyectivo* si para todo epimorfismo de módulos $M \longrightarrow N$ y todo homomorfismo $P \longrightarrow N$ existe un homomorfismo que hace conmutativo el diagrama siguiente:



Dados dos A-módulos M y N, representaremos por $\mathrm{Hom}(M,N)$ al conjunto de todos los homomorfismos de A-módulos de M en N, que tiene estructura de grupo con la suma definida puntualmente. Si $\alpha : N \longrightarrow N'$ es un homomorfismo de A-módulos, la composición con α define claramente un homomorfismo de grupos $\alpha_\# : \mathrm{Hom}(M,N) \longrightarrow \mathrm{Hom}(M,N')$.

La definición de módulo proyectivo equivale a que $\alpha_\#$ es suprayectivo cuando α lo es. La situación general es la siguiente:

Teorema 1.51 *Si A es un anillo, $0 \longrightarrow N' \xrightarrow{\alpha} N \xrightarrow{\beta} N'' \longrightarrow 0$ es una sucesión exacta de A-módulos y M es un A-módulo, entonces la sucesión*

$$0 \longrightarrow \mathrm{Hom}(M,N') \xrightarrow{\alpha_\#} \mathrm{Hom}(M,N) \xrightarrow{\beta_\#} \mathrm{Hom}(M,N'') \longrightarrow 0$$

es exacta salvo quizá en $\mathrm{Hom}(M,N'')$. La exactitud en $\mathrm{Hom}(M,N'')$ (para toda sucesión exacta de partida) equivale a que M sea un A-módulo proyectivo.

La segunda parte es inmediata por la definición de módulo proyectivo. La primera parte se demuestra sin dificultad.[11]

El teorema siguiente nos proporciona una caracterización más descriptiva de los módulos proyectivos: son los sumandos directos de los módulos libres.

Teorema 1.52 *Sea A un anillo y M un A-módulo. Las afirmaciones siguientes son equivalentes:*

a) M es proyectivo.

b) Toda sucesión exacta de módulos $0 \longrightarrow C \xrightarrow{\beta} N \xrightarrow{\alpha} M \longrightarrow 0$ se escinde.

c) Existe un A-módulo M' tal que $M \oplus M'$ es libre.

Demostración:

a) $\Rightarrow$ b) Aplicamos la proyectividad a la identidad $M \longrightarrow M$, lo que nos da un homomorfismo $\gamma : M \longrightarrow N$. La escisión se debe a que si $n \in N$, entonces $\alpha(n - \gamma(\alpha(n)) = 0$, luego $b = n - \gamma(\alpha(n)) \in \mathrm{Im}\,\beta$ y $n = b + \gamma(\alpha(n))$. Por otra

[11] Véase el teorema 14.14 de mi libro de *Teoría de cuerpos de clases.*

parte, si $\beta(c) = \gamma(m)$, aplicando α obtenemos que $m = 0$, luego la suma es directa.

b) $\Rightarrow$ c) Podemos formar una sucesión exacta como la de b) con N libre. Entonces $N = \gamma[C] \oplus \gamma[M]$.

c) $\Rightarrow$ a) Consideremos un epimorfismo $\alpha : N \longrightarrow P$ y un homomorfismo $\beta : M \longrightarrow P$. Extendemos trivialmente β a $M \oplus M'$. Consideramos una base de este módulo y a cada uno de sus elementos le asignamos una antiimagen en N de su imagen en P. Esta asignación se extiende a un homomorfismo γ, el cual se restringe a su vez a un homomorfismo sobre M que cumple lo requerido. ∎

La condición c) implica en particular que todo módulo libre es proyectivo. En la prueba del teorema anterior se ve que si M es un módulo proyectivo finitamente generado, entonces el módulo M' tal que $M \oplus M'$ es libre se puede tomar también finitamente generado. También es obvio que la suma directa de módulos proyectivos es proyectiva y que todo sumando directo de un módulo proyectivo es proyectivo.

Muchas propiedades de los módulos libres pueden generalizarse a módulos proyectivos. Por ejemplo:

Teorema 1.53 *Sea G un grupo finito, sea $A \longrightarrow B$ un homomorfismo de anillos conmutativos, sean P, V dos $A[G]$-módulos finitamente generados, con P proyectivo. Entonces existe un isomorfismo natural de B-módulos*

$$\mathrm{Hom}(P, V) \otimes_A B \cong \mathrm{Hom}(P \otimes_A B, V \otimes_A B).$$

Demostración: Claramente tenemos un homomorfismo de B-módulos

$$\phi : \mathrm{Hom}(P, V) \otimes_A B \longrightarrow \mathrm{Hom}(P \otimes_A B, V \otimes_A B)$$

dado por $\phi(f \otimes b) = f \otimes m_b$, donde, $m_b : B \longrightarrow B$ es la multiplicación por b. Hemos de probar que es un isomorfismo. Supongamos en primer lugar que P es un $A[G]$-módulo libre de rango r, con lo que

$$P \otimes_A B \cong P \otimes_{A[G]} A[G] \otimes_A B \cong P \otimes_{A[G]} B[G]$$

es un $B[G]$-módulo libre de rango r. Entonces ϕ se descompone en una sucesión de isomorfismos:

$$\mathrm{Hom}(P, V) \otimes_A B \cong V^r \otimes_A B \cong (V \otimes_A B)^r \cong \mathrm{Hom}(P \otimes_A B, V \otimes_A B).$$

En el caso general, existe un $A[G]$-módulo P' tal que $L = P \oplus P'$ es libre. Tenemos un diagrama conmutativo

$$\begin{array}{ccc} \mathrm{Hom}(P, V)_B \oplus \mathrm{Hom}(P', V)_B & \longrightarrow & \mathrm{Hom}(P_B, V_B) \oplus \mathrm{Hom}(P'_B, V_B) \\ \downarrow & & \downarrow \\ \mathrm{Hom}(L, V)_B & \longrightarrow & \mathrm{Hom}(L_B, V_B) \end{array}$$

donde el subíndice B representa el producto $\otimes_A B$. Las flechas verticales son isomorfismos, la flecha horizontal inferior es un isomorfismo por la parte ya probada y la flecha horizontal superior es la suma directa $\phi_P + \phi_{P'}$ de los homomorfismos correspondientes a los módulos P y P'. Concluimos que ésta es también un isomorfismo y, por consiguiente, que también lo son ϕ_P y $\phi_{P'}$. ∎

Dejamos a cargo del lector la demostración del teorema siguiente, que es análoga a la del teorema anterior:

Teorema 1.54 *Sea A un anillo conmutativo y $G \longrightarrow H$ un homomorfismo de grupos finitos, sea P un $A[G]$-módulo proyectivo y V un $A[H]$-módulo finitamente generado. Entonces existe un isomorfismo natural de A-módulos*

$$\mathrm{Hom}_{A[G]}(P, V) \cong \mathrm{Hom}_{A[H]}(P \otimes_{A[G]} A[H], V).$$

Los módulos proyectivos cumplen una propiedad análoga al teorema 1.51 con productos tensoriales (aunque, en este caso, no es una caracterización de la proyectividad):

Teorema 1.55 *Si A es un anillo, $0 \longrightarrow N' \xrightarrow{\alpha} N \xrightarrow{\beta} N'' \longrightarrow 0$ es una sucesión exacta de A-módulos y M es un A-módulo, entonces la sucesión*

$$0 \longrightarrow M \otimes_A N' \xrightarrow{1\otimes\alpha} M \otimes_A N \xrightarrow{1\otimes\beta} M \otimes_A N'' \longrightarrow 0$$

es exacta salvo quizá en $M \otimes_A N'$. Si M es proyectivo también es exacta en dicho grupo.

Demostración: La exactitud en $M \otimes_A N''$ es trivial, al igual que el hecho de que $\mathrm{Im}(1 \otimes \alpha) \subset \mathrm{N}(1 \otimes \beta)$. Para probar la inclusión opuesta llamamos $H = \mathrm{Im}(1\otimes\alpha)$. Puesto que $H \subset \mathrm{N}(1\otimes\beta)$, la aplicación $1\otimes\beta$ induce un homomorfismo $\phi : (M \otimes_A N)/H \longrightarrow M \otimes_A N''$ que cumple $\phi([m \otimes n]) = m \otimes \beta(n)$.

Por otra parte, la aplicación $m \otimes \beta(n) \mapsto [m \otimes n]$ está bien definida y es inversa de ϕ, luego ϕ es un isomorfismo y, por consiguiente, $\mathrm{N}(1 \otimes \beta)/H = 0$.

Nos falta probar que si M es proyectivo entonces $1 \otimes \alpha$ es inyectivo. Esto es claro si M es un A-módulo libre, pues entonces $M \cong \bigoplus_{i\in I} A$, con lo que

$$M \otimes_A N' \cong \bigoplus_{i\in I} A \otimes_A N' \cong \bigoplus_{i\in I} N',$$

e igualmente

$$M \otimes_A N \cong \bigoplus_{i\in I} N,$$

de modo que $1 \otimes \alpha$ coincide con el monomorfismo natural

$$\bigoplus_{i\in I} N' \longrightarrow \bigoplus_{i\in I} N$$

inducido por α. En el caso general, podemos considerar un A-módulo M' tal que $M \oplus M'$ sea libre. Tenemos un diagrama conmutativo

$$\begin{array}{ccc} (M \oplus M') \otimes_A N' & \xrightarrow{1\otimes\alpha} & (M \oplus M') \otimes_A N \\ \uparrow & & \uparrow \\ (M \otimes_A N') \oplus (M' \otimes_A N') & \longrightarrow & (M \otimes_A N) \oplus (M' \otimes_A N) \end{array}$$

donde las flechas verticales son isomorfismos. La fila superior es inyectiva por el caso ya probado, luego también lo es la fila inferior y, en particular, su restricción a $M \otimes_A N'$, que es $1 \otimes \alpha$. ∎

Es bien conocido que si M es un A-módulo (finitamente generado) existe un grupo libre P (finitamente generado) y un epimorfismo $f : P \longrightarrow M$. Obviamente, esto es cierto en particular si cambiamos "libre" por "proyectivo", pero, en el caso de anillos artinianos, este cambio nos permite precisar la elección de P hasta hacerla canónica:

Definición 1.56 Si A es un anillo, diremos que un homomorfismo de A-módulos $f : P \longrightarrow M$ es *esencial* si $f[P] = M$ y $f[M'] \neq M$ para todo submódulo $M' \subsetneq P$. Una *envoltura proyectiva* de un A-módulo M es un homomorfismo esencial $f : P \longrightarrow M$, donde P es proyectivo.

Teorema 1.57 *Si A es un anillo artiniano y M es un A-módulo finitamente generado, entonces M tiene una envoltura proyectiva, que es única salvo isomorfismo, y es un A-módulo finitamente generado.*

Demostración: Sea $f : L \longrightarrow M$ un epimorfismo de A-módulos, donde L es un A-módulo libre finitamente generado. Sea N su núcleo. Para cada submódulo $N' \subset N$, consideremos el epimorfismo canónico

$$f_{N'} : L/N' \longrightarrow L/N \longrightarrow M.$$

Observemos que $f_N : L/N \longrightarrow M$ es un homomorfismo esencial (porque es un isomorfismo) y, como L es un A-módulo artiniano, podemos tomar un $N' \subset N$ minimal para la propiedad de que $f_{N'} : L/N' \longrightarrow M$ sea esencial. Llamemos $P = L/N'$. Vamos a probar que P es proyectivo, con lo que será una envoltura proyectiva de M. Claramente es un A-módulo finitamente generado.

Consideremos el epimorfismo canónico $p : L \longrightarrow P$. Usando de nuevo que L es artiniano, podemos considerar un submódulo $Q \subset L$ que sea minimal respecto a la propiedad de que $p|_Q : Q \longrightarrow P$ sea suprayectiva. Como L es proyectivo, existe un homomorfismo $q : L \longrightarrow Q$ que hace conmutativo el diagrama siguiente:

$$\begin{array}{ccccc} Q & \xrightarrow{p} & P & \longrightarrow & 0 \\ {\scriptstyle q}\uparrow & \nearrow_{\pi} & & & \\ L & & & & \end{array}$$

Este q ha de ser suprayectivo pues, en caso contrario, el submódulo $q[L] \subset Q$ contradiría la minimalidad de Q. Sea $N'' \subset N' \subset L$ el núcleo de q. Ahora consideramos el diagrama conmutativo

$$\begin{array}{ccc} L/N'' & \xrightarrow{f_{N''}} & L/N \\ & \searrow^{p} & \uparrow{\scriptstyle f_{N'}} \\ & & L/N' \end{array} \qquad \text{o, equivalentemente,} \qquad \begin{array}{ccc} Q & \xrightarrow{f_{N''}} & M \\ & \searrow^{p} & \uparrow{\scriptstyle f_{N'}} \\ & & P \end{array}$$

y observamos que tanto p como $f_{N'}$ son esenciales, luego $f_{N''}$ también lo es. La minimalidad de N' implica entonces que $N'' = N'$, luego p es un isomorfismo. Esto significa que la sucesión exacta

$$0 \longrightarrow N' \longrightarrow L \longrightarrow P \longrightarrow 0$$

se escinde, luego $L \cong N' \oplus Q \cong N' \oplus P$, y esto prueba que P es proyectivo.

Veamos ahora la unicidad. Si $P' \longrightarrow M$ es otra envoltura proyectiva, la proyectividad de P nos da un homomorfismo g que cierra el diagrama siguiente:

$$\begin{array}{ccccc} P' & \longrightarrow & M & \longrightarrow & 0 \\ {\scriptstyle g}\uparrow & \nearrow & & & \\ P & & & & \end{array}$$

Como $P' \longrightarrow M$ es esencial, ha de ser $g[P] = P'$, luego g es un epimorfismo. Como P' es proyectivo, la sucesión exacta

$$0 \longrightarrow \mathrm{N}(g) \longrightarrow P \longrightarrow P' \longrightarrow 0$$

se escinde, luego $P = \mathrm{N}(g) \oplus P'$ y, como $P \longrightarrow M$ es esencial, ha de ser $\mathrm{N}(g) = 0$, luego g es un isomorfismo. ∎

Terminaremos con un resultado que necesitaremos más adelante sobre $k[G]$-módulos proyectivos:

Teorema 1.58 *Sea G un grupo finito, k un cuerpo y P, V dos $k[G]$-módulos finitamente generados. Si P es proyectivo, entonces $P \otimes_k V$ es proyectivo.*

Demostración: Existe un $k[G]$-módulo libre finitamente generado L tal que $L = P \oplus C$, para cierto $k[G]$-submódulo C de L. Entonces

$$L \otimes_k V = (P \otimes_k V) \oplus (C \otimes_k V),$$

y basta probar que $L \otimes_k V$ es libre. A su vez, podemos descomponer L en suma directa de submódulos isomorfos a $k[G]$, con lo que basta probar que $k[G] \otimes_k V$ es libre.

Si $v_1, \ldots, v_n$ es una base de V como k-espacio vectorial, sabemos que $\sigma \otimes v_i$ (donde σ recorre G) es una k-base de $k[G] \otimes_k V$. Basta probar que $1 \otimes v_i$ es una $k[G]$-base de $k[G] \otimes V$.

Como $\sigma\otimes v_i = (1\otimes(v_i\sigma^{-1}))\sigma$ y $v_i\sigma^{-1}$ es combinación lineal de los v_i, es claro que los tensores $1\otimes v_i$ son un sistema generador de $k[G]\otimes V$ como $k[G]$-módulo. Supongamos ahora que

$$\sum_i (1\otimes v_i)x_i = 0,$$

donde $x_i = \sum_{\sigma\in G} \alpha_i^\sigma \sigma \in k[G]$. Entonces

$$\sum_i (1\otimes v_i)x_i = \sum_i x_i\otimes v_i x_i = \sum_{i,\sigma} \alpha_i^\sigma\sigma\otimes\alpha_i^\sigma v_i\sigma$$

$$= \sum_{i,\sigma}(\alpha_i^\sigma)^2(\sigma\otimes\sum_j \beta_{ij}^\sigma v_j) = \sum_{i,\sigma,j}(\alpha_i^\sigma)^2\beta_{ij}^\sigma(\sigma\otimes v_j),$$

donde (β_{ij}^σ) es la matriz en la base v_i del automorfismo $v\mapsto v\sigma$. Por consiguiente, para todo j, σ,

$$\sum_i (\alpha_i^\sigma)^2\beta_{ij}^\sigma = 0.$$

Para cada $\sigma\in G$ fijo, esto equivale a la ecuación matricial $((\alpha_i^\sigma)^2)(\beta_{ij}^\sigma) = 0$. Como la matriz (β_{ij}^σ) tiene inversa, esto implica que $\alpha_i^\sigma = 0$ para todo i, σ, luego $x_i = 0$ para todo i. ∎

1.4 Módulos de homomorfismos

En esta sección G será un grupo finito y k un cuerpo. Claramente, todo $k[G]$-módulo tiene una estructura natural de k-espacio vectorial, de modo que si V y W son dos $k[G]$-módulos, podemos distinguir entre el grupo $\mathrm{Hom}_G(V,W)$ de los homomorfismos de $k[G]$-módulos de $V\longrightarrow W$ y el grupo $\mathrm{Hom}_k(V,W)$ de las aplicaciones lineales $V\longrightarrow W$. Ambos tienen una estructura natural de k-espacio vectorial con el producto definido puntualmente. De hecho, el primero es un subespacio del segundo.

Más aún, si V y W son $k[G]$-módulos, podemos dotar a $\mathrm{Hom}_k(V,W)$ de estructura de $k[G]$-módulo con el producto dado por

$$(f\sigma)(v) = f(v\sigma^{-1})\sigma,$$

para todo $f\in\mathrm{Hom}_k(V,W)$, $\sigma\in G$, $v\in V$.

Observemos que si, en general, para cada $k[G]$-módulo M, definimos el $K[G]$-submódulo

$$M^G = \{m\in M \mid m\sigma = m \text{ para todo } \sigma\in G\},$$

se cumple que

$$\mathrm{Hom}_G(V,W) = \mathrm{Hom}_k(V,W)^G.$$

El siguiente caso particular tiene especial interés:

Definición 1.59 Definimos el $k[G]$-módulo *dual* de un $k[G]$-módulo V como $V^* = \mathrm{Hom}_k(V,k)$, donde consideramos a k como un $k[G]$-módulo trivial, es decir, con el producto dado por $\alpha\sigma = \alpha$, para todo $\alpha\in k$ y todo $\sigma\in G$. Así, el producto en V^* viene dado por $(f\sigma)(v) = f(v\sigma^{-1})$.

Si $\alpha : V \longrightarrow W$ es un homomorfismo de $k[G]$-módulos, la composición con α determina un *homomorfismo dual* $\alpha^* : W^* \longrightarrow V^*$. El teorema siguiente se demuestra sin dificultad:

Teorema 1.60 *Si* $0 \longrightarrow V' \xrightarrow{\alpha} V \xrightarrow{\beta} V'' \longrightarrow 0$ *es una sucesión exacta de* $k[G]$*-módulos, entonces la sucesión*

$$0 \longrightarrow V''^* \xrightarrow{\beta^*} V^* \xrightarrow{\alpha^*} V'^* \longrightarrow 0$$

también es exacta.

Si V es un $k[G]$-módulo finitamente generado, entonces es también un k-espacio vectorial de dimensión finita, y se cumple que $\dim_k V = \dim_k V^*$. En efecto, si $v_1, \dots, v_n$ es una k-base de V, es fácil ver que una k-base de V^* es la *base dual* $v_1^*, \dots, v_n^*$ dada por

$$v_i^*(v_j) = \begin{cases} 1 & \text{si } i = j, \\ 0 & \text{si } i \neq j. \end{cases}$$

En particular V y V^* son isomorfos como k-espacios vectoriales, si bien el isomorfismo no es canónico, sino que tenemos un isomorfismo distinto para cada elección de una base en V. Por el contrario, (siempre bajo la hipótesis de que sea finitamente generado) V es canónicamente isomorfo (incluso como $k[G]$-módulo) a su bidual. Un isomorfismo $\phi : V \longrightarrow V^{**}$ independiente de la elección de bases es el dado por $\phi(v)(f) = f(v)$. En efecto, es fácil ver que si $v_1, \dots, v_n$ es cualquier base de V, entonces $\phi(v_i) = v_i^{**}$, lo que prueba que ϕ es un isomorfismo de espacios vectoriales. Se trata de un isomorfismo de módulos porque

$$\phi(v\sigma)(f) = f(v\sigma) = (f\sigma^{-1})(v) = \phi(v)(f\sigma^{-1}) = (\phi(v)\sigma)(f),$$

luego $\phi(v\sigma) = \phi(v)\sigma$.

Teorema 1.61 *Si* V *y* W *son dos* $k[G]$*-módulos finitamente generados, entonces*

$$(V \oplus W)^* \cong V^* \oplus W^*, \qquad (V \otimes_k W)^* \cong V^* \otimes_k W^*.$$

Demostración: Se comprueba sin dificultad que $f \mapsto (f|_V, f|_W)$ determina un isomorfismo de $k[G]$-módulos entre el dual de la suma y la suma de los duales. Para el producto tensorial definimos $\phi : V^* \otimes_k W^* \longrightarrow (V \otimes_k W)^*$ mediante

$$\phi(f \otimes g)(v \otimes w) = f(v)g(w).$$

Se trata de un homomorfismo de módulos, pues

$$\phi((f\otimes g)\sigma)(v\otimes w) = \phi((f\sigma)\otimes(g\sigma))(v\otimes w) = (f\sigma)(v)(g\sigma)(w) = f(v\sigma^{-1})g(w\sigma^{-1})$$

$$= \phi(f \otimes g)((v\sigma^{-1}) \otimes (w\sigma^{-1})) = \phi(f \otimes g)((v \otimes w)\sigma^{-1}) = (\phi(f \otimes g)\sigma)(v \otimes w),$$

luego $\phi((f \otimes g)\sigma) = \phi(f \otimes g)\sigma$.

Por otra parte, si $v_1, \ldots, v_n$ y $w_1, \ldots, w_m$ son bases de V y W respectivamente, se cumple que $v_i^* \otimes w_j^*$ es una base de $V^* \otimes_k W^*$, y es claro que $\phi(v_i^* \otimes w_j^*) = (v_i \otimes w_j)^*$, por lo que ϕ es un isomorfismo de espacios vectoriales, y también, por tanto, un isomorfismo de módulos. ∎

Ahora podemos relacionar los módulos de homomorfismos con el producto tensorial:

Teorema 1.62 *Si V, W son dos $k[G]$-módulos finitamente generados, tenemos un isomorfismo natural de $k[G]$-módulos*

$$\mathrm{Hom}_k(V, W) \cong V^* \otimes_k W.$$

Demostración: Definimos $\phi : V^* \otimes_k W \longrightarrow \mathrm{Hom}_k(V, W)$ mediante

$$\phi(f \otimes w)(v) = f(v)w.$$

Veamos que es un homomorfismo de $k[G]$-módulos:

$$\phi((f \otimes w)\sigma)(v) = \phi((f\sigma) \otimes (w\sigma))(v) = (f\sigma)(v)w\sigma$$

$$= f(v\sigma^{-1})w\sigma = \phi(f \otimes w)(v\sigma^{-1})\sigma = (\phi(f \otimes w)\sigma)(v).$$

Se trata de un isomorfismo, pues si $v_1, \ldots, v_n$ y $w_1, \ldots, w_m$ son bases de V y W, respectivamente, los tensores $v_i^* \otimes w_j$ forman una base de $V^* \otimes_k W$, y es fácil ver que los homomorfismos $\phi(v_i^* \otimes w_j)$ forman una base de $\mathrm{Hom}_k(V, W)$. ∎

Con esto podemos probar que la dualización de un módulo de homomorfismos equivale a permutar los módulos:

Teorema 1.63 *Si V, W son dos $k[G]$-módulos finitamente generados, entonces*

$$\mathrm{Hom}_k(V, W)^* \cong \mathrm{Hom}_k(W, V).$$

Demostración: Aplicando los resultados precedentes obtenemos que

$$\mathrm{Hom}_k(V, W)^* \cong (V^* \otimes_k W)^* \cong V^{**} \otimes_k W^* \cong V \otimes_k W^*$$

$$\cong W^* \otimes_k V \cong \mathrm{Hom}_k(W, V).$$

∎

Teorema 1.64 *Si V es un $k[G]$-módulo finitamente generado, entonces V es libre o proyectivo si y sólo si lo es V^*.*

Demostración: Teniendo en cuenta que $V \cong V^{**}$, sólo hemos de probar una implicación. Tratemos primero el caso en que $V = k[G]$. Consideramos entonces el isomorfismo de espacios vectoriales $\phi : k[G] \longrightarrow k[G]^*$ dado por $\phi(\sigma) = \sigma^*$. Vamos a probar que es un isomorfismo de $k[G]$-módulos. En efecto,

$$(\phi(\sigma)\tau)(\rho) = (\sigma^*\tau)(\rho) = \sigma^*(\rho\tau^{-1}) = \begin{cases} 1 & \text{si } \rho\tau^{-1} = \sigma, \\ 0 & \text{si } \rho\tau^{-1} \neq \sigma, \end{cases}$$

luego $\phi(\sigma)\tau = (\sigma\tau)^* = \phi(\sigma\tau)$.

Por consiguiente, si V es un $k[G]$-módulo libre por la derecha, tenemos que $V \cong k[G] \oplus \cdots \oplus k[G]$, y es claro entonces que

$$V^* \cong k[G]^* \oplus \cdots \oplus k[G]^* \cong k[G] \oplus \cdots \oplus k[G],$$

donde en la última suma directa consideramos a $k[G]$ como módulo por la izquierda.

Por último, si V es proyectivo, entonces existe un $K[G]$-módulo W (finitamente generado) tal que $V \oplus W$ es libre, y entonces $(V \oplus W)^* \cong V^* \oplus W^*$ es libre también, luego V^* es proyectivo. ∎

Teorema 1.65 *Si V es un $k[G]$-módulo finitamente generado que genera el carácter χ, entonces, el carácter χ^* de V^* viene dado por $\chi^*(\sigma) = \chi(\sigma^{-1})$.*

Demostración: Sea $v_1, \ldots, v_n$ una k-base de V. Dado $\sigma \in G$, sea $A = (a_{ij})$ la matriz de la multiplicación por σ^{-1} en dicha base y sea (a^*_{ij}) la matriz de la multiplicación por σ en la base $v_1^*, \ldots, v_n^*$ de V^*. Tenemos que

$$v_i\sigma^{-1} = \sum_j a_{ij}v_j, \qquad v_i^*\sigma = \sum_j a^*_{ij}v_j^*,$$

luego $a^*_{ii} = (v_i^*\sigma)(v_i) = v_i^*(v_i\sigma^{-1}) = a_{ii}$. Sumando para todo i obtenemos que $\chi^*(\sigma) = \chi(\sigma^{-1})$. ∎

Dedicamos el resto de la sección a demostrar el teorema siguiente:

Teorema 1.66 *Si P, Q son dos $k[G]$-módulos finitamente generados y P es proyectivo,*

$$\dim_k \mathrm{Hom}_G(P, Q) = \dim_k \mathrm{Hom}_G(Q, P).$$

Observemos que el teorema 1.64 implica que P^* también es proyectivo, luego los teoremas 1.58 y 1.62 implican que $\mathrm{Hom}_k(P, Q)$ también lo es. A su vez, el teorema 1.63 reduce entonces la prueba del teorema 1.66 a demostrar lo siguiente:

Teorema 1.67 *Si V es un $k[G]$-módulo proyectivo finitamente generado,*

$$\dim_k V^G = \dim_k V^{*G}.$$

En efecto, en las condiciones de 1.66, tomamos $V = \mathrm{Hom}_k(P, Q)$, que es un $k[G]$-módulo proyectivo, al igual que $V^* \cong \mathrm{Hom}_k(Q, P)$ (por 1.63 y 1.64). Por consiguiente, $V^G = \mathrm{Hom}_G(P, Q)$ y

$$V^{*G} \cong \mathrm{Hom}_k(Q, P)^G = \mathrm{Hom}_G(Q, P).$$

∎

Para probar 1.67 definimos

$$T = \sum_{\sigma \in G} \sigma \in k[G], \quad I = \langle T \rangle_k, \quad J = \langle \sigma - 1 \mid \sigma \in G \rangle_k.$$

Es inmediato que los subespacios vectoriales I, J son, de hecho, ideales biláteros de $k[G]$. Para cada $k[G]$-módulo M, definimos $M_G = M/MJ$. El teorema 1.67 es consecuencia inmediata del teorema siguiente:

Teorema 1.68 *Si V es un $k[G]$-módulo proyectivo finitamente generado, existen isomorfismos naturales*

$$V_G \cong V^G, \qquad (V^*)_G \cong (V^G)^*.$$

En efecto, admitiendo esto concluimos que

$$\dim_k V^G = \dim_k (V^G)^* = \dim_k (V^*)_G = \dim_k (V^*)^G.$$

Para probar 1.68 observamos en primer lugar que $k[G]^G = I = k[G]I$. En efecto, si $x = \sum a_\sigma \sigma \in k[G]^G$, comparando coeficientes en la igualdad $x\tau^{-1} = x$ vemos que $a_\tau = a_1$ para todo $\tau \in G$, luego $x = a_1 T \in I$.

Esto implica a su vez que si L es un $k[G]$-módulo libre, $L^G = LI = LT$. Basta descomponer L en suma directa de copias de $k[G]$. Si V es proyectivo, entonces existe otro $k[G]$-módulo W tal que $V \oplus W$ es libre, con lo que

$$V^G \oplus W^G = (V \oplus W)^G = (V \oplus W)I = VI \oplus WI,$$

luego $V^G = VI$.

Ahora consideramos la sucesión exacta de $k[G]$-módulos

$$0 \longrightarrow J \longrightarrow k[G] \xrightarrow{\phi} k \longrightarrow 0,$$

donde consideramos a k como $k[G]$-módulo trivial y ϕ viene dado por $\sigma \mapsto 1$. La sucesión es exacta porque J está claramente contenido en el núcleo de ϕ, y ambos subespacios tienen dimensión igual a $|G| - 1$. Si V es un $k[G]$-módulo proyectivo, el teorema 1.55 nos da la sucesión exacta de $k[G]$-módulos

$$0 \longrightarrow VJ \longrightarrow V \longrightarrow V \otimes_{k[G]} k \longrightarrow 0.$$

Por consiguiente,

$$V_G = V/VJ \cong V \otimes_{k[G]} k \cong VT = V^G.$$

En efecto, el homomorfismo de $k[G]$-módulos $\psi : V \otimes_{k[G]} k \longrightarrow VT$ dado por $v \otimes \alpha = vT\alpha$ es un isomorfismo, ya que tiene por inverso al dado por $vT \mapsto v \otimes 1$. Éste está bien definido pues, si $vT = v'T$, entonces $(v - v')T = 0$, luego

$$(v \otimes 1) - (v' \otimes 1) = (v - v') \otimes 1 = (v - v') \otimes T1 = (v - v')T \otimes 1 = 0.$$

Con esto tenemos probada la primera parte de 1.68. Para la segunda empezamos observando que

$$k[G]^* J = \langle \sigma^* - 1^* \mid \sigma \in G \rangle_k .$$

En efecto, es fácil ver que

$$\sigma^*(\tau - 1) = (\sigma\tau)^* - \sigma^* = ((\sigma\tau)^* - 1^*) - (\sigma^* - 1^*),$$

lo que nos da una inclusión y, en particular,

$$1^*(\tau - 1) = \tau^* - 1^*,$$

lo que nos da la otra inclusión. Por lo tanto, $\dim_k k[G]^*J = |G| - 1$, y esto implica la exactitud de la sucesión

$$0 \longrightarrow k[G]^*J \longrightarrow k[G]^* \longrightarrow I^* \longrightarrow 0,$$

donde el epimorfismo es el dual de la inclusión $I \longrightarrow k[G]$. Si L es un $k[G]$-módulo libre finitamente generado, entonces L^* es suma directa de un número finito de copias de $k[G]^*$, de donde se sigue la exactitud de la sucesión

$$0 \longrightarrow L^*J \longrightarrow L^* \longrightarrow (L^G)^* \longrightarrow 0.$$

Finalmente, si V es un $k[G]$-módulo proyectivo, tomamos W tal que $V \oplus W$ sea libre y tenemos la sucesión exacta

$$0 \longrightarrow V^*J \oplus W^*J \longrightarrow V^* \oplus W^* \longrightarrow (V^G)^* \oplus (W^G)^* \longrightarrow 0,$$

de donde se sigue la exactitud de

$$0 \longrightarrow V^*J \longrightarrow V^* \longrightarrow (V^G)^* \longrightarrow 0.$$

Por consiguiente,

$$(V^*)_G = V^*/V^*J \cong (V^G)^*,$$

lo que termina la prueba de 1.68 y, por lo tanto, de 1.66. ∎

Capítulo II

Teoría de caracteres

En este capítulo desarrollaremos la teoría de representaciones ordinarias de grupos finitos, es decir, que estudiaremos las representaciones sobre cuerpos de característica 0 y, más concretamente, sobre cuerpos algebraicamente cerrados. La característica más notable de este caso es que las representaciones están completamente determinadas por sus caracteres.

2.1 Caracteres

Presentamos aquí los resultados básicos sobre los caracteres de las representaciones ordinarias de grupos finitos:

NOTA: *En esta sección sobrentenderemos que el cuerpo de coeficientes K sobre el que consideramos las representaciones es algebraicamente cerrado y de característica* 0.

Entre otras cosas, veremos que los caracteres no dependen del cuerpo K considerado (en las condiciones indicadas). Esto nos permitirá, en las secciones posteriores, restringirnos al caso $K = \mathbb{C}$ sin pérdida de generalidad. Más concretamente, el hecho de que K tenga característica 0 se traduce en que $\mathbb{Q} \subset K$ y, como K es algebraicamente cerrado, contiene a la clausura algebraica $\mathbb{A}$ de $\mathbb{Q}$. Probaremos que todas las representaciones matriciales de G en K son isomorfas a representaciones sobre $\mathbb{A}$.

Teorema 2.1 *Si $\rho : G \longrightarrow \mathrm{Aut}(V)$ es una representación y $\sigma \in G$, entonces V admite una base formada por vectores propios de $\rho(\sigma)$, y los valores propios son raíces $|G|$-ésimas de la unidad.*

Demostración: Restringiendo ρ al subgrupo generado por σ, podemos suponer que G está generado por σ. Como K es algebraicamente cerrado, el automorfismo $\rho(\sigma)$ tiene al menos un valor propio $\alpha_1 \in K$ (una raíz de su polinomio característico). Sea $v_1 \in V$ un vector propio asociado a α_1, de modo

que $v_1\sigma = \alpha_1 v_1$ y, en general, $v_1\sigma^n = \alpha_1^n v_1$. Así pues, $W_1 = \langle v_1 \rangle$ es un $K[G]$-submódulo. Por 1.12 podemos descomponer $V = W_1 \oplus V_1$, donde V_1 es también un $K[G]$-submódulo.

Repitiendo el mismo razonamiento con V_1 podemos encontrar un $K[G]$-submódulo $W_2 = \langle v_2 \rangle$ y una descomposición $V = W_1 \oplus W_2 \oplus V_2$. Tras un número finito de pasos llegamos a una descomposición $V = W_1 \oplus \cdots \oplus W_n$ en $K[G]$-submódulos de la forma $W_i = \langle v_i \rangle$, donde cada v_i es obviamente un vector propio de $\rho(\sigma)$.

La matriz de $\rho(\sigma)$ en esta base es diagonal, y los elementos de la diagonal son sus valores propios α_i. Si $n = |G|$, se cumple que $\sigma^n = 1$, luego $\alpha_i^n = 1$, luego los valores propios α_i son raíces n-simas de la unidad. ∎

En general no es posible elegir una base de V tal que la matriz de $\rho(\sigma)$ sea diagonal simultáneamente para todo $\sigma \in G$, pero, como la traza $\chi(\sigma)$ se puede calcular a partir de la matriz de $\rho(\sigma)$ en cualquier base, concluimos que

$$\chi(\sigma) = \epsilon_1 + \cdots + \epsilon_n,$$

donde los números $\epsilon_i \in K$ son raíces $|G|$-ésimas de la unidad y, en particular, son enteros algebraicos (es decir, que son raíces de polinomios mónicos con coeficientes enteros). Conviene destacar este hecho:

Teorema 2.2 *Los valores que toman los caracteres de los grupos finitos son enteros algebraicos.*

En particular, los caracteres pueden verse como aplicaciones $\chi : G \longrightarrow \mathbb{A}$ (aunque todavía no podemos asegurar que las representaciones matriciales que los generan tengan necesariamente sus coeficientes en $\mathbb{A}$). Observemos que en $\mathbb{A} \subset \mathbb{C}$ podemos considerar la conjugación compleja, que representaremos con una barra, como es habitual.

Teorema 2.3 *Si $\chi : G \longrightarrow \mathbb{A}$ es un carácter de un grupo finito G, entonces, para todo $\sigma \in G$, se cumple que $\chi(\sigma^{-1}) = \overline{\chi(\sigma)}$.*

Demostración: Sea $\rho : G \longrightarrow \mathrm{Aut}(V)$ una representación que genere el carácter dado. Según 2.1, podemos elegir una base de V en la que $\rho(\sigma)$ admite una matriz diagonal (α_{ij}) cuya diagonal está formada por raíces de la unidad, que son elementos de $\mathbb{A}$ de módulo 1. Entonces

$$\chi(\sigma^{-1}) = \sum_i \alpha_{ii}^{-1} = \sum_i \bar{\alpha}_{ii} = \overline{\chi(\sigma)}.$$

∎

Como tercera aplicación de 2.1 mostramos que un carácter determina el núcleo de la representación que lo genera:

Definición 2.4 Si $\chi : G \longrightarrow \mathbb{A}$ es un carácter de un grupo finito G, llamaremos *núcleo* de χ al conjunto

$$\mathrm{N}(\chi) = \{\sigma \in G \mid \chi(\sigma) = \chi(1)\}.$$

Teorema 2.5 *Si $\rho : G \longrightarrow \mathrm{Aut}(G)$ es una representación de un grupo finito G y χ es el carácter que determina, entonces el núcleo de χ es el núcleo de ρ.*

DEMOSTRACIÓN: Evidentemente, $\sigma \in G$ está en el núcleo de ρ si y sólo si $\rho(\sigma) = I_n$, donde n es el grado de la representación, luego, en tal caso, se cumple que $\chi(\sigma) = n = \chi(1)$. Recíprocamente, si $\chi(\sigma) = n$, sabemos que, en una base adecuada, $\rho(\sigma)$ se corresponde con una matriz diagonal y $\chi(\sigma) = \epsilon_1 + \cdots + \epsilon_n$ es la suma de dicha diagonal. Los ϵ_i pueden verse como números complejos de módulo 1, luego la parte real de cada uno de ellos es ≤ 1. Para que la suma dé n es necesario que todas las partes reales sean 1, lo cual implica que $\epsilon_i = 1$ y, por consiguiente, que $\rho(\sigma) = I_n$, de modo que σ está en el núcleo de ρ. ∎

Definición 2.6 Si G es un grupo finito, N es un subgrupo normal, para cada carácter $\chi : G/N \longrightarrow \mathbb{A}$ de G/N definimos el carácter $\hat{\chi} : G \longrightarrow \mathbb{A}$ dado por $\hat{\chi}(\sigma) = \chi(\sigma N)$.

Se trata ciertamente de un carácter porque si $\rho : G/N \longrightarrow \mathrm{Aut}(V)$ es la representación que determina χ, entonces la composición $G \longrightarrow G/N \longrightarrow \mathrm{Aut}(V)$ es una representación de G que genera $\hat{\chi}$.

Es claro que χ es irreducible si y sólo si lo es $\hat{\chi}$. Además, tenemos que $N \leq \mathrm{N}(\hat{\chi})$. Recíprocamente, es claro que todo carácter ψ de G que cumpla $N \leq \mathrm{N}(\psi)$ es de la forma $\psi = \hat{\chi}$, para cierto carácter $\chi : G/N \longrightarrow \mathbb{A}$.

En vista de esto, en lo sucesivo identificaremos los caracteres de un grupo cociente G/N con los caracteres de G cuyo núcleo contiene a N.

Las propiedades fundamentales de los caracteres se deducen del teorema siguiente:

Teorema 2.7 (Lema de Schur) *Sean $\rho_i : G \longrightarrow \mathrm{Aut}(V_i)$, para $i = 1, 2$ dos representaciones irreducibles de un grupo finito G y sea $f : V_1 \longrightarrow V_2$ un homomorfismo de $K[G]$-módulos. Si las representaciones no son isomorfas, se cumple que $f = 0$ y, si $V_1 = V_2$ y $\rho_1 = \rho_2$, entonces existe un $\alpha \in K$ tal que $f(v) = \alpha v$, para todo $v \in V_1$.*

DEMOSTRACIÓN: Si $f \neq 0$, el núcleo de V_1 ha de ser un $K[G]$-submódulo distinto de V_1, luego ha de ser trivial, y la imagen ha de ser un $K[G]$-submódulo no trivial de V_2, luego ha de ser todo V_2. Esto prueba que f es un isomorfismo y las representaciones son isomorfas.

Si suponemos que ambas representaciones son la misma, sea $\alpha \in K$ un valor propio de f (aquí usamos que K es algebraicamente cerrado). Sea $f' : V_1 \longrightarrow V_1$ la aplicación lineal dada por $f'(v) = f(v) - \alpha v$. Es claro que es un homomorfismo de $K[G]$-módulos que y su núcleo no es trivial (porque contiene a los vectores propios asociados a α) luego, por la parte ya probada, $f' = 0$, luego $f(v) = \alpha v$ para todo $v \in V_1$. ∎

Para extraer consecuencias del lema de Schur conviene introducir la notación siguiente:

Definición 2.8 Si G es un grupo finito, representamos por K^G al conjunto de funciones $\phi : G \longrightarrow K$. Definimos en K^G la forma bilineal simétrica

$$\langle \phi, \psi \rangle = \frac{1}{|G|} \sum_{\sigma \in G} \phi(\sigma)\psi(\sigma^{-1}).$$

Teorema 2.9 (Relaciones de ortogonalidad) *Si χ_1 y χ_2 son dos caracteres irreducibles de un grupo finito G, entonces*

$$\langle \chi_1, \chi_2 \rangle = \begin{cases} 1 & si\ \chi_1 = \chi_2, \\ 0 & si\ \chi_1 \neq \chi_2. \end{cases}$$

DEMOSTRACIÓN: Sean $\rho_i : G \longrightarrow \mathrm{Aut}(V_i)$ representaciones que generen los caracteres χ_i. Sea $h : V_1 \longrightarrow V_2$ una aplicación lineal arbitraria y sea $h^0 : V_1 \longrightarrow V_2$ la aplicación lineal dada por

$$h^0(v) = \frac{1}{|G|} \sum_{\sigma \in G} h(v\sigma)\sigma^{-1}.$$

Se cumple que h^0 es un homomorfismo de $K[G]$-módulos, pues

$$h^0(v\tau) = \frac{1}{|G|} \sum_{\sigma \in G} h(v\tau\sigma)\sigma^{-1} = \left(\frac{1}{|G|} \sum_{\sigma \in G} h(v\tau\sigma)(\tau\sigma)^{-1} \right) \tau = h^0(v)\tau.$$

Fijemos bases de ambos espacios vectoriales, sean $(r^1_{ij}(\sigma))$, $(r^2_{ij}(\sigma))$ las matrices de $\rho_i(\sigma)$ en las bases respectivas y sean (x_{ij}), (x^0_{ij}) las matrices de h y h^0, respectivamente. Entonces,

$$x^0_{ij} = \frac{1}{|G|} \sum_{\sigma,k,l} r^1_{ik}(\sigma) x_{kl} r^2_{lj}(\sigma^{-1}).$$

Si $\chi_1 \neq \chi_2$, las representaciones no son isomorfas, luego, según el lema de Schur, ha de ser $h^0 = 0$, cualquiera que sea la aplicación h de partida. Así pues, el miembro derecho de la igualdad anterior ha de ser nulo cualesquiera que sean los valores de x_{kl}. Si hacemos $x_{ij} = 1$ y $x_{kl} = 0$ cuando $(k, l) \neq (i, j)$, nos queda que

$$\frac{1}{|G|} \sum_{\sigma \in G} r^1_{ii}(\sigma) r^2_{jj}(\sigma^{-1}) = 0$$

y, sumando para todo i, j, queda que

$$\langle \chi_1, \chi_2 \rangle = \frac{1}{|G|} \sum_{\sigma \in G} \chi_1(\sigma)\chi_2(\sigma^{-1}) = 0.$$

Tomemos ahora $\rho_1 = \rho_2$. Entonces el lema de Schur nos da que $h^0(v) = \alpha v$ para todo $v \in V_1$. El valor de α depende de h, y podemos calcularlo. Para ello observamos que

$$n\alpha = \mathrm{Tr}(h^0) = \frac{1}{|G|} \sum_{\sigma \in G} \mathrm{Tr}(\rho_1(\sigma) \circ h \circ \rho_2(\sigma^{-1})) = \frac{1}{|G|} \sum_{\sigma \in G} \mathrm{Tr}(h) = \mathrm{Tr}(h),$$

luego $\alpha = (1/n)\,\mathrm{Tr}(h)$. En el caso $i \neq j$, tomando igualmente $x_{ij} = 1$ y $x_{kl} = 0$ cuando $(k,l) \neq (i,j)$, obtenemos igualmente que

$$\frac{1}{|G|}\sum_{\sigma\in G} r^1_{ii}(\sigma) r^1_{jj}(\sigma^{-1}) = 0.$$

En cambio, para $i = j$, la misma elección de x_{kl} hace que $\mathrm{Tr}(h) = 1$, luego

$$\frac{1}{n} = \frac{1}{|G|}\sum_{\sigma\in G} r^1_{ii}(\sigma) r^1_{jj}(\sigma^{-1}).$$

Al sumar para todo i y todo j, la igualdad $i = j$ se da n veces, luego sumamos n veces la última ecuación y llegamos a que

$$\langle \chi_1, \chi_1\rangle = \frac{1}{|G|}\sum_{\sigma\in G} \chi_1(\sigma)\chi_1(\sigma^{-1}) = 1.$$

■

En realidad, la prueba del teorema anterior contiene más información que la que indica su enunciado, puesto que hemos probado que $\langle \chi_1, \chi_2\rangle = 0$, no bajo la hipótesis de que $\chi_1 \neq \chi_2$, sino bajo la hipótesis de que las representaciones ρ_1 y ρ_2 no eran isomorfas. Por consiguiente, si dos representaciones irreducibles no son isomorfas, sus caracteres χ_1 y χ_2 han de ser distintos o, de lo contrario, cumplirían que $\langle \chi_1, \chi_2\rangle = 1$, mientras que hemos visto que $\langle \chi_1, \chi_2\rangle = 0$.

En otras palabras, tenemos que dos representaciones irreducibles de un grupo G son isomorfas si y sólo si determinan el mismo carácter. Enseguida probaremos que esto es cierto aunque las representaciones no sean irreducibles, pero para ello conviene probar antes lo siguiente:

Teorema 2.10 *Sea $\rho : G \longrightarrow \mathrm{Aut}(V)$ una representación de G, sea ϕ su carácter y sea $V = W_1 \oplus \cdots \oplus W_m$ una descomposición de V en subespacios invariantes irreducibles. Para cada carácter irreducible χ de G, el número de subespacios W_i que determinan una representación con carácter χ es $\langle \phi, \chi\rangle$.*

Demostración: Sea χ_i el carácter de la subrepresentación asociada a W_i. Entonces $\phi = \chi_1 + \cdots + \chi_m$, luego $\langle \phi, \chi\rangle = \langle \chi_1, \chi\rangle + \cdots + \langle \chi_m, \chi\rangle$, y las relaciones de ortogonalidad implican que este valor es el número de índices i tales que $\chi_i = \chi$. ■

Dicho de otro modo, si una representación tiene carácter ϕ, es necesariamente la suma directa de tantas representaciones irreducibles de carácter χ como indica el producto $\langle \phi, \chi\rangle$. Así pues:

Teorema 2.11 *Dos representaciones de un grupo finito G son isomorfas si y sólo si determinan el mismo carácter.*

Concluimos también que todo carácter ϕ se descompone de forma única como combinación lineal

$$\phi = n_1\chi_1 + \cdots + n_m\chi_m$$

de caracteres irreducibles con coeficientes enteros $n_i \geq 0$. Además,

$$\langle \phi, \phi \rangle = n_1^2 + \cdots + n_m^2,$$

luego ϕ es irreducible si y sólo si $\langle \phi, \phi \rangle = 1$.

Ejemplo El carácter χ que hemos calculado para el grupo D_4 en la página 10 es irreducible, pues

$$\langle \chi, \chi \rangle = \frac{1}{8} \sum_{\sigma \in G} \chi(\sigma)^2 = \frac{1}{8}(4+4) = 1.$$

■

Vamos a probar que el número de caracteres irreducibles es finito. Para ello consideramos la representación regular $\rho : G \longrightarrow \mathrm{Aut}(K[G])$. En el ejemplo de la página 10 hemos visto que

$$r_G(\tau) = \begin{cases} g & \text{si } \tau = 1, \\ 0 & \text{si } \tau \neq 1, \end{cases}$$

donde g es el orden de G.

Ahora, si χ es cualquier carácter irreducible de G, tenemos que

$$\langle r_G, \chi \rangle = \chi(1).$$

Por lo tanto, si $r_G = n_1\chi_1 + \cdots + n_h\chi_h$ es la descomposición de r_G en suma de caracteres irreducibles, los caracteres χ_i resultan ser todos los caracteres irreducibles de G, y $n_i = \chi_i(1)$ es el grado de χ_i. Teniendo en cuenta que $\langle r_G, r_G \rangle = g$, tenemos probado el teorema siguiente:

Teorema 2.12 *Un grupo finito G tiene un número finito de caracteres irreducibles $\chi_1, \ldots, \chi_h$, cuyos grados n_i verifican la relación*

$$n_1^2 + \cdots + n_h^2 = |G|.$$

Ejemplo El grupo D_4 tiene cinco clases de conjugación, luego cinco caracteres irreducibles, $\chi_1, \chi_2, \chi_3, \chi_4, \chi_5$, de los cuales conocemos dos: el carácter trivial $\chi_1 = 1$ y el calculado en la página 10 (al que numeraremos como χ_5). Los tres que faltan tienen grados n_i que han de cumplir $1 + n_2^2 + n_3^2 + n_4^2 + 4 = 8$, luego los tres han de ser de grado 1. ■

Si aplicamos el teorema 2.12 al caso $K = \mathbb{A}$, vemos que G tiene h representaciones irreducibles sobre $\mathbb{A}$, con caracteres χ_i, cuyos grados al cuadrado suman $|G|$. Si ahora K es un cuerpo arbitrario (algebraicamente cerrado de característica 0), cada una de las representaciones irreducibles de G sobre $\mathbb{A}$ determina por extensión de escalares (definición 1.6) una representación sobre K con la misma representación matricial asociada, por lo que tiene el mismo grado y, más aún, el mismo carácter. Como la relación $\langle \chi_i, \chi_i \rangle = 1$ no depende

del cuerpo considerado, vemos que las extensiones de las representaciones de G sobre $\mathbb{A}$ siguen siendo irreducibles sobre K y, como sus grados siguen sumando $|G|$, no puede haber más representaciones irreducibles de G sobre K. Si, por último, tenemos en cuenta que toda representación es suma directa de representaciones irreducibles, tenemos probado el teorema siguiente:

Teorema 2.13 *Toda representación de un grupo G sobre un cuerpo K es isomorfa a la extensión de escalares de una representación ρ de G sobre $\mathbb{A}$. Además, la extensión ρ^K es irreducible si y sólo si lo es ρ. En particular, los caracteres (irreducibles) de G sobre K coinciden con sus caracteres (irreducibles) sobre $\mathbb{A}$.*

Por consiguiente, a partir de aquí podríamos trabajar exclusivamente en el caso $K = \mathbb{A}$ sin pérdida de generalidad, pero nos será más cómodo aún trabajar en el caso $K = \mathbb{C}$.

2.2 Caracteres complejos

Para trabajar con caracteres complejos es más natural sustituir la forma bilineal $\langle\ ,\ \rangle$ por el siguiente producto escalar:

Definición 2.14 Si G es un grupo finito, definimos en el espacio vectorial $\mathbb{C}^G$ el producto escalar dado por

$$(\phi, \psi) = \frac{1}{|G|} \sum_{\sigma \in G} \phi(\sigma)\overline{\psi(\sigma)}.$$

Observemos que es ciertamente un producto escalar, es decir, que cumple las propiedades[1]

a) $(\phi, \psi) = \overline{(\psi, \phi)}$,

b) $(\phi + \psi, \chi) = (\phi, \chi) + (\psi, \chi)$, $\quad (\phi, \psi + \chi) = (\phi, \psi) + (\phi, \chi)$,

c) $(\alpha\phi, \psi) = \alpha(\phi, \psi)$, $\quad (\phi, \alpha\psi) = \bar{\alpha}(\phi, \psi)$,

d) $(\phi, \phi) \geq 0$ y $(\phi, \phi) = 0$ si y sólo si $\phi = 0$,

para todo ϕ, ψ, $\chi \in \mathbb{C}^G$ y todo $\alpha \in \mathbb{C}$.

Por otra parte, el teorema 2.3 prueba que, si $\phi, \psi \in \mathbb{C}^G$ son caracteres de G, entonces $\langle \phi, \psi \rangle = (\phi, \psi)$. Ahora observamos que en la sección anterior sólo hemos usado la forma bilineal $\langle\ ,\ \rangle$ sobre caracteres, por lo que todos los resultados de la sección anterior son válidos igualmente cambiando la forma bilineal $\langle\ ,\ \rangle$ por el producto escalar $(\ ,\ )$.

Para trabajar con funciones arbitrarias de $\mathbb{C}^G$ es más práctico el producto escalar.

[1] Véase la definición 3.36 de mi libro de *Análisis*.

Definición 2.15 Si G es un grupo finito, una *función de clases* en G es una aplicación $f : G \longrightarrow \mathbb{C}$ tal que $f(\rho^{-1}\tau\rho) = f(\tau)$ para todo par de elementos $\tau, \rho \in G$, es decir, una función que es constante en cada clase de conjugación de G. Llamaremos $F(G) \subset \mathbb{C}^G$ al subespacio vectorial formado por todas las funciones de clases.

Tras la definición 1.15 hemos probado que los caracteres de G son funciones de clases. Tenemos un isomorfismo natural $K^G \cong K[G]$ de espacios vectoriales que identifica cada función $\phi \in K^G$ con el elemento

$$\sum_{\sigma\in G} \phi(\sigma)\sigma \in K[G].$$

De acuerdo con el teorema 1.5, este isomorfismo hace corresponder $F(G)$ con el centro de $\mathbb{C}[G]$.

Probamos ahora una nueva consecuencia del lema de Schur, de la que extraeremos a su vez numerosas consecuencias sobre los caracteres de un grupo finito.

Teorema 2.16 *Sea $\rho : G \longrightarrow \mathrm{Aut}(V)$ una representación irreducible de grado n y carácter χ, y sea $\phi \in F(G)$ una función de clases, que podemos identificar con*

$$x = \sum_{\sigma\in G} \phi(\sigma)\sigma \in Z(\mathbb{C}[G]).$$

Entonces, para todo $v \in V$, se cumple que

$$vx = \frac{|G|}{n}(\phi, \overline{\chi})v.$$

Demostración: Como x está en el centro de $\mathbb{C}[G]$, es claro que la aplicación lineal $f : V \longrightarrow V$ dada por $f(v) = vx$ es un homomorfismo de $\mathbb{C}[G]$-módulos, luego el lema de Schur implica que existe un $\alpha \in \mathbb{C}$ tal que $f(v) = \alpha v$, para todo $v \in V$. Sólo hemos de calcular α. Para ello usamos la linealidad de la traza:

$$n\alpha = \mathrm{Tr}(f) = \sum_{\sigma\in G} \phi(\sigma)\,\mathrm{Tr}(\rho(\sigma)) = \sum_{\sigma\in G} \phi(\sigma)\chi(\sigma) = |G|(\phi, \overline{\chi}).$$

■

La primera consecuencia es la siguiente:

Teorema 2.17 *Si G es un grupo finito, sus caracteres irreducibles forman una base (ortonormal) del espacio $F(G)$ de las funciones de clases.*

Demostración: Sean $\chi_1, \ldots, \chi_h$ los caracteres irreducibles de G. Las relaciones de ortogonalidad implican que son linealmente independientes, luego sólo hemos de probar que generan $H = F(G)$. Para ello basta probar que la dimensión de H es h y, a su vez, para ello basta probar que los conjugados $\overline{\chi}_1, \ldots, \overline{\chi}_h$ generan H. Notemos que $(\overline{\chi}_i, \overline{\chi}_j) = (\chi_j, \chi_i)$, luego los conjugados también son ortonormales.

Tomamos $\psi \in H$ y consideramos la función de clases

$$\phi = \psi - \sum_{i=1}^{h} (\psi, \overline{\chi}_i)\overline{\chi}_i,$$

que tiene la propiedad de que $(\phi, \overline{\chi}_i) = 0$ para todo i. Sólo hemos de probar que esto implica que $\phi = 0$. Sea $x \in Z(\mathbb{C}[G])$ el elemento correspondiente a ϕ a través del isomorfismo natural.

Consideremos una representación $\rho : G \longrightarrow \mathrm{Aut}(V)$. Si es irreducible, el teorema anterior nos da que $vx = 0$, para todo $v \in V$. Si no es irreducible, llegamos a la misma conclusión descomponiéndolo en suma directa de submódulos irreducibles.

Vamos a aplicar esto al caso en que $V = \mathbb{C}[G]$, es decir, a la representación regular de G, y para $v = 1$. Entonces,

$$0 = 1x = \sum_{\sigma \in G} \phi(\sigma)\sigma,$$

luego $\phi = 0$. ∎

Es evidente que la dimensión de $F(G)$ es igual al número de clases de conjugación de G, luego:

Teorema 2.18 *El número de caracteres irreducibles de un grupo G es igual a su número de clases de conjugación.*

Si $\chi_1, \ldots, \chi_h$ son los caracteres irreducibles de un grupo G, tenemos que toda función de clases f se expresa de forma única como

$$f = \sum_{i=1}^{h} (f, \chi_i)\chi_i,$$

luego la condición necesaria y suficiente para que una función de clases $f \neq 0$ sea un carácter es que (f, χ_i) sea un número natural para todo i.

La segunda consecuencia de 2.16 es que, si en un $\mathbb{C}[G]$-módulo agrupamos todos los submódulos isomorfos, obtenemos una descomposición única:

Teorema 2.19 *Sea G un grupo finito y sean $\chi_1, \ldots, \chi_h$ sus caracteres irreducibles. Si V es un $\mathbb{C}[G]$-módulo y llamamos V_i a la suma de todos sus $\mathbb{C}[G]$-submódulos irreducibles de carácter χ_i, se cumple que*

$$V = \bigoplus_{i=1}^{h} V_i.$$

Equivalentemente: podemos encontrar distintas descomposiciones de V en suma directa de $\mathbb{C}[G]$-submódulos irreducibles, pero, si en cada una de ellas agrupamos todos los sumandos correspondientes al mismo carácter χ_i, el módulo V_i que obtenemos es independiente de la descomposición de partida.

DEMOSTRACIÓN: Llamemos n_i al grado de χ_i. Consideremos el elemento

$$x = \frac{n_i}{|G|}\sum_{\sigma\in G}\overline{\chi_i(\sigma)}\sigma \in Z(\mathbb{C}[G])$$

y llamemos $p_i : V \longrightarrow V$ a la aplicación lineal dada por $v \mapsto vx$. Como $x \in Z(\mathbb{C}[G])$, se trata, de hecho, de un homomorfismo de $\mathbb{C}[G]$-módulos.

Si W es un $\mathbb{C}[G]$-submódulo irreducible de V, la restricción $p_i|_W : W \longrightarrow W$ es también la multiplicación por x, y podemos aplicar el teorema 2.16, según el cual $p_i|_W$ es la homotecia de razón

$$\frac{n_i}{n}(\overline{\chi}_i, \overline{\chi}) = \frac{n_i}{n}(\chi, \chi_i),$$

donde χ es el carácter de W y n su grado. Así pues, $p_i|_W = 0$ si $\chi \neq \chi_i$ y $p_i|_W$ es la identidad si $\chi = \chi_i$. Esto implica que la imagen de p_i es V_i, que $p_i : V \longrightarrow V_i$ se restringe a la identidad en V_i y que es nula sobre cada V_j con $j \neq i$. Es obvio que V es la suma de los V_i y la existencia de estas proyecciones implica que la suma es directa. ∎

El teorema 2.2 afirma que los valores que toman los caracteres son enteros algebraicos. La siguiente consecuencia de 2.16 es otra propiedad de integridad:

Teorema 2.20 *Sea χ un carácter irreducible de grado n de un grupo G y sea $\psi : G \longrightarrow \mathbb{C}$ una función de clases cuyas imágenes sean enteros algebraicos. Entonces*

$$\frac{1}{n}\sum_{\sigma\in G}\psi(\sigma)\chi(\sigma)$$

es un entero algebraico.

DEMOSTRACIÓN: Consideremos la aplicación $T : Z(\mathbb{C}[G]) \longrightarrow \mathbb{C}$ dada por

$$T(x) = \frac{|G|}{n}(\phi, \overline{\chi}), \qquad \text{donde } x = \sum_{\sigma\in G}\phi(\sigma)\sigma.$$

El teorema 2.16 afirma que el homomorfismo $V \longrightarrow V$ dado por $v \mapsto vx$ es la homotecia de razón $T(x)$. Como $(vx)y = v(xy)$, concluimos que la homotecia de razón $T(xy)$ es la composición de la homotecia de razón $T(x)$ seguida de la homotecia de razón $T(y)$ o, más simplemente: $T(xy) = T(x)T(y)$. Es obvio que T conserva la suma, de modo que es un homomorfismo de anillos (conmutativos y unitarios).

Según 1.5, si $\mathrm{cl}(G) = \{c_1, \ldots, c_h\}$, el centro de $\mathbb{C}[G]$ tiene por base los elementos de la forma

$$e_i = \sum_{\sigma\in c_i}\sigma.$$

Se cumple que $e_ie_j \in \mathbb{Z}[G] \cap Z(\mathbb{C}[G]) = \langle e_1, \ldots, e_h\rangle_{\mathbb{Z}}$, luego el álgebra $\mathbb{Z}[e_1, \ldots, e_h]$ es un $\mathbb{Z}$-módulo finitamente generado, lo que prueba[2] que los e_i

[2]Véase el teorema 3.58 de mi libro de *Álgebra conmutativa*.

son enteros sobre $\mathbb{Z}$. Eligiendo $\sigma_i \in c_i$, podemos expresar

$$x = \sum_{\sigma\in G} \psi(\sigma)\sigma = \sum_{i=1}^{h} \psi(\sigma_i)e_i.$$

Por hipótesis, cada $\psi(\sigma_i)$ es un entero algebraico, luego $x \in Z(\mathbb{C}[G])$ es entero sobre $\mathbb{Z}$. Como T es un homomorfismo de anillos, esto implica que $T(x) \in \mathbb{C}$ es un entero algebraico. Explícitamente:

$$T(x) = \frac{|G|}{n}(\psi, \overline{\chi}) = \frac{1}{n}\sum_{\sigma\in G} \psi(\sigma)\chi(\sigma).$$

■

Veamos una primera aplicación (veremos otras en la sección siguiente):

Teorema 2.21 *Los grados de las representaciones irreducibles de un grupo G dividen al orden de G.*

Demostración: Basta probar que si χ es un carácter irreducible de G, entonces $\chi(1) \mid |G|$. Para ello aplicamos el teorema anterior a la función $\psi = \overline{\chi}$, lo que nos da que

$$\frac{1}{n}\sum_{\sigma\in G} \chi(\sigma)\overline{\chi}(\sigma) = \frac{|G|}{n}(\chi, \chi) = \frac{|G|}{n}$$

es un entero algebraico. Como es un número racional, ha de ser entero, y esto significa que $n \mid |G|$. ■

Los teoremas 2.12 y 2.18 nos dan una caracterización de los grupos abelianos:

Teorema 2.22 *Un grupo finito G es abeliano si y sólo si todos sus caracteres irreducibles tienen grado 1.*

Demostración: Sea g el orden de G y h su número de clases. Es claro que G es abeliano si y sólo si $g = h$. Si $n_1, \ldots, n_h$ son los grados de los caracteres irreducibles de G, sabemos que

$$n_1^2 + \cdots + n_h^2 = g,$$

luego $g = h$ si y sólo si $n_i = 1$ para todo i. ■

Observemos que $\mathrm{LG}(1, \mathbb{C}) \cong \mathbb{C}^*$ y el isomorfismo puede verse como el que a cada matriz le asigna su traza, luego una representación matricial de grado 1 de un grupo G puede verse como un homomorfismo de grupos $G \longrightarrow \mathbb{C}^*$, que se identifica a su vez con su carácter. En definitiva, los caracteres de grado 1 de un grupo finito G son simplemente los homomorfismos de grupos[3] $\chi : G \longrightarrow \mathbb{C}^*$.

[3]En particular, los caracteres irreducibles de los grupos abelianos finitos coinciden con los caracteres definidos, por ejemplo, en 11.12 de mi libro de *Teoría de números*.

2.3 Ejemplos y aplicaciones

Reunimos en esta sección algunos resultados adicionales sobre caracteres que no nos harán falta más adelante.

Ejemplo Nos faltaba calcular los caracteres de grado 1 del grupo D_4. Observemos que el centro de D_4 es $Z(D_4) = \{1, \sigma^2\}$. (El centro de un grupo está formado por los elementos cuya clase de conjugación es trivial.) El cociente $D_4/Z(D_4)$ es abeliano, luego tiene cuatro caracteres de grado 1, que son, por lo tanto, los tres caracteres que buscamos, más el trivial.

Concretamente, $D_4/Z(D_4) \cong C_2 \times C_2$, sus elementos tienen todos orden 2, luego sus caracteres tienen que tomar valores en $\mathbb{C}^*$ iguales a ± 1. Teniendo esto en cuenta es fácil calcular la *tabla de caracteres* (irreducibles) de D_4:

D_4	1	σ	σ^2	τ	$\sigma\tau$
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	1	-1	1	1	-1
χ_4	1	-1	1	-1	1
χ_5	2	0	-2	0	0

Notemos que podríamos haber calculado χ_5 a partir de los otros caracteres sin necesidad de conocer la representación que lo genera. Basta tener en cuenta que $r_G = \chi_1 + \chi_2 + \chi_3 + \chi_4 + 2\chi_5$ y que r_G toma siempre el valor 0 salvo en 1. ∎

Ejemplo En $Q = \mathbb{R}^4$ es posible definir una estructura de anillo de división conocida como el álgebra de los cuaterniones.[4] Si llamamos $1, i, j, k$ a la base canónica de $\mathbb{R}^4$, el producto de Q está completamente determinado por las relaciones

$$i^2 = j^2 = k^2 = -1, \quad ij = k, \quad ji = -k, \quad jk = i, \quad kj = -i, \quad ki = j, \quad ik = -j.$$

Se sigue entonces que el conjunto $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ es un subgrupo del grupo de unidades de Q, conocido como el *grupo cuaternio.* Tiene cinco clases de conjugación:

$$\mathrm{cl}(Q_8) = \{\{1\}, \{-1\}, \{\pm i\}, \{\pm j\}, \{\pm k\}\}$$

y el cociente $Q_8/\{\pm 1\} \cong C_2 \times C_2$ nos da cuatro caracteres de grado 1 análogos a los que hemos obtenido para D_4 en el ejemplo anterior. Esto implica que el quinto carácter ha de tener grado 2 y, teniendo en cuenta que puede calcularse a partir del carácter regular de Q_8, concluimos que la tabla de caracteres de Q_8 es idéntica a la de D_4 (biyectando adecuadamente las clases de conjugación), a pesar de que ambos grupos no son isomorfos. ∎

Ejercicio: Calcular la tabla de caracteres de Σ_3.

[4] Véase la sección 5.3 de mi libro de *Geometría.*

Relaciones de ortogonalidad duales A la hora de calcular tablas de caracteres, es útil contar con que no sólo las filas de la tabla son ortogonales dos a dos, sino que las columnas también lo son. En efecto:

Teorema 2.23 *Sea G un grupo finito, sean $\chi_1, \dots, \chi_h$ sus caracteres irreducibles y sean $\sigma, \tau \in G$. Entonces*

$$\sum_{r=1}^{h} \chi_r(\sigma)\overline{\chi_r(\tau)} = \begin{cases} |G|/|\mathrm{cl}_G(\sigma)| & si \ \ \mathrm{cl}_G(\sigma) = \mathrm{cl}_G(\tau), \\ 0 & si \ \ \mathrm{cl}_G(\sigma) \neq \mathrm{cl}_G(\tau). \end{cases}$$

Demostración: Sean $\sigma_1, \dots, \sigma_h$ representantes de las clases de conjugación de G y sea $h_i = |\mathrm{cl}_G(\sigma_i)|$. En estos términos, lo que hemos de probar es que

$$\sum_{r=1}^{h} \chi_r(\sigma_i)\overline{\chi_r(\sigma_j)} = \frac{|G|}{h_j}\delta_{ij},$$

donde (δ_{ij}) es la matriz identidad. Consideremos las matrices B y C dadas por

$$b_{ij} = \frac{h_j}{|G|}\overline{\chi_i(\sigma_j)}, \qquad c_{ij} = \chi_j(\sigma_i).$$

Entonces, el elemento (i, j) de BC es

$$\frac{1}{|G|}\sum_{r=1}^{h} h_r \overline{\chi_i(\sigma_r)}\chi_j(\sigma_r) = \frac{1}{|G|}\sum_{\sigma\in G} \overline{\chi_i(\sigma)}\chi_j(\sigma) = \delta_{ij},$$

por las relaciones de ortogonalidad, luego $BC = I$. Esto implica que $CB = I$, lo que se traduce precisamente en la relación que queríamos probar. ∎

Caracteres de productos directos Vamos a determinar los caracteres de un producto directo de grupos $G = G_1 \times G_2$. Observemos que, como $G_1 \cong G/G_2$, podemos considerar a cada carácter χ de G_1 como un carácter de G. Concretamente, entendiendo que $\chi(g_1 g_2) = \chi(g_1)$. Lo mismo es válido para los caracteres de G_2.

Teorema 2.24 *Sea $G = G_1 \times G_2$ un producto directo de grupos. Si χ_i es un carácter irreducible de G_i, entonces $\chi_1\chi_2$ es un carácter irreducible de G, y todo carácter irreducible de G es de esta forma.*

Demostración: Sabemos que $\chi_1\chi_2$ es un carácter de G, aunque, en general, el producto de caracteres irreducibles no tiene por qué ser irreducible. No obstante, multiplicando las ecuaciones

$$(\chi_1, \chi_1) = \frac{1}{|G_1|}\sum_{g_1\in G_1} |\chi_1(g_1)|^2 = 1, \quad (\chi_2, \chi_2) = \frac{1}{|G_2|}\sum_{g_2\in G_2} |\chi_2(g_2)|^2 = 1,$$

obtenemos que $(\chi_1\chi_2, \chi_1\chi_2) = 1$, luego $\chi_1\chi_2$ es irreducible.

Si $\chi_1^i, \dots, \chi_{h_i}^i$ son los caracteres irreducibles de G_i, es claro que los caracteres $\chi_k^1\chi_l^2$ son distintos dos a dos, pues el producto determina los factores por restricción. Sabemos que

$$\sum_k \chi_k^1(1)^2 = |G_1|, \quad \sum_l \chi_l^2(1)^2 = |G_2|,$$

y multiplicando ambas ecuaciones obtenemos que

$$\sum_{k,l} (\chi_k^1\chi_l^2)(1)^2 = |G|,$$

luego G no puede tener más caracteres irreducibles. ∎

En particular, descomponiendo un grupo abeliano como producto de grupos cíclicos, podemos determinar fácilmente todos sus caracteres irreducibles. Sólo tenemos que observar que los caracteres irreducibles de un grupo cíclico $G = \langle\sigma\rangle$ de orden n son los homomorfismos $\chi : G \longrightarrow \mathbb{C}^*$ determinados por que $\chi(\sigma)$ es una raíz n-sima de la unidad. Hay n raíces posibles que dan lugar a los n caracteres irreducibles de G.

El grado de un carácter irreducible Hemos probado que el grado de un carácter irreducible de un grupo finito G debe dividir al orden de G. Este resultado puede mejorarse.

Teorema 2.25 *Si G es un grupo finito, el grado de cualquier carácter irreducible de G divide al índice $|G : Z(G)|$.*

Demostración: Sea $g = |G|$ y $c = |Z(G)|$. Consideremos una representación irreducible $\rho : G \longrightarrow \mathrm{Aut}(V)$ de grado n. Si $\sigma \in Z(G) \subset Z(\mathbb{C}[G])$, el teorema 2.16 nos dice que $\rho(\sigma)$ es una homotecia en V de razón $\lambda(\sigma)$, de modo que $\lambda : Z(G) \longrightarrow \mathbb{C}^*$ es un homomorfismo de grupos.

Fijemos ahora un número natural $m \geq 1$ y consideremos el grupo G^m (el producto directo de G por sí mismo m veces). Si χ es el carácter de ρ, podemos considerar en G^m el carácter χ^m, que, según hemos visto en la sección anterior, es irreducible, y está asociado a la representación

$$\rho^m : G^m \longrightarrow \mathrm{Aut}(V \otimes_{\mathbb{C}[G]} \cdots \otimes_{\mathbb{C}[G]} V)$$

dada por[5] $\rho^m(\sigma_1, \dots, \sigma_m)(v_1 \otimes \cdots \otimes v_m) = v_1\sigma_1 \otimes \cdots \otimes v_m\sigma_m$. Por consiguiente, si $(\sigma_1, \dots, \sigma_m) \in \mathbb{Z}(G)^m$, tenemos que $\rho^m(\sigma_1, \dots, \sigma_m)$ es la homotecia de razón $\lambda(\sigma_1 \cdots \sigma_m)$.

Consideremos el subgrupo H de $Z(G)^m$ formado por los elementos que cumplen $\sigma_1 \cdots \sigma_m = 1$. Tenemos que H está en el núcleo de ρ^m, luego podemos ver a ρ^m como representación de G^m/H. El teorema 2.21 implica que el grado de ρ^m, que es n^m, divide el orden de este cociente, que es g^m/c^{m-1}. Así pues,

[5]Con más detalle, al considerar a χ como carácter del i-ésimo factor, su representación asociada es la dada por $G^m \xrightarrow{p_i} G \xrightarrow{\rho} \mathrm{Aut}(V)$, y el producto tensorial de estas representaciones de G^m es el indicado.

existe un $k \in \mathbb{Z}$ tal que $kn^m = g^m/c^{m-1}$ o, lo que es lo mismo, $(g/cn)^m \in c^{-1}\mathbb{Z}$, para todo $m \geq 1$.

Esto implica que $\mathbb{Z}[g/cn] \subset c^{-1}\mathbb{Z}$, luego la $\mathbb{Z}$-álgebra $\mathbb{Z}[g/cn]$ es un $\mathbb{Z}$-módulo finitamente generado, luego g/cn es un entero algebraico y un número racional, luego $g/cn \in \mathbb{Z}$, luego $n \mid g/c = |G : Z(G)|$. ∎

Para un resultado más preciso, véase el teorema 2.40, más abajo.

Subgrupos normales El teorema 2.5 nos permite reconocer el núcleo de un carácter a partir de la tabla de caracteres de un grupo. Obviamente, los núcleos de caracteres son subgrupos normales. Los demás subgrupos normales de un grupo dado pueden calcularse a partir de la tabla de caracteres sin más que tener en cuenta que son intersecciones de núcleos:

Teorema 2.26 *Todo subgrupo normal de un grupo finito es la intersección de los núcleos de los caracteres irreducibles que lo contienen.*

Demostración: Es trivial: sea G un grupo y N un subgrupo normal. Los caracteres irreducibles que contienen a N en su núcleo son los caracteres irreducibles de G/N, luego todo se reduce a probar que la intersección de los núcleos de todos los caracteres irreducibles de un grupo dado es trivial, pero ello se debe a que dicha intersección es el núcleo de la representación regular, que es fiel. ∎

Recordemos que el subgrupo derivado de un grupo G es el menor subgrupo G' tal que el cociente G/G' es abeliano.

Teorema 2.27 *El subgrupo derivado de un grupo finito es la intersección de los núcleos de los caracteres irreducibles de grado* 1*.*

Demostración: Si un carácter irreducible $\chi : G \longrightarrow \mathbb{C}$ cumple $G' \leq \mathrm{N}(\chi)$, entonces χ es un carácter irreducible de G/G' y, como el cociente es abeliano, χ tiene grado 1. Recíprocamente, si χ tiene grado 1, entonces es un homomorfismo $\chi : G \longrightarrow \mathbb{C}^*$, luego $G/\mathrm{N}(\chi)$ es abeliano y, por consiguiente, $G' \leq \mathrm{N}(\chi)$. ∎

En particular, el número de caracteres de grado 1 de un grupo finito G es igual al índice $|G : G'|$.

También podemos calcular el centro de un grupo a partir de su tabla de caracteres. Para ello definimos el *centro* de un carácter $\chi : G \longrightarrow \mathbb{C}$ como el conjunto

$$Z(\chi) = \{\sigma \in G \mid |\chi(\sigma)| = \chi(1)\}.$$

Teorema 2.28 *Sea G un grupo finito.*

a) Si χ es un carácter de G asociado a una representación $\rho : G \longrightarrow \mathrm{Aut}(V)$, entonces

$$Z(\chi) = \{\sigma \in G \mid \rho(\sigma) \text{ es una homotecia }\}.$$

b) $Z(\chi)$ es un subgrupo de G y $Z(\chi)/\mathrm{N}(\chi)$ es cíclico.

c) $Z(G)$ es la intersección de los centros de todos los caracteres irreducibles de G.

d) Si χ es un carácter irreducible y fiel de G, entonces $Z(G) = Z(\chi)$.

DEMOSTRACIÓN: a) Dado $\sigma \in G$, sabemos que, eligiendo una base en V, podemos suponer que la matriz asociada al automorfismo $\rho(\sigma)$ es diagonal y $\chi(\sigma) = \epsilon_1 + \cdots + \epsilon_n$ es la suma de dicha diagonal. Además, todos los ϵ_i tienen módulo 1.

Tenemos que $\sigma \in Z(\chi)$ si y sólo si $|\epsilon_1 + \cdots + \epsilon_n| = n$, y es fácil ver que esto ocurre sí y sólo si todos los ϵ_i son iguales, es decir, si y sólo si $\rho(\sigma)$ es una homotecia de razón ϵ.

b) Ahora es inmediato que $Z(\chi)$ es un subgrupo de G. Más aún, si llamamos $\lambda(\sigma)$ a la razón de la homotecia $\rho(\sigma)$, tenemos que $\lambda : Z(\chi) \longrightarrow \mathbb{C}^*$ es un homomorfismo de grupos cuyo núcleo es $\mathrm{N}(\chi)$, $Z(\chi)/\mathrm{N}(\chi)$ es isomorfo a un subgrupo finito de $\mathbb{C}^*$, luego ha de ser cíclico.

c) Si χ es irreducible, el teorema 2.16 implica que $Z(G) \leq Z(\chi)$. Por otra parte, como $\rho[Z(\chi)]$ está formado por homotecias, $\rho[Z(\chi)] \leq Z(\rho[G])$. Teniendo en cuenta el isomorfismo natural $\rho[G] \cong G/\mathrm{N}(\chi)$, vemos que

$$Z(\chi)/\mathrm{N}(\chi) \leq Z(G/\mathrm{N}(\chi)).$$

Si σ pertenece a los centros de todos los caracteres irreducibles de G y $\tau \in G$, se cumple que $\sigma\tau\sigma^{-1}\tau^{-1} \in \mathrm{N}(\chi)$, y esto vale para todo carácter irreducible χ, luego $\sigma\tau\sigma^{-1}\tau^{-1} = 1$, lo que implica que $\sigma \in Z(G)$.

d) Si χ es un carácter irreducible y fiel de G, en c) hemos probado que $Z(\chi) \leq Z(G)$, y también la inclusión opuesta, luego $Z(G) = Z(\chi)$. ∎

En particular, vemos que una condición necesaria para que un grupo G pueda tener un carácter irreducible y fiel es que $Z(G)$ sea cíclico. Hay ejemplos que muestran que no es suficiente.

El teorema $p^a q^b$ de Burnside Terminamos con una aplicación típica de la teoría de caracteres. Se trata de un teorema muy difícil de probar si no se usa la teoría de caracteres y con una prueba muy simple en términos de caracteres.

Necesitamos un resultado previo:

Teorema 2.29 *Sea χ un carácter irreducible de un grupo finito G y sea $\sigma \in G$ tal que $|\mathrm{cl}_G(\sigma)|$ sea primo con $\chi(1)$. Entonces $\chi(\sigma) = 0$ o bien $|\chi(\sigma)| = \chi(1)$.*

DEMOSTRACIÓN: Sean $u, v \in \mathbb{Z}$ tales que $u|\mathrm{cl}_G(\sigma)| + v\chi(1) = 1$. Entonces

$$\frac{u|\mathrm{cl}_G(\sigma)|\chi(\sigma)}{\chi(1)} + v\chi(\sigma) = \frac{\chi(\sigma)}{\chi(1)}.$$

El miembro izquierdo es un entero algebraico por el teorema 2.20, aplicado a la función de clases ψ que vale 1 sobre $\mathrm{cl}_G(\sigma)$ y 0 en las demás clases. Por consiguiente, el número $a = \chi(\sigma)/\chi(1)$ también es un entero algebraico.

Sea K la adjunción a $\mathbb{Q}$ de las raíces del polinomio mínimo de a sobre $\mathbb{Q}$. Si $a = a_1, \ldots, a_n$ son estas raíces, tenemos que a_i es la imagen de a por un $\mathbb{Q}$-automorfismo de K. Como $\chi(\sigma)$ es suma de $\chi(1)$ raíces de la unidad, cada a_i es de la forma

$$\frac{\text{suma de } \chi(1) \text{ raíces de la unidad}}{\chi(1)},$$

luego $|a_i| \leq 1$. Por consiguiente $|\,\mathrm{N}_{\mathbb{Q}}^K(a)| \leq 1$ y esta norma es un entero algebraico, a la vez que un número racional, luego ha de ser un número entero, más concretamente, 0 o ± 1.

Si $\mathrm{N}_{\mathbb{Q}}^K(a) = 0$, entonces $a = 0$ y $\chi(\sigma) = 0$, mientras que si $\mathrm{N}_{\mathbb{Q}}^K(a) = \pm 1$, ha de ser $|a| = 1$, luego $|\chi(\sigma)| = \chi(1)$. ∎

El teorema 1.28 afirma que todo p-grupo es nilpotente y, por consiguiente, resoluble. El teorema de Burnside generaliza este hecho a grupos con orden divisible entre dos primos:

Teorema 2.30 (Burnside) *Todo grupo de orden $p^a q^b$, con p y q primos, es resoluble.*

Demostración: Sea G un grupo de orden $p^a q^b$. Razonamos por inducción sobre el orden de G, es decir, suponemos que el teorema es cierto para todos los grupos de orden menor que $|G|$. Si G es abeliano, es trivialmente resoluble, luego podemos suponer que $Z(G) < G$.

Sea P un p-subgrupo de Sylow de G y sea $\sigma \in Z(P)$ un elemento $\sigma \neq 1$. (Existe por el teorema 1.21.) Consideremos la clase de conjugación $C = \mathrm{cl}_G(\sigma)$. Entonces $P \leq C_G(\sigma)$, luego $p \nmid |G : C_G(\sigma)|$ y, por el teorema 1.19, tenemos que $|C| = |G : C_G(\sigma)| = q^{b'}$, para cierto $b' \leq b$.

Basta probar que G tiene un subgrupo $1 < N \lhd G$, pues entonces N y G/N son resolubles por hipótesis de inducción, luego G también lo es. Supongamos que no es así, es decir, que G es un grupo simple no abeliano.

Si $b' = 0$, entonces $\sigma \in Z(G) \neq 1$, lo que nos da una contradicción. Supongamos, pues, que $b' > 0$. Sean $\chi_1, \ldots, \chi_h$ los caracteres irreducibles de G, donde $\chi_1 = 1$. El teorema 2.23 nos da que

$$0 = \sum_{i=1}^{h} \chi_i(1)\chi_i(\sigma) = 1 + \sum_{i=2}^{h} \chi_i(1)\chi_i(\sigma).$$

Podemos ordenar los caracteres de modo que $q \nmid \chi_i(1)$ para $1 \leq i \leq h_0$ y $q \mid \chi_i(1)$ para $h_0 < i \leq h$. En el primer caso, tenemos que $\chi_i(1)$ es primo con $|\mathrm{cl}_G(\sigma)|$, luego el teorema anterior nos da que $\chi_i(\sigma) = 0$ o bien $|\chi_i(\sigma)| = \chi_i(1)$. Si se da esta segunda posibilidad, como χ_i es fiel (porque G es simple), 2.28 nos da que $\sigma \in Z(G)$, lo cual es imposible. Por consiguiente, ha de ser $\chi_i(\sigma) = 0$. Esto nos reduce la igualdad anterior a

$$1 + \sum_{i=h_0+1}^{h} \chi_i(1)\chi_i(\sigma) = 0,$$

donde q divide a cada $\chi_i(1)$, pero esto es absurdo, porque nos permite expresar el número racional $1/q$ como combinación lineal entera de enteros algebraicos, lo que implica que $1/q \in \mathbb{Z}$. ∎

2.4 Caracteres inducidos

Si G es un grupo finito y H es un subgrupo, podemos considerar a $\mathbb{C}[H]$ como subespacio vectorial de $\mathbb{C}[G]$, lo que, a su vez, nos permite considerar a $\mathbb{C}[G]$ como $\mathbb{C}[H]$-módulo. Esto nos lleva a la definición siguiente:

Definición 2.31 Sea G un grupo finito y H un subgrupo. Consideremos una representación lineal $\rho : H \longrightarrow \mathrm{Aut}(W)$. Llamaremos *representación inducida* ρ^G a la representación de G asociada al $\mathbb{C}[G]$-módulo $W \otimes_{\mathbb{C}[H]} \mathbb{C}[G]$. Si ψ es el carácter de ρ, llamaremos *carácter inducido* ψ^G al carácter de G asociado a ρ^G.

Es obvio que, si $H \leq K \leq G$ y ψ es un carácter de H, entonces $(\psi^K)^G = \psi^G$.

Vamos a ver que ψ^G puede calcularse directamente a partir de ψ sin necesidad de conocer la representación que lo genera. Para ello conviene introducir la notación siguiente:

Definición 2.32 Sea G un grupo finito y H un subgrupo de G. Si ϕ es una función de clases en H, llamaremos $\phi^0 : G \longrightarrow \mathbb{C}$ a la función dada por

$$\phi^0(\sigma) = \begin{cases} \phi(\sigma) & \text{si } \sigma \in H, \\ 0 & \text{si } \sigma \notin H. \end{cases}$$

En estos términos, los caracteres inducidos se calculan como indica el teorema siguiente:

Teorema 2.33 *Sea G un grupo finito y H un subgrupo y sea R un sistema de representantes de las clases de congruencia por la derecha de G módulo H. Entonces, si ψ es un carácter de H, para todo $\sigma \in G$ se cumple que*

$$\psi^G(\sigma) = \sum_{\tau \in R} \psi^0(\tau\sigma\tau^{-1}) = \frac{1}{|H|} \sum_{\tau \in G} \psi^0(\tau\sigma\tau^{-1}).$$

Demostración: Sea $\rho : H \longrightarrow \mathrm{Aut}(W)$ la representación que determina el carácter dado ψ. Tenemos que cada $\sigma \in G$ se expresa de forma única como $\sigma = h\tau$, con $\tau \in R$. Es claro entonces que

$$\mathbb{C}[G] = \bigoplus_{\tau \in R} \mathbb{C}[H]\tau.$$

Por consiguiente, ψ^G es el carácter de

$$V = W \otimes_{\mathbb{C}[H]} \mathbb{C}[G] = \bigoplus_{\tau \in R} W\tau.$$

Fijado $\sigma \in G$, para cada $\tau \in R$, podemos expresar $\tau\sigma = h\tau_\sigma$, con $\tau_\sigma \in R$ y $h \in H$. De este modo, $(W\tau)\sigma = W\tau_\sigma$. Si fijamos una base B de W, la unión de los trasladados $B\tau$, con $\tau \in R$, es una base de V. Para calcular la traza de $\rho^G(\sigma)$ en esta base observamos que, si $\tau_\sigma \neq \tau$, las filas de la matriz de $\rho^G(\sigma)$ correspondientes a los vectores de $B\tau$ tienen ceros en la diagonal. Por el contrario, si $\tau_\sigma = \tau$, las suma de la diagonal de las filas correspondientes a $B\tau$ es la traza de $\rho^G(\sigma)|_{W\tau}$. Así pues:

$$\psi^G(\sigma) = \sum_{\tau \in R_\sigma} \mathrm{Tr}(\rho^G(\sigma)|_{W\tau}),$$

donde $R_\sigma = \{\tau \in R \mid \tau_\sigma = \tau\}$. Observemos que $\tau_\sigma = \tau$ equivale a que $\tau\sigma = h\tau$, es decir, que $\tau\sigma\tau^{-1} \in H$. Por último, observamos que el isomorfismo $f : W \longrightarrow W\tau$ dado por $f(w) = w\tau$ cumple

$$f(w\tau\sigma\tau^{-1}) = w\tau\sigma = f(w)\sigma.$$

Esto significa que $\rho^G(\sigma)|_{W\tau}$ se identifica a través de f con $\rho(\tau\sigma\tau^{-1})$, luego

$$\mathrm{Tr}(\rho^G(\sigma)|_{W\tau}) = \mathrm{Tr}(\rho(\tau\sigma\tau^{-1})) = \psi(\tau\sigma\tau^{-1}) = \psi^0(\tau\sigma\tau^{-1}).$$

Con esto obtenemos la primera fórmula del enunciado. La segunda se sigue de la primera debido a que, si $\tau \in R$ cumple $\tau\sigma\tau^{-1} \in H$, entonces, para cada $h \in H$ tenemos que $\tau' = h\tau \in G$ cumple $\tau'\sigma\tau'^{-1} \in H$ y $\psi(\tau'\sigma\tau'^{-1}) = \psi(\tau\sigma\tau^{-1})$ y, recíprocamente, todo $\tau' \in G$ que cumple $\tau'\sigma\tau'^{-1} \in H$ es de la forma $\tau' = h\tau$, para un único $\tau \in R$ tal que $\tau\sigma\tau^{-1} \in H$. En definitiva, cada sumando de la primera fórmula se corresponde con $|H|$ sumandos idénticos en la segunda. ∎

En particular, tenemos la relación entre los grados:

$$\psi^G(1) = |G : H|\psi(1).$$

Definición 2.34 Sea G un grupo finito, sea H un subgrupo de G y sea R un sistema de representantes de las clases de congruencia por la derecha de G módulo H. Para cada función de clases $\phi : H \longrightarrow \mathbb{C}$, definimos $\phi^G : G \longrightarrow \mathbb{C}$ mediante

$$\phi^G(\sigma) = \sum_{\tau \in R} \phi^0(\tau\sigma\tau^{-1}) = \frac{1}{|H|} \sum_{\tau \in G} \phi^0(\tau\sigma\tau^{-1}).$$

Hemos visto que si ϕ es un carácter de H, entonces ϕ^G es un carácter de G. En general, se cumple que ϕ^G es una función de clases de G. Esto se comprueba directamente sin dificultad o, alternativamente, basta observar que la aplicación $\phi \mapsto \phi^G$ es $\mathbb{C}$-lineal y que toda función de clases es combinación lineal de caracteres.

Notemos que también hay una forma natural (y mucho más simple) de pasar de un carácter de G a un carácter de H:

Definición 2.35 Sea G un grupo finito y H un subgrupo de G. Si ϕ es una función de clases de G, llamaremos ϕ_H a su restricción a H, que es también una función de clases en H, y es un carácter si ϕ lo es.

Entre estas dos operaciones hay una relación sencilla:

Teorema 2.36 (Reciprocidad de Frobenius) *Sea G un grupo finito y H un subgrupo. Sean $\phi : H \longrightarrow \mathbb{C}$ y $\psi : G \longrightarrow \mathbb{C}$ funciones de clases. Entonces*

$$(\phi, \psi_H) = (\phi^G, \psi).$$

DEMOSTRACIÓN: Basta realizar un cálculo directo:

$$(\phi^G, \psi) = \frac{1}{|G|}\sum_{\sigma\in G}\phi^G(\sigma)\overline{\psi(\sigma)} = \frac{1}{|G|}\,\frac{1}{|H|}\sum_{\sigma,\tau\in G}\phi^0(\tau\sigma\tau^{-1})\overline{\psi(\sigma)}$$

$$= \frac{1}{|G|}\,\frac{1}{|H|}\sum_{\sigma',\tau\in G}\phi^0(\sigma')\overline{\psi(\tau^{-1}\sigma'\tau)} = \frac{1}{|G|}\,\frac{1}{|H|}\sum_{\sigma',\tau\in G}\phi^0(\sigma')\overline{\psi(\sigma')}$$

$$= \frac{1}{|H|}\sum_{\sigma'\in H}\phi(\sigma')\overline{\psi(\sigma')} = (\phi, \psi_H).$$

■

Otra fórmula de interés que relaciona funciones de clase inducidas y restricciones es la siguiente:

Teorema 2.37 *Sea G un grupo finito y H un subgrupo. Sean $\phi : H \longrightarrow \mathbb{C}$ y $\psi : G \longrightarrow \mathbb{C}$ funciones de clases. Entonces $(\phi \cdot \psi_H)^G = \phi^G \cdot \psi$.*

DEMOSTRACIÓN: Para cada $\sigma \in G$, tenemos que

$$(\phi \cdot \psi_H)^G(\sigma) = \frac{1}{|H|}\sum_{\tau\in G}\phi^0(\tau\sigma\tau^{-1})\psi_H^0(\tau\sigma\tau^{-1})$$

$$= \frac{1}{|H|}\sum_{\tau\in G}\phi^0(\tau\sigma\tau^{-1})\psi(\sigma) = \phi^G(\sigma)\psi(\sigma).$$

■

Ahora necesitamos un resultado técnico:

Teorema 2.38 *Sea G un grupo finito y N un subgrupo normal, sea χ un carácter irreducible de G tal que χ_N sea suma de al menos dos caracteres irreducibles distintos. Entonces existe un subgrupo $N \leq H < G$ y un carácter irreducible ψ de H tal que $\chi = \psi^G$.*

DEMOSTRACIÓN: Sea V un $\mathbb{C}[G]$-módulo asociado a χ, de modo que χ_N está asociado a V como $\mathbb{C}[N]$-módulo. Sea

$$V = \bigoplus_{i=1}^{h} V_i$$

la descomposición de V como $\mathbb{C}[N]$-módulo dada por el teorema 2.19. Por hipótesis, la suma tiene al menos dos sumandos no nulos.

En general, si W es un $\mathbb{C}[N]$-submódulo de V y $\sigma \in G$, se cumple que $W\sigma$ es también un $\mathbb{C}[N]$-submódulo, pues, si $n \in N$, se cumple que

$$W\sigma n = W(\sigma n \sigma^{-1})\sigma = W\sigma,$$

pues $\sigma n \sigma^{-1} \in N$. Además, si W tiene carácter χ_i, el carácter de $W\sigma$ es

$$\chi_i^\sigma(n) = \chi_i(\sigma n \sigma^{-1}),$$

que depende únicamente de χ_i y σ. Es claro que si W es irreducible, también lo es $W\sigma$, luego vemos que la multiplicación por σ transforma todos los submódulos irreducibles de un mismo V_i (es decir, todos los submódulos con un mismo carácter χ_i), en submódulos de un mismo V_j, por lo que $V_i\sigma = V_j$.

Fijemos un índice i_0 tal que $V_{i_0} \neq 0$ y sea $H = \{\sigma \in G \mid V_{i_0}\sigma = V_{i_0}\}$. Claramente, $N \leq H < G$. La segunda desigualdad es estricta porque, de lo contrario, V_{i_0} sería un $\mathbb{C}[G]$-submódulo de V, pero V es irreducible, luego sería $V = V_{i_0}$, cuando, por hipótesis, hay al menos dos sumandos no nulos.

Sea ψ el carácter de H asociado a $W = V_{i_0}$. Para probar que $\chi = \psi^G$ basta ver que, si R es un sistema de representantes de las clases de congruencia por la derecha de G módulo H, se cumple que

$$V = \bigoplus_{\tau \in R} W\tau,$$

pues esto implica que $V \cong W \otimes_{\mathbb{C}[H]} \mathbb{C}[G]$.

Si $\tau_1, \tau_2 \in R$ y $W\tau_1 = W\tau_2$, entonces $\tau_1\tau_2^{-1} \in H$, luego $\tau_1 = \tau_2$. Esto implica que cada $W\tau = V_{i_0}\tau$ con $\tau \in R$ es un V_i, luego la suma de los $W\tau$ es directa (porque lo es la de los V_i). Además, dicha suma directa es un $\mathbb{C}[G]$-submódulo de V, luego es todo V. ∎

En general no es cierto que todo carácter de un grupo esté inducido desde un subgrupo, pero sí lo es en el caso de los grupos superresolubles:

Teorema 2.39 *Si G es un grupo finito superresoluble, todo carácter irreducible de G está inducido por un carácter de grado 1 de un subgrupo de G.*

Demostración: Razonando por inducción, podemos suponer que el teorema es cierto para todo grupo de orden estrictamente menor que $|G|$. Sea χ un carácter irreducible de G. Podemos suponer que χ es fiel, es decir, que la representación $\rho : G \longrightarrow \mathrm{Aut}(V)$ que lo genera es inyectiva, pues, si tuviera núcleo $N \neq 1$, podríamos ver a χ como carácter de G/N, luego habría un subgrupo $H/N \leq G/N$ y un carácter ψ de grado 1 en H/N tal que $\chi = \psi^G$.

También podemos suponer que G no es abeliano, pues en caso contrario χ ya tiene grado 1 y no hay nada que probar.

Por el teorema 1.32, existe un subgrupo $Z(G) \lhd N \lhd G$. Como ρ es un monomorfismo, tenemos que $Z(\rho[G]) \lhd \rho[N]$. Por consiguiente, no todos los automorfismos en $\rho[N]$ son homotecias (ya que las homotecias conmutan con

todos los automorfismos), luego $\chi|_N$ ha de ser suma de al menos dos caracteres irreducibles distintos. (En caso contrario, como N es abeliano, $\chi|_N$ sería múltiplo de un único carácter de grado 1, y $\rho[N]$ constaría únicamente de homotecias.)

El teorema 2.38 nos da que $\chi = \psi^G$, para cierto carácter irreducible ψ de un subgrupo $H < G$. Como H también es superresoluble, podemos aplicar la hipótesis de inducción para concluir que $\psi = \phi^H$, para cierto carácter ϕ de grado 1, luego también $\chi = \phi^G$. ∎

Terminamos esta sección con una aplicación de 2.38:

Teorema 2.40 *Si G es un grupo finito y N es un subgrupo normal abeliano, entonces el grado de todo carácter irreducible de G divide al índice $|G : N|$.*

Demostración: Razonando por inducción, podemos suponer que el teorema es cierto para todo grupo de orden menor que $|G|$. Sea χ un carácter irreducible de G y supongamos que χ_N se descompone en suma de al menos dos caracteres irreducibles distintos. Entonces, por 2.38, existe un subgrupo $N \leq H < G$ tal que $\chi = \psi^G$, para cierto carácter ψ de H. Por hipótesis de inducción $\psi(1) \mid |H : N|$, luego

$$\chi(1) = \psi^G(1) = |G : H|\, \psi(1) \mid |G : N|.$$

Supongamos ahora que $\chi_N = n\psi$, para cierto carácter irreducible ψ de N, que será de grado 1, porque N es abeliano. Sea $\rho : G \longrightarrow \mathrm{LG}(n, \mathbb{C})$ una representación matricial que genere a χ, consideremos $G' = \rho[G] \leq \mathrm{LG}(n, \mathbb{C})$ y sea $N' = \rho[N]$. Tenemos un epimorfismo $G/N \longrightarrow G'/N'$, luego

$$|G' : N'| \,\Big|\, |G : N|.$$

El hecho de que $\chi_N = n\psi$ se traduce en que las matrices de N' son de la forma ϵI_n, luego $N' \leq Z(G')$. La inclusión $G' \longrightarrow \mathrm{LG}(n, \mathbb{C})$ es una representación irreducible de G' de grado n, luego 2.25 nos da que $n \mid |G' : N'| \,\Big|\, |G : N|$. ∎

2.5 El teorema de Brauer

La finalidad de esta sección es demostrar el teorema siguiente:

Teorema 2.41 (Brauer) *Si G es un grupo finito, todo carácter de G se expresa como combinación lineal con coeficientes enteros de caracteres inducidos por caracteres de grado* 1.

Para probarlo empezamos introduciendo el concepto siguiente:

Definición 2.42 Diremos que un grupo finito H es *p-elemental,* donde p es un número primo, si puede expresase como producto directo $H = C \times P$, donde C es un grupo cíclico de orden primo con p y P es un p-grupo (un grupo de orden potencia de p). Un grupo H es *elemental* si es p-elemental para algún primo p.

Todo grupo cíclico finito es p-elemental para todo primo p, pues se descompone como producto de grupos cíclicos de órdenes potencias de primos, y basta agrupar todos los factores que sean p-grupos por una parte, y todos los que no lo sean por otra.

Por otra parte, todo grupo elemental es nilpotente por ser producto directo de dos grupos nilpotentes. En particular es superresoluble.

Ahora podemos reducir la prueba del teorema de Brauer al resultado siguiente:

Teorema 2.43 *Si G es un grupo finito, todo carácter de G se expresa como combinación lineal con coeficientes enteros de caracteres inducidos desde subgrupos elementales.*

En efecto, de este teorema se sigue el teorema de Brauer, ya que si tenemos

$$\chi = n_1\phi_1^G + \cdots + n_r\phi_r^G,$$

donde cada ϕ_i es un carácter de un subgrupo elemental $H_i \leq G$, descomponiendo cada ϕ_i en suma de caracteres irreducibles podemos suponer que cada ϕ_i es irreducible y, como H_i es superresoluble, el teorema 2.39 nos da que ϕ_i está inducido a su vez por un carácter de grado 1, luego lo mismo vale para ϕ_i^G. ∎

Para tratar con combinaciones lineales enteras de caracteres conviene introducir el concepto siguiente:

Definición 2.44 Si G es un grupo finito y $\chi_1, \ldots, \chi_h$ son sus caracteres irreducibles, llamaremos $R(G) = \mathbb{Z}\chi_1 \oplus \cdots \oplus \mathbb{Z}\chi_h$ al subgrupo generado por los caracteres χ_i en el espacio $F(G)$ de las funciones de clase de G. A sus elementos los llamaremos *caracteres virtuales* de G.

Como los caracteres irreducibles son una base del $\mathbb{C}$-espacio vectorial $F(G)$ de las funciones de clases de G, es claro que también son una base de $R(G)$ como $\mathbb{Z}$-módulo. También es obvio que todo carácter virtual se expresa de forma única como diferencia de dos caracteres. Como el producto de caracteres es un carácter, tenemos que $R(G)$ es un subanillo de $F(G)$.

El teorema 2.43 es consecuencia, a su vez, del teorema siguiente:

Teorema 2.45 *Sea G un grupo finito y sea V_p el subgrupo de $R(G)$ generado por los caracteres inducidos desde subgrupos p-elementales de G. Entonces el cociente $R(G)/V_p$ es finito y su orden es primo con p.*

En efecto, si admitimos este resultado, sólo tenemos que probar que $R(G)$ es la suma V de los subgrupos V_p, para todo primo p. Como $V_p \leq V \leq R(G)$, tenemos que el cociente $R(G)/V$ es finito, y su orden es primo con p, para todo primo p, luego ha de ser $R(G) = V$. ∎

Observemos ahora que, si H es un subgrupo de G, el teorema 2.37 implica que el subgrupo de $R(G)$ generado por los caracteres inducidos desde H es un

ideal de $R(G)$, y V_p es la suma de estos ideales cuando H recorre los subgrupos p-elementales de G. Por consiguiente, V_p es también un ideal de $R(G)$. Veamos ahora que 2.45 es consecuencia del teorema siguiente:

Teorema 2.46 *Sea G un grupo finito de orden $|G| = p^i m$, donde $p \nmid m$, y sea V_p el subgrupo de $R(G)$ generado por los caracteres inducidos desde subgrupos p-elementales de G. Entonces $m \in V_p$.*

En efecto, $R(G)$ es un $\mathbb{Z}$-módulo finitamente generado, luego $R(G)/V_p$ también lo es. Por consiguiente, es producto de un número finito de grupos cíclicos.

Si $m \in V_p$, como éste es un ideal, tenemos que $m\phi \in V_p$ para todo $\phi \in R(G)$, lo que significa que todos los elementos de $R(G)/V_p$ tienen orden divisor de m. Por consiguiente, $R(G)/V_p$ es producto de un número finito de grupos cíclicos finitos de orden primo con p, y esto prueba 2.45. ∎

Consideremos ahora el anillo D de los enteros ciclotómicos de orden g, es decir, la $\mathbb{Z}$-subálgebra de $\mathbb{C}$ generada por las raíces g-ésimas de la unidad. Se trata de un $\mathbb{Z}$-módulo libre de rango finito. Fijemos una base $D = \langle \omega_1, \ldots, \omega_c \rangle_{\mathbb{Z}}$ tal que $\omega_1 = 1$. Vamos a trabajar en el producto tensorial $D \otimes_{\mathbb{Z}} R(G)$.

Como $R(G)$ es el $\mathbb{Z}$-módulo libre que tiene por base los caracteres irreducibles $\chi_1, \ldots, \chi_h$ de G, tenemos, por una parte, que $D \otimes_{\mathbb{Z}} R(G)$ es el D-módulo libre generado por los elementos $1 \otimes \chi_i$. Podemos identificarlo con el D-submódulo generado por $\chi_1, \ldots, \chi_h$ en el espacio $F(G)$ de las funciones de clases de G (de modo que identificamos cada $1 \otimes \chi_i$ con χ_i). Así, $R(G)$ es el conjunto de elementos de $D \otimes_{\mathbb{Z}} R(G)$ cuyas coordenadas en la base $1 \otimes \chi_i$ (o χ_i) son enteras.

Por otra parte, $D \otimes_{\mathbb{Z}} R(G)$ es también el $R(G)$-módulo libre de base $\omega_i \otimes 1$, y los elementos de $R(G)$ son los que en esta base tienen todas las coordenadas nulas excepto la de $\omega_1 \otimes 1 = 1 \otimes 1$.

Es claro entonces que $(D \otimes_{\mathbb{Z}} V_p) \cap R(G) = V_p$. (Un elemento de la intersección es un elemento de $D \otimes_{\mathbb{Z}} R(G)$ cuyas coordenadas en la base $\omega_i \otimes 1$ están en V_p y son todas nulas menos la de $\omega_1 \otimes 1$.) Por consiguiente, para probar 2.46 basta ver que $m \in D \otimes_{\mathbb{Z}} V_p$.

El hecho de que $R(G)$ sea un subanillo de $F(G)$ y que V_p sea un ideal, implica inmediatamente que $D \otimes_{\mathbb{Z}} R(G)$ también es un subanillo de $F(G)$ y que $D \otimes_{\mathbb{Z}} V_p$ es un ideal de $D \otimes_{\mathbb{Z}} R(G)$.

Teorema 2.47 *Sea G un grupo de orden g y sea $\phi : G \longrightarrow g\mathbb{Z}$ una función de clases que toma valores múltiplos de g. Entonces ϕ es combinación lineal con coeficientes en D de caracteres inducidos por caracteres de subgrupos cíclicos de G.*

Demostración: Podemos expresar $\phi = g\psi$, donde $\psi : G \longrightarrow \mathbb{Z}$ es otra función de clases. Para cada subgrupo cíclico $C \leq G$, definimos la función de clases $\theta_C : C \longrightarrow \mathbb{Z}$ mediante

$$\theta_C(x) = \begin{cases} |C| & \text{si } x \text{ genera } C, \\ 0 & \text{en otro caso.} \end{cases}$$

Si $C(G)$ es el conjunto de todos los subgrupos cíclicos de G, tenemos que

$$\sum_{C\in C(G)} \theta_C^G(x) = \sum_{y\in G} \sum_{C\in C(G)} \frac{\theta_C^0(yxy^{-1})}{|C|} = \sum_{y\in G} 1 = g.$$

Por lo tanto,

$$\phi = g\psi = \sum_{C\in C(G)} \theta_C^G\psi = \sum_{C\in C(G)} (\theta_C\psi_C)^G.$$

Falta probar que la función de clases $\eta_C = \theta_C\psi_C$ es combinación lineal con coeficientes en D de caracteres de C. Ciertamente, como toda función de clases, es combinación lineal de los caracteres irreducibles de C. Si χ es uno de ellos, su coeficiente en la combinación lineal es (η_C, χ) y, en efecto, se cumple que

$$(\eta_C, \chi) = \frac{1}{|C|}\sum_{\sigma\in C} \theta_C(\sigma)\psi(\sigma)\overline{\chi(\sigma)} = \sum_{\sigma} \psi(\sigma)\chi(\sigma^{-1}) \in D$$

donde en el último sumatorio σ recorre los generadores de C. El resultado está en D porque los caracteres de C y de G toman valores en D. (Precisamente para esto hemos introducido D en sustitución de $\mathbb{Z}$.) ∎

Puesto que todo grupo cíclico es p-elemental, el teorema anterior implica, en particular, que $\phi \in D \otimes_{\mathbb{Z}} V_p$.

Con esto podemos reducir el teorema de Brauer al resultado siguiente:

Teorema 2.48 *En las condiciones previas al teorema anterior, existe una función de clases $\psi : G \longrightarrow \mathbb{Z}$ tal que $\psi \in D \otimes_{\mathbb{Z}} V_p$ y, para todo $x \in G$, se cumple que $p \nmid \psi(x)$.*

En efecto, dada una función ψ en estas condiciones, si $g = p^i m$, llamemos N al orden del grupo de unidades de $\mathbb{Z}/p^i\mathbb{Z}$, de modo que $k^N \equiv 1$ (mód p^i), para todo entero k primo con p. En particular, $\psi(x)^N \equiv 1$ (mód p^i), para todo $x \in G$, luego la función de clases $m(\psi^N - 1)$ toma valores enteros múltiplos de g.

Por el teorema 2.47, tenemos que $m(\psi^N - 1) \in D \otimes_{\mathbb{Z}} V_p$. Por otra parte, $\psi \in D \otimes_{\mathbb{Z}} V_p$, y éste es un ideal de $D \otimes_{\mathbb{Z}} R(G)$, luego también $m\psi^N \in D \otimes_{\mathbb{Z}} V_p$, con lo que concluimos que $m \in D \otimes_{\mathbb{Z}} V_p$, y ya hemos visto que esto implica el teorema de Brauer. ∎

Tenemos pendiente demostrar 2.48.

Si G es un grupo finito y sea p un número primo. Diremos que $x \in G$ es un *p-elemento* si su orden es potencia de p, y es un *p'-elemento* si su orden es primo con p.

En general, si el orden de x es $m = p^i m'$, donde $p \nmid m'$, existen $u, v \in \mathbb{Z}$ tales que $up^i + vm' = 1$, con lo que $x_p = x^{vm'}$, $x_{p'} = x^{up^i}$ cumplen que

$$x = x_p x_{p'} = x_{p'} x_p, \quad x_p^{p^i} = x_{p'}^{m'} = 1,$$

es decir, que todo $x \in G$ puede descomponerse como producto de un p-elemento y un p'-elemento, a los que llamaremos, respectivamente, *p-componente* y *p'-componente* de x.

Necesitaremos este resultado técnico:

Teorema 2.49 *En las condiciones anteriores, sea $\psi : G \longrightarrow \mathbb{Z}$ una función de clases que cumpla $\psi \in D \otimes_{\mathbb{Z}} R(G)$. Si $x \in G$ y $x_{p'}$ es su p'-componente, entonces $\psi(x) \equiv \psi(x_{p'})$ (mód p).*

Demostración: Sea $C = \langle x \rangle$, de modo que $x_{p'} \in C$. Observamos que $\psi_C \in D \otimes_{\mathbb{Z}} R(C)$, luego no perdemos generalidad si suponemos que G está generado por x. Tenemos, pues, que

$$\psi = \sum_i d_i \chi_i,$$

con $d_i \in D$ y donde los caracteres irreducibles χ_i tienen todos grado 1 (porque G es abeliano), luego son homomorfismos de grupos $\chi_i : G \longrightarrow D^*$. Si $q = p^i$ es el orden de la p-componente de x, tenemos que $x^q = x_{p'}^q$, luego $\chi_i(x)^q = \chi_i(x_{p'})^q$. Por consiguiente:

$$\psi(x)^q = \left(\sum_i d_i \chi_i(x)\right)^q \equiv \sum_i d_i \chi_i(x)^q = \sum_i d_i \chi_i(x_{p'})^q$$

$$\equiv \left(\sum_i d_i \chi_i(x_{p'})\right)^q = \psi(x_{p'})^q \text{ (mód } p),$$

donde las congruencias son módulo el ideal generado por p en D. Ahora bien, como los extremos son enteros, concluimos que

$$\psi(x)^q \equiv \psi(x_{p'})^q \text{ (mód } p)$$

en $\mathbb{Z}$ y, como q es potencia de p, esto equivale a que $\psi(x) \equiv \psi(x_{p'})$ (mód p). ∎

Con esto estamos en condiciones de construir una función ψ en las condiciones del teorema 2.48. Para ello partimos de un sistema de representantes $\{x_i\}_i$ de las clases de conjugación de G formadas por p'-elementos. Sea P_i un p-subgrupo de Sylow del centralizador $C_G(x_i)$ y sea $C_i = \langle x_i \rangle$.

Como los elementos de C_i conmutan con los de P_i, tenemos que $H_i = C_i P_i$ es un subgrupo de G y, como $C_i \cap P_i = 1$ (porque el orden de C_i es primo con el orden de P_i), concluimos que el producto $H_i = C_i \times P_i$ es directo, luego H_i es un subgrupo p-elemental de G.

Sea $\phi_i : C_i \longrightarrow \mathbb{Z}$ la función de clases dada por

$$\phi_i(x) = \begin{cases} |C_i| & \text{si } x = x_i, \\ 0 & \text{si } x \neq x_i. \end{cases}$$

Se cumple que $\phi_i \in D \otimes_{\mathbb{Z}} R(C_i)$, pues, al expresar ϕ_i como combinación lineal de los caracteres de C_i, el coeficiente de cada carácter χ es

$$(\phi_i, \chi) = \overline{\chi(x_i)} = \chi(x_i^{-1}) \in D.$$

Definimos ahora $\psi_i : H_i \longrightarrow \mathbb{Z}$ mediante $\psi_i(x,y) = \phi_i(x)$, donde $x \in C_i$, $y \in P_i$. Viendo a C_i como cociente de H_i, tenemos que las funciones de clase de C_i determinan funciones de clase de H_i, y ψ_i es precisamente la función determinada por ϕ_i. Es claro entonces que $\psi_i \in D \otimes_{\mathbb{Z}} R(H_i)$ (porque ψ_i es combinación lineal con coeficientes en D de los caracteres de H_i determinados por los caracteres de C_i). Por consiguiente, $\psi_i^G \in D \otimes_{\mathbb{Z}} V_p$.

Por la propia definición de la función inducida por una función de clases es inmediato que ψ_i^G toma valores enteros. Vamos a probar que

$$\psi_i^G(x_i) \not\equiv 0 \ (\text{mód } p), \qquad \psi_i^G(x_j) = 0 \quad \text{para } j \neq i.$$

En efecto, si $y \in G$ cumple que $yx_jy^{-1} \in H_i$, entonces, como se trata de un p'-elemento, ha de ser $yx_jy^{-1} \in C_i$ y, para $j \neq i$, ha de ser $yx_jy^{-1} \neq x_i$, luego $\psi_i(yx_jy^{-1}) = \phi_i(yx_jy^{-1}) = 0$, y esto implica que $\psi_i^G(x_j) = 0$.

Por el contrario, el conjunto de los $y \in G$ tales que $yx_iy^{-1} = x_i$ es precisamente el centralizador $C_G(x_i)$, luego

$$\psi_i^G(x_i) = \frac{1}{|H_i|}\sum_{y\in G} \psi_i^0(y^{-1}x_iy) = \frac{|C_G(x_i)||C_i|}{|C_i||P_i|} = \frac{|C_G(x_i)|}{|P_i|},$$

que no es divisible entre p porque P_i es un p-subgrupo de Sylow del centralizador.

Ahora es fácil ver que la función

$$\psi = \sum_i \psi_i^G$$

cumple el teorema 2.48, pues, ciertamente $\psi \in D \otimes_{\mathbb{Z}} V_p$, toma valores enteros y, para todo $x \in G$, el teorema 2.49 nos da que $\psi(x) \equiv \psi(x_{p'})$ (mód p) y, a su vez, la p'-componente $x_{p'}$ está en la clase de conjugación de un x_i, luego

$$\psi(x) \equiv \psi(x_{p'}) = \psi(x_i) = \psi_i^G(x_i) \not\equiv 0 \ (\text{mód } p).$$

Esto prueba 2.48 y, por consiguiente, termina la demostración del teorema de Brauer. ∎

2.6 Caracteres en grupos cociente

Ya hemos visto que cada carácter de un grupo cociente G/N (y, más en general, cada función de clases) induce un carácter (o una función de clases) en G mediante $\phi_G(\sigma) = \phi(\sigma N)$. Ahora vamos a definir una correspondencia en sentido inverso análoga a la definición de los caracteres inducidos.

Para ello observamos que la representación $\rho : G \longrightarrow \mathrm{Aut}(\mathbb{C}[G/N])$ dada por $\rho(\sigma)(N\tau) = N\tau\sigma$ determina en $\mathbb{C}[G/N]$ una estructura natural de $\mathbb{C}[G]$-módulo que nos permite dar la definición siguiente:

Definición 2.50 Sea $\rho : G \longrightarrow \mathrm{Aut}(V)$ una representación lineal de un grupo finito G y sea N un subgrupo normal. Definimos la representación $\rho^{G/N}$ del grupo cociente G/N como la asociada al $\mathbb{C}[G/N]$-módulo $V \otimes_{\mathbb{C}[G]} \mathbb{C}[G/N]$. Si χ es el carácter de ρ, llamaremos $\chi^{G/N}$ al carácter de $\rho^{G/N}$.

Vamos a ver cómo calcular $\chi^{G/N}$ a partir de χ sin necesidad de considerar las representaciones correspondientes.

Llamemos V^N al subespacio de V fijado por los elementos de N. El hecho de que N sea un subgrupo normal implica que V^N es un $\mathbb{C}[G]$-submódulo de V, y la representación $G \longrightarrow \mathrm{Aut}(V^N)$ tiene a N en su núcleo, luego induce una representación de G/N o, lo que es lo mismo, podemos considerar a V^N como $\mathbb{C}[G/N]$-módulo de forma natural.

Consideremos a aplicación lineal $p : V \longrightarrow V^N$ dada por

$$p(v) = \frac{1}{|N|}\sum_{n\in N} vn.$$

Es inmediato comprobar que es un homomorfismo de $\mathbb{C}[G]$-módulos, que su imagen es ciertamente V^N y que se restringe a la identidad en V^N, luego, llamando W al núcleo de p, tenemos que $V = V^N \oplus W$, donde W es también un $\mathbb{C}[G]$-módulo.

La proyección p induce una aplicación lineal $f : V \otimes_{\mathbb{C}[G]} \mathbb{C}[G/N] \longrightarrow V^N$ dada por $f(v \otimes N\sigma) = p(v)\sigma$, que es claramente un homomorfismo de $\mathbb{C}[G/N]$-módulos y es, de hecho, un isomorfismo, pues admite como inversa a la aplicación g dada por $g(v) = v \otimes N1$.

Así pues, $\chi^{G/N}$ es también el carácter de la representación de G/N inducida por la restricción de ρ a V^N. Vamos a usar esta representación para calcular explícitamente $\chi^{G/N}$. Para cada $\sigma \in G$, definimos

$$x_\sigma = \frac{1}{|N|}\sum_{n\in N} n\sigma \in \mathbb{C}[G].$$

Es claro entonces que, si $v \in V$, se cumple que $vx_\sigma = p(v)\sigma$. Por consiguiente, $vx_\sigma = v\sigma$ para todo $v \in V^N$, mientras que $vx_\sigma = 0$ si $v \in W$. Esto significa que, fijando una base de V que sea unión de una base de V^N y otra de W, vemos que la multiplicación por x_σ es un endomorfismo de V que tiene la misma traza que la restricción de $\rho(\sigma)$ a V^N. Equivalentemente:

$$\chi^{G/N}(N\sigma) = \mathrm{Tr}(x_\sigma) = \frac{1}{|N|}\sum_{n\in N} \chi(n\sigma).$$

Para enunciar la conclusión a la que hemos llegado conviene dar primero la definición siguiente:

Definición 2.51 Sea G un grupo finito y N un subgrupo normal. Para cada función de clases $\phi : G \longrightarrow \mathbb{C}$, definimos la función de clases $\phi^{G/N} : G/N \longrightarrow \mathbb{C}$ mediante

$$\phi^{G/N}(N\sigma) = \frac{1}{|N|}\sum_{n\in N} \phi(n\sigma).$$

En estos términos hemos probado lo siguiente:

Teorema 2.52 *Si χ es un carácter de un grupo finito G y N es un subgrupo normal, entonces el carácter $\chi^{G/N}$ de G/N definido en* 2.50 *coincide con la función de clases de la definición anterior.*

O, dicho de otro modo, si χ es un carácter, $\chi^{G/N}$ también lo es.

A continuación probamos una fórmula análoga a la reciprocidad de Frobenius para caracteres inducidos:

Teorema 2.53 *Sea G un grupo finito, sea N un subgrupo normal, y sean $\phi : G \longrightarrow \mathbb{C}$, $\psi : G/N \longrightarrow \mathbb{C}$ funciones de clases. Entonces*

$$(\phi, \psi_G) = (\phi^{G/N}, \psi).$$

Demostración: Notemos que, por claridad, hemos representado por ψ_G la función ψ vista como función de G (que usualmente representamos también por ψ). Se trata de una comprobación rutinaria:

$$(\phi^{G/N}, \psi) = \frac{1}{|G:N|} \sum_{N\sigma \in G/N} \phi^{G/N}(N\sigma)\overline{\psi(N\sigma)}$$

$$= \frac{1}{|G|} \sum_{N\sigma \in G/N} \sum_{n \in N} \phi(n\sigma)\overline{\psi_G(n\sigma)} = \frac{1}{|G|} \sum_{\sigma \in G} \phi(\sigma)\overline{\psi_G(\sigma)} = (\phi, \psi_G).$$

■

2.7 Cuerpos no algebraicamente cerrados

Para terminar, vamos a ver qué podemos deducir de las representaciones de un grupo finito G sobre un cuerpo K no algebraicamente cerrado (de característica 0) a partir de lo que sabemos sobre el caso algebraicamente cerrado. Por simplicidad supondremos $K \subset \mathbb{C}$, aunque sería fácil razonar con cuerpos arbitrarios.

En principio, sabemos que si una representación de G sobre K está asociada al $K[G]$-módulo V, entonces $V_{\mathbb{C}} = \mathbb{C} \otimes_K V$ tiene una estructura natural de $\mathbb{C}[G]$-módulo que determina una representación de G sobre $\mathbb{C}$ que, eligiendo bases adecuadamente, se corresponde con la misma representación matricial que la representación de partida. En particular, el carácter de ambas representaciones es el mismo. Conviene observar que la estructura de $\mathbb{C}[G]$-módulo de $V_{\mathbb{C}}$ resulta explícita a través de los isomorfismos

$$V \otimes_{K[G]} \mathbb{C}[G] \cong V \otimes_{K[G]} \otimes K[G] \otimes_K \mathbb{C} \cong V \otimes_K \mathbb{C} \cong \mathbb{C} \otimes_K V = V_{\mathbb{C}}.$$

Es evidente que si V es reducible, entonces $V_{\mathbb{C}}$ también lo es, pero en la página 11 hemos visto un ejemplo en el que V es irreducible pero $V_{\mathbb{C}}$ no lo es.

Recordemos que una representación de G se dice realizable sobre K si está asociada a un $\mathbb{C}[G]$-módulo de la forma $V_{\mathbb{C}}$, para cierto $K[G]$-módulo V. Igualmente, diremos que un carácter χ es *realizable* sobre K si lo es su representación asociada.

El teorema siguiente nos permitirá relacionar el producto escalar con las representaciones en K:

Teorema 2.54 *Sean V y W dos $\mathbb{C}[G]$-módulos con caracteres asociados χ y ψ. Entonces*

$$(\chi, \psi) = \dim_{\mathbb{C}} \mathrm{Hom}(V, W).$$

DEMOSTRACIÓN: Sean $V = V_1 \oplus \cdots \oplus V_m$, $W = W_1 \oplus \cdots \oplus W_m$ las descomposiciones de V y W en $\mathbb{C}[G]$-módulos irreducibles, asociadas a los caracteres irreducibles χ_i y ψ_j. Cada homomorfismo $\alpha : V \longrightarrow W$ está determinado por las restricciones $\alpha_i = \alpha|_{V_i} : V_i \longrightarrow W$, cada una de las cuales está determinada por sus proyecciones $\alpha_{ij} : V_i \longrightarrow W_j$. Recíprocamente, cualquier familia de homomorfismos de $\mathbb{C}[G]$-módulos α_{ij} determina un homomorfismo α. Esto significa que

$$\mathrm{Hom}(V, W) = \bigoplus_{i,j} \mathrm{Hom}(V_i, W_j),$$

luego

$$\dim_{\mathbb{C}} \mathrm{Hom}(V, W) = \sum_{i,j} \dim_{\mathbb{C}} \mathrm{Hom}(V_i, W_j)$$

y, por otra parte,

$$(\chi, \psi) = \sum_{i,j} (\chi_i, \psi_j).$$

Esto reduce el teorema al caso en que V y W son irreducibles, en cuyo caso, el lema de Schur 2.7 nos da que $\mathrm{Hom}(V, W) = 0$ si $V \not\cong W$ (o, equivalentemente, si $\chi \neq \psi$) y $\mathrm{Hom}(V, W) \cong \mathbb{C}$ si $V \cong W$ (es decir, si $\chi = \psi$). Ahora basta aplicar las relaciones de ortogonalidad. ∎

Con esto podemos demostrar el resultado fundamental en que nos vamos a apoyar:

Teorema 2.55 *Sea K un subcuerpo de $\mathbb{C}$ y sean V y W dos $K[G]$-módulos irreducibles no isomorfos con caracteres ϕ y χ. Entonces $(\phi, \psi) = 0$.*

DEMOSTRACIÓN: Supongamos que $(\phi, \psi) \neq 0$. El teorema anterior nos da que $\mathrm{Hom}(V_{\mathbb{C}}, W_{\mathbb{C}}) \neq 0$. Tomemos, pues, un $\mathbb{C}[G]$-homomorfismo no nulo $f : V_{\mathbb{C}} \longrightarrow W_{\mathbb{C}}$. Fijando una K-base de $\mathbb{C}$, podemos descomponer

$$V_{\mathbb{C}} = \bigoplus_{\alpha \in B} \alpha \otimes V, \quad W_{\mathbb{C}} = \bigoplus_{\beta \in B} \beta \otimes W.$$

Tomemos $x \in V_{\mathbb{C}}$ tal que $f(x) \neq 0$. Podemos suponer que $x = \alpha \otimes v_0 \in \alpha \otimes V$, para cierto $\alpha \in B$ y cierto $v_0 \in V$. Por otra parte, existe $\beta \in B$ tal que $p_\beta(f(x)) \neq 0$, donde $p_\beta : W_{\mathbb{C}} \longrightarrow W$ es la proyección en $\beta \otimes W$. Observemos que $p_\beta(w\sigma) = p_\beta(w)\sigma$ para todo $w \in W_{\mathbb{C}}$ y todo $\sigma \in G$.

Definimos $\bar{f} : V \longrightarrow W$ mediante $\bar{f}(v) = p_\beta(f(\alpha \otimes v))$. Es claro que $\bar{f}$ es un $K[G]$-homomorfismo, y es no nulo, pues $\bar{f}(v_0) = p_\beta(f(x)) \neq 0$.

Así pues,[6] $\mathrm{Hom}(V, W) \neq 0$ y, como V y W son $K[G]$-módulos irreducibles, esto implica que $V \cong W$ (por el argumento empleado en la demostración del lema de Schur 2.7, pues esa parte no utiliza que K sea algebraicamente cerrado).

■

Así pues, si dos $K[G]$-módulos irreducibles V y W no son isomorfos, los $\mathbb{C}[G]$-módulos $V_\mathbb{C}$ y $W_\mathbb{C}$, aunque pueden ser reducibles, no pueden tener componentes irreducibles comunes. En particular no son isomorfos, luego no puede ocurrir que dos $K[G]$-módulos no isomorfos se vuelvan isomorfos por una extensión de coeficientes. Vemos también que dos $K[G]$-módulos irreducibles distintos tienen caracteres distintos (los mismos que $V_\mathbb{C}$ y $W_\mathbb{C}$), luego un $K[G]$-módulo irreducible está determinado salvo isomorfismo por su carácter.

Enseguida veremos que estos hechos son válidos para módulos arbitrarios, no necesariamente irreducibles. Para extraer más consecuencias del teorema anterior conviene introducir el concepto siguiente:

Definición 2.56 Sea K un subcuerpo de $\mathbb{C}$ y G un grupo finito. Recordemos (definición 2.44) que $R(G)$ es el anillo de los caracteres virtuales de G, es decir, el subgrupo generado por los caracteres de G en el espacio $F(G)$ de las funciones de clase de G. Definimos $R_K(G)$ como el subgrupo de $R(G)$ generado por los caracteres de G realizables sobre K.

En estos términos es inmediato el teorema siguiente:

Teorema 2.57 *Si K es un subcuerpo de $\mathbb{C}$ y G es un grupo finito, el grupo $R_K(G)$ es un $\mathbb{Z}$-módulo libre que tiene por base a los caracteres de G irreducibles sobre K. Más aún, esta base es ortogonal respecto al producto escalar de $R(G)$.*

Demostración: Hemos de entender que los caracteres de G irreducibles sobre K son los caracteres de las representaciones irreducibles de G sobre K (que no tienen por qué corresponder a $\mathbb{C}[G]$-módulos irreducibles). Es claro que $R_K(G)$ está generado por los caracteres irreducibles sobre K (pues toda representación de G sobre K es suma de representaciones irreducibles). La última afirmación del enunciado es precisamente el teorema anterior, y ésta implica a su vez que los caracteres irreducibles sobre K son linealmente independientes.

■

Todavía podemos decir más: sean $\chi_1, \ldots, \chi_r$ los caracteres de G irreducibles sobre K. Es claro que el carácter regular r_G es realizable sobre K (mediante el $K[G]$-módulo $K[G]$), luego podemos expresarlo en la forma

$$r_G = n_1\chi_1 + \cdots + n_r\chi_r,$$

[6] Más en general, podríamos haber usado el teorema 1.53, que nos da el isomorfismo:

$$\mathrm{Hom}(V_\mathbb{C}, W_\mathbb{C}) \cong \mathbb{C} \otimes_K \mathrm{Hom}(V, W).$$

donde los n_i son números naturales. Por otra parte, sabemos que r_G se expresa como combinación lineal de todos los caracteres irreducibles de G. De aquí deducimos varios hechos:

a) Un mismo carácter irreducible de G no puede aparecer en la descomposición de dos caracteres distintos χ_i. (Esto es por el teorema anterior.)

b) Todos los n_i son no nulos, es decir, que r_G contiene a todos los caracteres de G irreducibles sobre K. (De lo contrario, los caracteres en que se descompone χ_i no aparecerían en la descomposición de r_G, por la propiedad anterior.)

c) Todo carácter irreducible de G aparece en la descomposición de un (único) carácter de G irreducible sobre K.

A su vez, de aquí deducimos que dos $K[G]$-módulos son isomorfos si y sólo si tienen el mismo carácter. En efecto, si no son isomorfos y sus caracteres son ϕ y ψ, en las descomposiciones de los $K[G]$-módulos en $K[G]$-submódulos irreducibles ha de haber algún sumando con multiplicidad diferente en ambos, lo que se traduce en que ϕ y ψ se expresan como combinaciones lineales distintas de los χ_i, luego $\phi \neq \psi$, porque los χ_i son una base.

En particular, si χ es un carácter de G realizable sobre K, el $K[G]$-módulo que lo realiza es único salvo isomorfismo.

Teorema 2.58 *Si K es un subcuerpo de $\mathbb{C}$, para que un carácter χ de G sea realizable sobre K es necesario y suficiente que $\chi \in R_K(G)$.*

Demostración: Obviamente, la condición es necesaria. Si $\chi \in R_K(G)$, el teorema anterior nos da que

$$\chi = n_1\chi_1 + \cdots + n_r\chi_r,$$

donde los χ_i son caracteres de representaciones irreducibles de G sobre K y los n_i son números enteros. Basta probar que, de hecho, son números naturales, pero esto se debe a que $(\chi, \chi_i) = n_i(\chi_i, \chi_i)$ y, como χ y χ_i son caracteres de G (no necesariamente irreducibles), sucede que (χ, χ_i), $(\chi_i, \chi_i) \geq 0$, luego también $n_i \geq 0$. ∎

Definición 2.59 Si K es un subcuerpo de $\mathbb{C}$ y G es un grupo finito, diremos que un $K[G]$-módulo irreducible V es *absolutamente irreducible* si $V_{\mathbb{C}}$ es irreducible. Llamaremos caracteres absolutamente irreducibles a los caracteres de G realizables sobre K mediante $K[G]$-módulos absolutamente irreducibles.

Observemos que un carácter χ de G sobre K es absolutamente irreducible si y sólo si $(\chi, \chi) = 1$, y en tal caso es irreducible en cualquier extensión de K.

Teorema 2.60 *Si G es un grupo finito y K es un subcuerpo de $\mathbb{C}$, las afirmaciones siguientes son equivalentes:*

a) Todo carácter irreducible de G sobre K es absolutamente irreducible.

b) Todo carácter de G es realizable sobre K.

c) $R_K(G) = R(G)$.

DEMOSTRACIÓN: Si se cumple a) y χ es un carácter irreducible de G, sabemos que aparece en la descomposición de un carácter de G irreducible sobre K, pero, como éste es absolutamente irreducible, ha de ser el propio χ. Así pues, todo carácter irreducible de G es realizable sobre K, y lo mismo vale para los demás caracteres.

El teorema anterior nos da que b) $\Rightarrow$ c).

Si se cumple c), entonces $R_K(G)$ y $R(G)$ tienen el mismo rango sobre $\mathbb{Z}$, luego hay el mismo número de caracteres irreducibles de G sobre K que sobre $\mathbb{C}$, lo cual sólo es posible si todos los caracteres irreducibles de G sobre K son también irreducibles sobre $\mathbb{C}$. ∎

Definición 2.61 Se dice que un cuerpo $K \subset \mathbb{C}$ es un *cuerpo de escisión* de un grupo finito G si cumple las condiciones del teorema anterior.

Ahora es fácil ver que todos los resultados que conocemos para representaciones sobre $\mathbb{C}$ son válidos para representaciones sobre cualquier cuerpo de escisión[7] de G.

Terminamos probando que un cuerpo de escisión puede ser relativamente pequeño:

Teorema 2.62 *Sea G un grupo finito, sea m el exponente de G, es decir, el mínimo común múltiplo de los órdenes de los elementos de G y sea $K \subset \mathbb{C}$ un cuerpo que contenga a las raíces m-simas de la unidad. Entonces K es un cuerpo de escisión para G.*

DEMOSTRACIÓN: Basta probar que todo carácter χ de G está en $R_K(G)$. Por el teorema de Brauer, basta probar a su vez que $\psi^G \in R_K(G)$, donde ψ es un carácter de grado 1 de un subgrupo H de G. Ahora bien, como los elementos de H tienen órdenes divisores de m y $\psi : H \longrightarrow \mathbb{C}^*$ es un homomorfismo, es claro que $\psi \in R_K(H)$. Si V es un $K[H]$-módulo asociado a ψ, entonces su $\mathbb{C}[H]$-módulo asociado es $V \otimes_{K[H]} \mathbb{C}[H]$, luego el $\mathbb{C}[G]$-módulo asociado a ψ^G es

$$V \otimes_{K[H]} \mathbb{C}[H] \otimes_{\mathbb{C}[H]} \mathbb{C}[G] \cong V \otimes_{K[H]} \mathbb{C}[G] \cong (V \otimes_{K[H]} K[G]) \otimes_{K[G]} \mathbb{C}[G]$$

luego $\psi^G \in R_K(G)$. ∎

[7]Más aún, es fácil ver que son válidos para cualquier cuerpo de escisión de G definido en un contexto más general, a saber, como un cuerpo de característica 0 tal que las representaciones irreducibles de G sobre K se conservan irreducibles sobre la clausura algebraica de K.

Capítulo III

La teoría general

3.1 Anillos y módulos semisimples

El resultado fundamental de la teoría de representaciones ordinarias es que toda representación (sobre un cuerpo de característica 0) se descompone en suma directa de representaciones irreducibles. De hecho, esto es consecuencia del teorema 1.12, que sólo requiere que la característica del cuerpo no divida al orden del grupo. Vamos a introducir el marco algebraico adecuado para estudiar este hecho:

Definición 3.1 Si A es un anillo, un A-módulo M se dice *semisimple* si se descompone en suma directa de submódulos simples. Se dice que A es *semisimple* (por la izquierda o por la derecha) si lo es como A-módulo.

NOTA: *En lo sucesivo, por simplicidad, sobrentenderemos que los módulos e ideales que consideremos lo serán por la derecha, si bien es fácil ver que todos los resultados serán válidos para módulos e ideales por la izquierda modificando las pruebas de forma obvia.*

En primer lugar observamos que los anillos semisimples cumplen condiciones de finitud que no aparecen explícitamente en la definición:

Teorema 3.2 *Sea A un anillo semisimple. Entonces*

a) A es suma directa de un número finito de ideales simples.

b) A tiene longitud finita.

Demostración: En principio, A es suma directa de (tal vez infinitos) ideales simples. Ahora bien, $1 \in A$ ha de expresarse como suma de un número finito de elementos, cada uno en uno de dichos ideales. Pongamos que $1 = a_1 + \cdots + a_r$, con $a_i \in I_i$. Entonces, todo $a \in A$ se expresa como $a = 1a = a_1a + \cdots + a_ra$, lo que prueba que $A = I_1 \oplus \cdots \oplus I_r$. Esto prueba a).

Como I_i tiene obviamente longitud finita $l(I_i) = 1$, vemos que A también tiene longitud finta $l(A) = r$. Esto prueba b). ∎

Por el contrario un módulo semisimple podría ser suma directa de infinitos submódulos simples. En el teorema siguiente imponemos condiciones de finitud por simplicidad, pero podría demostrarse igualmente sin ellas, utilizando entonces el lema de Zorn. No obstante, lo cierto es que todos los anillos que vamos a considerar serán de longitud finita y todos los módulos finitamente generados.

Teorema 3.3 *Sea A un anillo de longitud finita y M un A-módulo finitamente generado. Las afirmaciones siguientes son equivalentes:*

a) M es semisimple.

b) Todo submódulo $N \subset M$ está complementado en M, es decir, existe otro submódulo R tal que $M = N \oplus R$.

c) M es suma de un número finito de submódulos simples.

Demostración: a) ⇒ b) Pongamos que $M = M_1 \oplus \cdots \oplus M_n$, donde cada M_i es simple. (Notemos que la suma ha de ser finita porque M tiene longitud finita. De hecho, los módulos M_i son necesariamente los factores de composición de M.) Como M_i no tiene submódulos propios, la intersección $N \cap M_i$ ha de ser igual a 0 o a M_i, es decir, o bien $M_i \subset N$ o bien $M_i \cap N = 0$.

Si $M_i \subset N$ para todo i, entonces $N = M$ y basta tomar $R = 0$. En caso contrario, podemos suponer que $M_1 \cap N = 0$. Reordenando los índices, podemos suponer que

$$(M_1 \oplus \cdots \oplus M_r) \cap N = 0$$

y que esto deja de ser cierto si añadimos cualquier otro sumando directo M_i con $i > r$. Vamos a probar que $M = N \oplus (M_1 \oplus \cdots \oplus M_r)$. Es claro que la suma es directa. Basta probar que la suma contiene a todos los M_j con $j > r$. Reordenando los índices, basta ver que la suma contiene a M_{r+1}. En caso contrario tendríamos que $M_{r+1} \cap (N \oplus (M_1 \oplus \cdots \oplus M_r)) = 0$, pero esto implica que $(M_1 \oplus \cdots \oplus M_{r+1}) \cap N = 0$, contradicción.

b) ⇒ c) Como M tiene longitud finita, contiene un submódulo simple M_1 (el primer término no nulo de una serie de composición). Por b) tenemos que $M = M_1 \oplus R_1$, para cierto submódulo R_1. Si $R_1 = 0$ o es simple, ya tenemos c); en caso contrario, R_1 contiene un submódulo simple M_2, y es claro que la suma $M_1 \oplus M_2$ es directa. De nuevo por b), podemos descomponer $M = M_1 \oplus M_2 \oplus R_2$ y, tras un número finito de pasos, hemos de llegar a una descomposición de M en suma (directa) de submódulos simples, ya que, si la longitud de M es n, no es posible que M tenga más de n sumandos directos no nulos.

c) ⇒ a) Supongamos que $M = M_1 + \cdots + M_n$ donde cada M_i es simple. Reordenando los índices, podemos suponer que la suma $M_1 \oplus \cdots \oplus M_r$ es directa y que esto es falso si añadimos cualquier otro sumando M_i con $i > r$. Vamos a probar que $M = M_1 \oplus \cdots \oplus M_r$. Para ello basta ver que esta suma directa

contiene a todos los M_i y, reordenando los índices, basta ver que contiene a M_{r+1}. Como éste es simple, tenemos que

$$(M_1 \oplus \cdots \oplus M_r) \cap M_{r+1}$$

ha de ser 0 o M_{r+1}. El primer caso no puede ser, porque entonces la suma $M_1 \oplus \cdots \oplus M_{r+1}$ sería directa, y el segundo caso equivale a la inclusión que queríamos probar: $M_{r+1} \subset M_1 \oplus \cdots \oplus M_r$. ∎

Tal y como hemos observado tras el teorema 1.47, si K es un cuerpo cualquiera y G es un grupo finito, la K-álgebra $K[G]$ tiene longitud finita, al igual que todos los $K[G]$-módulos finitamente generados (precisamente por 1.47). El teorema 1.12 implica entonces que, si $\operatorname{car} K \nmid |G|$, entonces todos los $K[G]$-módulos finitamente generados son semisimples. En realidad, el teorema siguiente muestra que esto es tanto como afirmar que $K[G]$ es semisimple:

Teorema 3.4 *Si A es un anillo semisimple, todo A-módulo finitamente generado*[1] *es semisimple.*

DEMOSTRACIÓN: Por hipótesis, $A = I_1 \oplus \cdots \oplus I_n$, donde cada I_i es un ideal derecho simple. Si $M = \langle m_1, \ldots, m_n \rangle$ es un A-módulo finitamente generado, cada $m_i I_j$ es un submódulo de M, y es claro que M es la suma de todos ellos. Por el teorema anterior, basta ver que son submódulos simples.

Podemos suponer que $m_i I_j \neq 0$, ya que en caso contrario podemos eliminar este módulo y M sigue siendo igual a la suma de los restantes. Consideramos el homomorfismo $f : I_j \longrightarrow m_i I_j$ dado por $f(a) = m_i a$. Obviamente es suprayectivo y, como I_j es simple, su núcleo ha de ser trivial. Así pues, $m_i I_j \cong I_j$ es simple. ∎

Tal y como hemos observado antes del teorema anterior, tenemos el teorema siguiente, que es el pilar sobre el que descansa la teoría de representaciones ordinarias:

Teorema 3.5 (Maschke) *Si G es un grupo finito y K es un cuerpo tal que $\operatorname{car} K \nmid |G|$, entonces la K-álgebra $K[G]$ es semisimple.*

(En principio, el teorema 1.12 prueba que $K[G]$ es semisimple por la derecha, pero igualmente se prueba que lo es por la izquierda.) En 3.26 probaremos el recíproco.

Así pues, todo cuanto digamos sobre anillos semisimples en general se aplicará en particular a las álgebras $K[G]$ (bajo la hipótesis sobre la característica del cuerpo).

Como primer paso en el estudio de la estructura de los anillos y módulos semisimples, vamos a probar una versión abstracta del teorema 2.19. Para ello probamos primero un hecho elemental:

[1] Si hubiéramos demostrado el teorema 3.3 sin las hipótesis de finitud, ahora podríamos concluir que todo módulo sobre un anillo semisimple es semisimple.

Teorema 3.6 *Si A es un anillo semisimple, I es un ideal simple y V es un A-módulo simple, entonces $I \cong V$ o bien $VI = 0$.*

DEMOSTRACIÓN: Es claro que VI es un submódulo de V, luego ha de ser $VI = 0$ o bien $VI = V$. En el segundo caso, tomamos un $v \in V$ tal que $vI \neq 0$ (recordemos que un módulo simple es no nulo por definición). Entonces vI es un submódulo no nulo, luego $vI = V$. Por último, el homomorfismo $I \longrightarrow V$ dado por $a \mapsto va$ es suprayectivo y, como I es simple, su núcleo ha de ser trivial, luego $I \cong V$. ∎

Teorema 3.7 *Sea A un anillo semisimple. Entonces:*

a) Existe un número finito de ideales simples $I_1, \ldots, I_h$ que no son isomorfos dos a dos (como A-módulos) y todo A-módulo simple (en particular, todo ideal simple) es isomorfo a uno de ellos.

b) Si A_i es la suma de todos los ideales simples de A isomorfos a I_i, entonces A_i es un ideal bilátero de A, así como un anillo semisimple (unitario), cuyos ideales simples son todos isomorfos a I_i como A_i-módulos.

c) $A = A_1 \oplus \cdots \oplus A_h$.

d) Si e_i es la unidad de A_i, se cumple que $e_1 + \cdots + e_h = 1$, $A_i = e_i A$, y $A_i A_j = 0$ para $i \neq j$.

DEMOSTRACIÓN: a) Todo A-módulo simple (en particular, todo ideal simple de A) es isomorfo a un factor de composición de A, luego sólo puede haber un número finito $I_1, \ldots, I_h$ de ideales simples no isomorfos entre sí.

b) El teorema anterior implica que si $i \neq j$, entonces $A_i A_j = 0$. Como A es suma directa de ideales simples (por ser semisimple), tenemos que $A = \sum A_i$. Por consiguiente, $AA_i \subset A_i A_i \subset A_i$, lo que prueba que, además de ser un ideal derecho, A_i también es un ideal izquierdo.

Por otra parte, podemos descomponer $1 = e_1 + \cdots + e_h$, con $e_i \in A_i$. Para todo $x \in A_i$, se cumple que

$$e_i x = (e_1 + \cdots + e_h)x = 1x = x,$$

e igualmente $xe_i = x$. Esto prueba que cada A_i es un anillo unitario con unidad e_i. (Notemos que, en particular, no puede ser $e_i = 0$, ya que entonces sería $A_i = 0$.) El teorema 3.3 nos da que A_i es semisimple, pues es suma de ideales simples, suma que podemos tomar finita porque A_i es noetheriano. Notemos además que los ideales simples de A contenidos en A_i coinciden con los ideales simples de A_i. Esto nos da también que todos los ideales simples de A_i son isomorfos entre sí.

c) Basta observar que si $0 = x_1 + \cdots + x_h$ con $x_i \in A_i$, entonces

$$0 = 0e_i = x_1 e_i + \cdots + x_h e_i = x_i e_i = x_i(e_1 + \cdots + e_h) = x_i 1 = x_i.$$

Lo que falta de d) ya es evidente. ∎

Ahora probamos un resultado análogo para módulos:

Teorema 3.8 *Con la notación del teorema anterior, si V es un A-módulo semisimple, entonces $V = VA_1 \oplus \cdots \oplus VA_h = Ve_1 \oplus \cdots \oplus Ve_h$, y VA_i es la suma de todos los submódulos de V isomorfos a I_i.*

DEMOSTRACIÓN: Llamemos V_i a la suma de todos los submódulos de V isomorfos a I_i. Si W es cualquier submódulo simple de V, entonces $WA = W$, luego W ha de ser isomorfo a algún I_i, pues de lo contrario sería $WA_i = 0$ (por el teorema 3.6) y también $WA = 0$.

Como V es semisimple, concluimos que $V = V_1 + \cdots + V_h$. Además, como V_i es suma de submódulos isomorfos a I_i, tenemos que $V_i e_j = 0$ si $i \neq j$, mientras que $V_i e_i = V_i$ (pues $v_i e_i = v_i(e_1 + \cdots + e_h) = v_i$). Por lo tanto, $V_i = V_i e_i = V_i A_i$. Sólo falta probar que la suma es directa, pero si $v_1 + \cdots + v_h = 0$, con $v_i \in V_i$, entonces

$$0 = 0e_i = v_1 e_i + \cdots + v_h e_i = v_i e_i = v_i(e_1 + \cdots + e_h) = v_i.$$

■

El siguiente paso para determinar la estructura de los anillos semisimples es estudiar los anillos A_i, que son anillos semisimples con una única clase de isomorfía de módulos simples.

Teorema 3.9 *Sea A un anillo semisimple con una única clase de isomorfía de ideales simples. Entonces:*

a) Los únicos ideales biláteros de A son 0 y A.

b) Si I es un ideal simple de A, entonces $AI = A$.

c) Si I, J son dos ideales simples, existe un $a \in A$ tal que $aI = J$.

DEMOSTRACIÓN: Veamos primero la propiedad c). Como A es semisimple, existe un ideal I' tal que $A = I \oplus I'$. Sea $\pi : A \longrightarrow I$ la proyección. Por hipótesis existe un isomorfismo $f : I \longrightarrow J$. Entonces, para cada $x \in I$, se cumple que $f(x) = f(\pi(x)) = f(\pi(1x)) = f(\pi(1))x = ax$, luego $J = aI$.

Esto prueba que todo J está en AI, lo cual, aplicado a los sumandos de una descomposición de A en suma de ideales simples, nos da que $AI = A$.

Un ideal bilátero L es en particular un A-módulo, luego, si es no nulo, se descompone en suma de ideales simples. En particular, existe un ideal simple $I \subset L$, pero por c) contiene a todos los demás, luego $L = A$. ■

Definición 3.10 Si A es un anillo y M es un A-módulo, definimos el *anulador* de M como el ideal

$$\mathrm{An}(M) = \{a \in A \mid Ma = 0\}.$$

Un A-módulo M es *fiel* si $\mathrm{An}(M) = 0$.

Ejercicio: Si M es un A-módulo e I es un ideal tal que $I \subset \mathrm{An}(M)$, entonces M es un A/I-módulo con el producto definido de forma natural.

Teorema 3.11 *Sea A un anillo semisimple con una única clase de isomorfía de ideales simples. Si V es un A-módulo simple, entonces V es fiel y, para todo ideal simple I de A, se cumple que $VI = V$.*

DEMOSTRACIÓN: Por el teorema anterior,

$$VI = (VA)I = V(AI) = VA = V.$$

Si $a \in \mathrm{An}(V)$, entonces $Va = 0$, luego $VAaA = VaA = 0A = 0$. Por consiguiente, no puede ser $AaA = A$ y, puesto que AaA es un ideal bilátero, ha de ser $AaA = 0$, lo que implica que $a = 0$. ∎

Veremos que la existencia de módulos simples y fieles tiene consecuencias importantes sobre la estructura del anillo. Para ello necesitamos estudiar los módulos simples. Empezamos por la versión abstracta del lema de Schur (compárese con 2.7):

Teorema 3.12 (Lema de Schur) *Sea A un anillo y sean V, W dos A-módulos simples. Entonces $\mathrm{Hom}_A(V, W)$ es nulo si $V \ncong W$ y es un anillo de división si $V = W$.*

DEMOSTRACIÓN: Es trivial: si $f : V \longrightarrow W$ es un homomorfismo de A-módulos no nulo, entonces su núcleo ha de ser nulo porque V es simple, y su imagen ha de ser todo W porque W es simple, luego f es un isomorfismo, luego si $V = W$ tiene inverso en el anillo de endomorfismos. ∎

De este modo, si V es un A-módulo simple, el anillo $D = \mathrm{End}_A(V)$ de los endomorfismos de V como A-módulo es un anillo de división. Ahora bien, podemos considerar a V como D-espacio vectorial con el producto $vf = f(v)$, lo cual nos permite considerar el anillo $\mathrm{End}_D(V)$ de los endomorfismos de V como D-espacio vectorial. Ahora probamos un resultado fundamental:

Teorema 3.13 (Teorema de densidad de Jacobson) *Sea A un anillo, sea V un A-módulo simple y sea $D = \mathrm{End}_A(V)$ el anillo de endomorfismos de V. Entonces, dados $f \in \mathrm{End}_D(V)$ y $c_1, \ldots, c_n \in V$, existe un $a \in A$ tal que $f(c_i) = c_i a$ para todo i.*

DEMOSTRACIÓN: Sea V^n la suma directa de n copias de V, que es un A-módulo semisimple. Definimos $f^n : V^n \longrightarrow V^n$ como el endomorfismo dado por $f^n(v_1, \ldots, v_n) = (f(v_1), \ldots, f(v_n))$. Llamemos $\mathrm{End}_A(V^n)$.

Observemos que cada $\phi \in \mathrm{End}_A(V^n)$ está completamente determinado por sus restricciones $\phi_i : V \longrightarrow V^n$ a cada sumando de V^n, las cuales a su vez están determinadas por sus composiciones con las proyecciones, que son endomorfismos $\phi_{ij} \in D$, de modo que

$$\phi(v_1, \ldots, v_n) = \Big(\sum_i \phi_{ij}(v_i)\Big)_j.$$

Como $f \in \mathrm{End}_D(V)$, se cumple que

$$f(\phi_{ij}(v_i)) = f(v_i\phi_{ij}) = f(v_i)\phi_{ij} = \phi_{ij}(f(v_i)),$$

de donde se sigue que $f^n(\phi(v)) = \phi(f^n(v))$ para todo $\phi \in \mathrm{End}_A(V^n)$ y todo $v \in V^n$.

Sea $c = (c_i) \in V^n$. Como V^n es un A-módulo semisimple, podemos descomponerlo en la forma $V^n = \langle c\rangle \oplus W$, para cierto A-submódulo W. Sea $\pi : V^n \longrightarrow cA$ la proyección en el primer sumando. Así, $\pi \in \mathrm{End}_A(V^n)$. Por consiguiente,

$$f^n(c) = f^n(\pi(c)) = \pi(f^n(c)) \in cA,$$

luego existe un $a \in A$ tal que $f^n(c) = ca$. Explícitamente, esto significa que $f(c_i) = c_i a$. ∎

Como consecuencia:

Teorema 3.14 *Sea A un anillo y V un A-módulo simple y fiel y consideremos el anillo de división $D = \mathrm{End}_A(V)$. Si V es un D-espacio vectorial de dimensión finita, entonces tenemos un isomorfismo de anillos $A \cong \mathrm{End}_D(V)$.*

Demostración: Sea $v_1, \ldots, v_n$ una D-base de V. Por el teorema anterior, si $f \in \mathrm{End}_D(V)$, existe un $a \in A$ tal que $f(v_i) = v_i a$ para todo i. Esto implica que $f(v) = va$ para todo $v \in V$, luego el homomorfismo de anillos $\phi : A \longrightarrow \mathrm{End}_D(V)$ dado por $\phi(a)(v) = va$ es un epimorfismo. Si a está en su núcleo, entonces $va = 0$ para todo $v \in V$, luego $a \in \mathrm{An}(V) = 0$. Así pues, ϕ es un isomorfismo. ∎

Ahora podemos enlazar con el teorema 3.11:

Teorema 3.15 *Sea A un anillo semisimple con una única clase de isomorfía de ideales, sea V un A-módulo simple y sea $D = \mathrm{End}_A(V)$. Entonces se cumple que $A \cong \mathrm{End}_D(V)$.*

Demostración: El teorema 3.11 nos da que V es fiel. Por el teorema anterior, sólo hemos de probar que V es un D-espacio vectorial de dimensión finita. En caso contrario, sean $\{v_n\}_{n\geq 0}$ elementos de V linealmente independientes sobre D. Basta considerar los ideales

$$I_t = \{a \in A \mid v_0 a = v_1 a = \cdots = v_t a = 0\}.$$

Podemos tomar $f \in \mathrm{End}_D(V)$ que cumpla $f(v_1) = \cdots = f(v_t) = 0$ y $f(v_{t+1}) = 1$, y el teorema 3.13 nos da entonces un $a \in I_t \setminus I_{t+1}$. Por consiguiente, tenemos una cadena de ideales

$$\cdots \subsetneq I_3 \subsetneq I_2 \subsetneq I_1 \subsetneq I_0 \subset A,$$

pero esto es imposible, ya que A es semisimple, luego tiene longitud finita y, en particular, es artiniano. ∎

Observemos que $V \cong D^n$ (como espacio vectorial por la derecha), por lo que $A \cong \mathrm{End}_D(V) \cong \mathrm{End}_D(D^n)$. Ahora necesitamos reparar en cierta sutileza sobre la correspondencia entre endomorfismos de un espacio vectorial y sus matrices en una base prefijada.

Si consideráramos a D^n como espacio vectorial por la izquierda (que no es nuestro caso), la matriz asociada a un endomorfismo $f \in \mathrm{End}_D(D^n)$ respecto de la base canónica es la matriz $M(f)$ que cumple $f(v) = vM(f)$, para todo $v \in D^n$, de modo que $M(fg) = M(f)M(g)$, por lo que la aplicación $f \mapsto M(f)$ es un isomorfismo $\mathrm{End}_D(D^n) \cong \mathrm{Mat}_n(D)$.

Sin embargo, si consideramos a D^n como espacio vectorial por la derecha, las aplicaciones $v \mapsto vA$ no son lineales (pues los escalares no pueden "salir" por la derecha), por lo que la matriz de un endomorfismo f ha de definirse como la que cumple $f(v)^t = M(f)v^t$, pero ahora sucede que $M(fg) = M(g)M(f)$, por lo que la aplicación $f \mapsto M(f)$ ya no es un homomorfismo de anillos.[2]

Para conseguir un isomorfismo en este caso observamos que, en general, si D es cualquier anillo, podemos definir el *anillo opuesto* D^{op} como el anillo sobre el mismo conjunto D con la misma suma, pero con el producto dado por $a \cdot b = ba$. Es fácil ver que si D es un anillo de división, entonces D^{op} también lo es y, dadas dos matrices $P, Q \in \mathrm{Mat}_n(D)$, tenemos que

$$PQ = \big(\sum_k p_{ik}q_{kj}\big) = \big(\sum_k q^t_{jk} \cdot p^t_{ki}\big) = (Q^t \cdot P^t)^t,$$

donde el producto $Q^t \cdot P^t$ es el del anillo $\mathrm{Mat}_n(D^{\mathrm{op}})$. De este modo,

$$M(fg)^t = (M(g)M(f))^t = M(f)^t \cdot M(g)^t,$$

por lo que la aplicación $f \mapsto M(f)^t$ determina un isomorfismo

$$\mathrm{End}_D(D^n) \cong \mathrm{Mat}_n(D^{\mathrm{op}}).$$

Teniendo esto en cuenta, el teorema siguiente es ya inmediato:

Teorema 3.16 (Wedderburn) *Sea A un anillo semisimple.*

a) Podemos descomponer $A = A_1 \oplus \cdots \oplus A_n$, donde los A_i son anillos (unitarios) tales que $A_iA_j = 0$ cuando $i \neq j$.

b) $A_i \cong \mathrm{Mat}_{n_i}(D_i^{\mathrm{op}})$, donde D_i es el anillo de división $D_i = \mathrm{End}_A(V_i)$, para cierto A-módulo simple V_i y $n_i = \dim_{D_i}(V_i)$.

c) Todo A-módulo simple es isomorfo a un único V_i.

d) Se cumple que $V_jA_i = 0$ si $i \neq j$, mientras que $V_iA_i = V_i$.

Notemos que, en virtud del teorema 3.15 y las observaciones posteriores, los isomorfismos $A_i \cong \mathrm{Mat}_{n_i}(D_i^{\mathrm{op}})$ son equivalentes a $A_i \cong \mathrm{End}_{D_i}(V_i)$ y, como se ve en la prueba de 3.14, el isomorfismo es el que a cada $a \in A_i$ le asigna la

[2]Para que lo fuera, tendríamos que definir el producto en $\mathrm{End}_D(D^n)$ como $(fg)(v) = f(g(v))$, pero, si definiéramos así la composición de aplicaciones, a la hora de considerar representaciones de grupos tendríamos que tratar con módulos por la izquierda, y volveríamos a tener el mismo problema.

multiplicación por a en V_i. Por consiguiente, la descomposición de A puede expresarse como un isomorfismo

$$\rho : A \longrightarrow \bigoplus_{i=1}^{n} \mathrm{End}_{D_i}(V_i),$$

donde la proyección i-ésima $\rho_i(a)$ es la multiplicación por a en V_i.

Como complemento al teorema de Wedderburn, vamos a probar el recíproco, es decir, que todo anillo cuya estructura sea la descrita por el teorema anterior es semisimple.

Teorema 3.17 *Si D es un anillo de división, el anillo $A = \mathrm{Mat}_n(D)$ es semisimple, y todos los A-módulos simples son isomorfos a $V = D^n$ con el producto usual de vector × matriz. Además, $A \cong \mathrm{End}_{D^{\mathrm{op}}}(V)$ y $D^{\mathrm{op}} \cong \mathrm{End}_A(V)$.*

Demostración: Es claro que si $v \in V$ es no nulo, se cumple que $vA = V$, luego V es un A-módulo simple. Fijemos una base $v_1, \ldots, v_n$ de V y definamos $\phi : A \longrightarrow V^n$ mediante $\phi(M) = (v_1M, \ldots, v_nM)$. Es claro que ϕ es un isomorfismo de A-módulos, luego A se descompone como suma directa de n ideales simples isomorfos a V. Esto prueba que A es semisimple y que tiene una única clase de isomorfía de A-módulos simples.

Observemos ahora que, para cada $d \in D$, podemos definir $\phi_d \in \mathrm{End}_A(V)$ mediante $\phi_d(v) = dv$ y, claramente, la aplicación $d \mapsto \phi_d$ determina un monomorfismo de anillos $D^{\mathrm{op}} \longrightarrow \mathrm{End}_A(V)$. Vamos a ver que es suprayectivo.

Para ello tomamos $\phi \in \mathrm{End}_A(V)$ y $v_0 \in V$ no nulo. Sea $V = Dv_0 \oplus W$ donde W es un D-espacio vectorial por la izquierda. Sea $\pi : V \longrightarrow Dv_0$ la proyección. Se trata de una aplicación lineal que puede calcularse con una matriz $M \in A$, es decir, $\pi(v) = vM$, para todo $v \in V$. Por consiguiente,

$$\phi(v_0) = \phi(\pi(v_0)) = \phi(v_0M) = \phi(v_0)M = \pi(\phi(v_0)) \in Dv_0,$$

luego existe un $d \in D$ tal que $\phi(v_0) = dv_0$. En principio, d depende de v_0, pero, para cualquier otro $v \in V$, existe una matriz $M \in A$ tal que $v = v_0M$, luego

$$\phi(v) = \phi(v_0M) = \phi(v_0)M = dv_0M = dv = \phi_d(v).$$

Así pues, $\phi = \phi_d$ y, por lo tanto, $D^{\mathrm{op}} \cong \mathrm{End}_A(V)$. El teorema 3.15 implica entonces que $A \cong \mathrm{End}_{D^{\mathrm{op}}}(V)$. ∎

Incidentalmente hemos demostrado que los anillos de matrices están determinados por su estructura de anillo:

Teorema 3.18 *Si D y E son anillos de división tales que $\mathrm{Mat}_m(D) \cong \mathrm{Mat}_n(E)$, entonces $m = n$ y $D \cong E$.*

Demostración: Llamemos $A = \mathrm{Mat}_m(D)$ y sea V un A-módulo simple. El teorema anterior nos da que $D^{\mathrm{op}} \cong \mathrm{End}_A(V) \cong E^{\mathrm{op}}$, luego $D \cong E$. Además, $m = \dim_D V = n$. ∎

Otra consecuencia destacable es la siguiente:

Teorema 3.19 *Todo anillo semisimple por la derecha lo es también por la izquierda, y viceversa.*

DEMOSTRACIÓN: Hemos probado que los anillos de matrices sobre un anillo de división son semisimples por la derecha, pero, cambiando sistemáticamente izquierda por derecha en el argumento, se prueba que también son semisimples por la izquierda.

Por otra parte, todo anillo semisimple por la derecha es suma directa de anillos de matrices sobre anillos de división, que son semisimples por la izquierda, luego el anillo de partida también lo es. ∎

3.2 El radical de Jacobson

En esta sección determinaremos la "distancia" que hay de un anillo arbitrario a un anillo semisimple. La clave es el concepto de radical de Jacobson:

Definición 3.20 Sea A un anillo. El *radical de Jacobson* de A, denotado por $J(A)$, es la intersección de todos los ideales derechos maximales[3] de A.

El teorema siguiente prueba, entre otras cosas, que $J(A)$ es también la intersección de los ideales izquierdos maximales:

Teorema 3.21 *Si A es un anillo y $x \in A$, las afirmaciones siguientes son equivalentes:*

a) $x \in J(A)$.

b) x *pertenece a todo ideal maximal derecho de* A.

c) $1 - xa$ *tiene inverso por la derecha, para todo* $a \in A$.

d) x *está en el anulador de todos los* A*-módulos simples por la derecha.*

Las afirmaciones anteriores son válidas también cambiando "derecha" por "izquierda". En particular, $J(A)$ *es un ideal bilátero de* A.

DEMOSTRACIÓN: a) $\Leftrightarrow$ b) es la definición de $J(A)$.

b) $\Rightarrow$ c) si $1 - xa$ no tiene inverso por la derecha, entonces $1 - xa$ genera un ideal derecho distinto de A, luego está contenido en un ideal maximal derecho I. Por hipótesis $x \in I$, pero entonces $xa \in I$ y $1 \in I$, contradicción.

c) $\Rightarrow$ d) Sea M un A-módulo simple por la derecha tal que $x \notin \mathrm{An}(M)$. Entonces existe $m \in M$ tal que $mx \neq 0$. Como M es simple, $M = \langle mx \rangle$. En particular, existe un $a \in A$ tal que $mxa = m$, luego $m(1-xa) = 0$. Como $1-xa$ tiene inverso por la derecha, $m = 0$, luego $mx = 0$, contradicción.

[3]Notemos que el lema de Zorn garantiza la existencia de ideales derechos maximales en cualquier anillo unitario, no necesariamente conmutativo.

d) ⇒ b) Si I es un ideal maximal derecho de A, entonces A/I es un A-módulo simple con anulador I, luego $x \in I$ por hipótesis.

Nos falta probar que todo lo dicho es válido también por la izquierda. Para ello observamos en primer lugar que la propiedad d) afirma que $J(A)$ es la intersección de los anuladores de todos los A-módulos simples por la derecha. Ahora bien, es inmediato que, si M es un A-módulo derecho, entonces $\mathrm{An}(M)$ es un ideal bilátero, luego $J(A)$ es intersección de ideales biláteros de A y, por consiguiente, es un ideal bilátero.

Ahora probamos que $x \in J(A)$ es también equivalente a:

e) $1 - axb$ *es una unidad, para todo* $a, b \in A$.

Obviamente, e) ⇒ c).

Si $x \in J(A)$, entonces $axb \in J(A)$, luego para probar e) basta ver que si $x \in J(A)$ entonces $1 - x$ es una unidad de A, es decir, que tiene inverso tanto por la derecha como por la izquierda. Por c) sabemos que tiene inverso u por la derecha, de modo que $(1 - x)u = 1$, o también, $u = 1 + xu$.

Como $x \in J(A)$, la propiedad c) nos da que $u = 1 + xu$ tiene inverso por la derecha, es decir, que existe $v \in A$ tal que $uv = 1$. Así

$$1 - x = (1 - x)1 = (1 - x)uv = v,$$

luego $u(1 - x) = uv = 1$, de modo que u es el inverso de $1 - x$ tanto por la derecha como por la izquierda.

Ahora basta observar que la condición e) no hace distinción alguna entre izquierda y derecha, por lo que si definimos $J_i(A)$ como la intersección de los ideales maximales izquierdos de A, podemos demostrar todas las equivalencias a) ⇒ b) ⇒ c) ⇒ d) ⇒ e) cambiando "derecha" por "izquierda" en todo momento (y $J(A)$ por $J_i(A)$), pero como e) permanece inalterada, concluimos que las diez afirmaciones —o nueve, si no contamos dos veces a e)— son equivalentes entre sí y, en particular, que $J(A) = J_i(A)$. ∎

A partir de aquí razonaremos con ideales y módulos por la derecha, pero todo lo dicho será válido igualmente por la izquierda.

Para anillos de longitud finita tenemos otra caracterización de $J(A)$. Un ideal I de un anillo es *nilpotente* si existe un $n \geq 1$ tal que $I^n = 0$.

Teorema 3.22 *Si A es un anillo de longitud finita, entonces $J(A)$ es el máximo ideal nilpotente de A.*

Demostración: Consideremos una serie de composición de A:

$$0 = I_0 \subset I_1 \subset \cdots \subset I_n = A.$$

Como los factores I_i/I_{i-1} son simples, tenemos que $(I_i/I_{i-1})J(A) = 0$ o, lo que es lo mismo, $I_iJ(A) \subset I_{i-1}$. Por consiguiente,

$$J(A)^n = I_nJ(A)^n \subset I_{n-1}J(A)^{n-1} \subset \cdots \subset I_1J(A) \subset I_0 = 0,$$

luego $J(A)^n = 0$. Esto prueba que $J(A)$ es nilpotente. Ahora tomemos un ideal nilpotente arbitrario I y veamos que $I \subset J(A)$.

Si $x \in I$ y $a \in A$, hemos de ver que $1 - xa$ tiene inverso por la derecha. De hecho, como $xa \in I$, basta ver que $1 - x$ tiene inverso por la derecha. Si $I^n = 0$, también $x^n = 0$, luego

$$(1 - x)(1 + x + \cdots + x^{n-1}) = 1 - x^n = 1.$$

Así pues, $x \in J(A)$. ∎

De este modo, en un anillo A que sea de longitud finita por la izquierda y por la derecha, el radical $J(A)$ contiene a todos los ideales (izquierdos, derechos y biláteros) nilpotentes, aunque esto no significa necesariamente que contenga a todos los elementos nilpotentes del anillo. Para que un elemento nilpotente esté en $J(A)$ ha de generar un ideal nilpotente. Esto sucede, por ejemplo, si $a \in Z(A)$.

Veamos finalmente la conexión con los anillos semisimples:

Teorema 3.23 *Un anillo A es semisimple si y sólo si es artiniano y $J(A) = 0$.*

Demostración: Sabemos que si A es semisimple entonces tiene longitud finita, luego es artiniano. Además, A se descompone como suma directa de ideales simples, y $J(A)$ anula a todos ellos, luego $AJ(A) = 0$, luego $J(A) = 0$.

Supongamos ahora que A es artiniano y cumple $J(A) = 0$. Sea M_1 un ideal maximal de A. Si $M_1 \neq 0$, entonces existe al menos otro ideal maximal M_2 (pues $J(A)$ es la intersección de todos ellos y es nulo), y ha de ser $M_1 \cap M_2 \subsetneq M_1$. Si la intersección es no nula, ha de haber un tercer ideal maximal M_3 tal que $M_1 \cap M_2 \cap M_3 \subsetneq M_1 \cap M_2$, pues de lo contrario sería $J(A) = M_1 \cap M_2 \neq 0$.

Como A es artiniano, esta cadena de ideales no se puede prolongar indefinidamente, luego podemos encontrar n ideales maximales tales que

$$\bigcap_{i=1}^{n} M_i = 0.$$

Sea $I_i = \bigcap_{j \neq i} M_j$. Así, I_i es un ideal tal que $I_i \cap M_i = 0$. En particular, $I_i \not\subset M_i$, luego $A = I_i \oplus M_i$, luego $I_i \cong A/M_i$ es un A-módulo simple. Basta probar que $A = I_1 \oplus \cdots \oplus I_m$.

Todo $a \in A$, se expresa de forma única como $a = u_i + m_i$, con $u_i \in I_i$, $m_i \in M_i$. Entonces

$$a - (u_1 + \cdots + u_n) = (a - u_i) - \sum_{j \neq i} u_j \in M_i,$$

pues $u_j \in I_j \subset M_i$. Por consiguiente,

$$a - (u_1 + \cdots + u_n) \in \bigcap_{i=1}^{n} M_i = 0.$$

Esto prueba que $A = I_1 + \cdots + I_n$. Por último, si

$$u_1 + \cdots + u_n = 0,$$

con $u_i \in I_i$, entonces

$$u_i = -\sum_{j \neq i} u_j \in I_i \cap M_i = 0,$$

luego la suma es directa. ∎

Como consecuencia:

Teorema 3.24 *Si A es un anillo artiniano, entonces $A/J(A)$ es semisimple.*

Demostración: Sabemos que $A/J(A)$ es artiniano. Teniendo en cuenta el teorema anterior, basta observar que $J(A/J(A)) = 0$, por ejemplo, porque los ideales maximales de $A/J(A)$ son los de la forma $I/J(A)$, donde I es un ideal maximal de A, luego la intersección de todos ellos es $J(A)/J(A) = 0$. ∎

Observemos también que si A es un anillo artiniano y V es un A-módulo simple, entonces $J(A)$ anula a V, luego V tiene una estructura natural de $A/J(A)$-módulo simple.

Teorema 3.25 *Si A es un anillo artiniano y M es un A-módulo finitamente generado, entonces M es semisimple si y sólo si $J(A) \subset \mathrm{An}(M)$.*

Demostración: Si M es semisimple, entonces se descompone como suma directa de A-módulos simples, y $J(A)$ los anula a todos, luego también a M. Recíprocamente, si $J(A)$ anula a M, entonces éste admite una estructura natural de $A/J(A)$-módulo finitamente generado, y $A/J(A)$ es semisimple, luego M es un $A/J(A)$-módulo semisimple, y esto implica claramente que es un A-módulo semisimple. ∎

Esto implica a su vez que si M es un A-módulo finitamente generado (donde A es artiniano), entonces $MJ(A)$ es el menor submódulo de M cuyo cociente es semisimple. En efecto, $M/MJ(A)$ es semisimple porque $(M/MJ(A))J(A) = 0$, y si M/N es semisimple entonces $(M/N)J(A) = 0$, luego $MJ(A) \subset N$.

En particular, puesto que $AJ(A) = J(A)$, tenemos que $J(A)$ es el menor ideal derecho (o izquierdo) cuyo cociente es un A-módulo semisimple, y también el menor ideal bilátero cuyo cociente es un anillo semisimple.

Como primera aplicación podemos demostrar el recíproco del teorema de Maschke:

Teorema 3.26 *Si G es un grupo finito y k es un cuerpo tal que $\operatorname{car} k \mid |G|$, entonces $k[G]$ no es semisimple.*

Demostración: Sea $u = \sum_{\sigma \in G} \sigma \in k[G]$. Observamos que

$$u^2 = \sum_{\sigma \in G} \sigma \sum_{\tau \in G} \tau = \sum_{\sigma \in G} \sum_{\tau \in G} \sigma\tau = \sum_{\sigma \in G} \sum_{\tau \in G} \tau = |G|u = 0.$$

Por otra parte, $u \in Z(k[G])$ y $u \neq 0$, luego el ideal $I = u(k[G])$ cumple $I^2 = 0$, $I \neq 0$, luego $0 \subsetneq I \subset J(k[G])$, luego $J(k[G]) \neq 0$ y $k[G]$ no es semisimple. ∎

Vamos a calcular explícitamente el radical de Jacobson de un álgebra $k[G]$ cuando G es un p-grupo y $\operatorname{car} k \mid |G|$. Para ello conviene observar primero unos hechos válidos en general:

Definición 3.27 Sea G un grupo finito y k un cuerpo, definimos $T : k[G] \longrightarrow k$ como la aplicación lineal determinada por que $T(\sigma) = 1$ para todo $\sigma \in G$ o, equivalentemente,

$$T\Big(\sum_{\sigma\in G} a_\sigma \sigma\Big) = \sum_{\sigma\in G} a_\sigma.$$

Claramente, $T(\sigma x) = T(x\sigma) = T(x)$, para todo $x \in k[G]$ y todo $\sigma \in G$. Esto implica que el núcleo de T es un ideal bilátero $M(G) \subset k[G]$, claramente maximal, pues $k[G]/M(G) \cong k$. Es fácil ver que $M(G) = \langle \sigma - 1 \mid \sigma \in G\rangle_k$.

Por otra parte, podemos definir el ideal bilátero $I(G) = \Big\langle \sum_{\sigma\in G} \sigma\Big\rangle_k$, y se comprueba inmediatamente que si $\operatorname{car} k \nmid |G|$, entonces

$$k[G] = M(G) \oplus I(G).$$

Por otra parte:

Ejemplo *Si G es un p-grupo y k es un cuerpo de característica p, entonces*

$$J(k[G]) = M(G).$$

En efecto, en estas condiciones $M(G)$ es el único ideal maximal derecho de $k[G]$, pues si M' es cualquier ideal derecho maximal, el teorema 1.14 nos da que $k[G]/M' \cong k$, considerando a k como $k[G]$-módulo trivial. Esto implica que $[1]\sigma = [1]$ para todo $\sigma \in G$, luego $\sigma - 1 \in M'$, luego $M(G) \subset M'$, luego $M(G) = M'$, por la maximalidad de $M(G)$. ∎

Veamos otra caracterización de $J(A)$ o, más en general, del submódulo $MJ(A)$ de un A-módulo dado.

Definición 3.28 Si A es un anillo y M un A-módulo, un submódulo N de M es *inesencial* en M si el único submódulo N' de M que cumple $N + N' = M$ es $N' = M$.

Obviamente, todo submódulo de un submódulo inesencial es inesencial. Este concepto está estrechamente relacionado con el de homomorfismo esencial, definido en 1.56:

Teorema 3.29 *Un epimorfismo de módulos $f : M \longrightarrow M'$ es esencial si y sólo si su núcleo es inesencial.*

DEMOSTRACIÓN: Basta tener en cuenta que si N es el núcleo de f y N' es un submódulo de M, entonces $f[N'] = M'$ si y sólo si $M = N + N'$. ∎

La relación con el radical de Jacobson es la siguiente:

Teorema 3.30 *Sea A un anillo de longitud finita y M un A-módulo finitamente generado. Entonces $MJ(A)$ es el mayor submódulo inesencial de M.*

DEMOSTRACIÓN: Sea N la intersección de todos los submódulos maximales de M (es decir, de los penúltimos términos de las series de composición de M). Vamos a probar que N es el mayor submódulo inesencial de M y que $MJ(A) = N$.

Si $N + M' = M$ pero $M' \subsetneq M$, entonces (completando una serie de composición) podemos tomar un submódulo maximal $M' \subset M'' \subsetneq M$, que también cumplirá $N + M'' = M$, pero esto es absurdo, puesto que $N \subset M''$, luego la suma se reduce a $M'' = M$. Así pues, N es inesencial.

Si $N' \subset M$ es un submódulo inesencial y M' es un submódulo maximal de M, entonces $M' \subset N' + M' \subsetneq M$, luego ha de ser $M' = N' + M'$, luego $N' \subset M'$. Como esto vale para todo M', de hecho $N' \subset N$.

Por otra parte, si M' es un submódulo maximal de M, entonces M/M' es simple, luego $MJ(A) \subset M'$, luego $MJ(A) \subset N$.

El cociente $M/MJ(A)$ es semisimple, luego podemos descomponerlo como

$$M/MJ(A) = M_1/MJ(A) \oplus \cdots \oplus M_h/MJ(A),$$

donde todos los sumandos son simples. Si llamamos $N_i = \bigoplus_{j \neq i} M_j$, entonces M/N_i es simple, luego N_i es maximal, luego $N \subset \bigcap_i N_i = MJ(A)$. ∎

3.3 Cuerpos de escisión

Si k es un cuerpo y A es una k-álgebra de dimensión finita, para cada extensión de cuerpos K/k podemos considerar el producto tensorial $A_K = K \otimes_k A$, que tiene una estructura natural de K-álgebra dada por

$$(\alpha \otimes a)(\beta \otimes b) = (\alpha\beta) \otimes (ab).$$

Si V es un A-módulo finitamente generado, entonces $V_K = K \otimes_k V$ tiene una estructura natural de A_K-módulo finitamente generado dado por

$$(\alpha \otimes v)(\beta \otimes a) = (\alpha\beta) \otimes (va).$$

Observemos que, si G es un grupo finito, $k[G]_K \cong K[G]$ y V_K es el mismo definido en 1.6.

Definición 3.31 Si A es una k-álgebra de dimensión finita y V es un A-módulo simple, diremos que es *absolutamente simple*[4] si V_K es simple para toda extensión de cuerpos K/k. Diremos que k es un *cuerpo de escisión* de A si todo A-módulo simple es absolutamente simple. Si G es un grupo finito, se dice que k es un *cuerpo de escisión* de G si lo es del álgebra $k[G]$.

Observemos que estas definiciones generalizan a 2.59 y 2.61. Aquí trabajamos en el contexto de k-álgebras arbitrarias y no en el de álgebras $k[G]$ porque así podremos aplicar el teorema siguiente, que nos permite trabajar con módulos fieles:

Teorema 3.32 *Si A es una k-álgebra de dimensión finita y V es un A-módulo, consideramos el homomorfismo de k-álgebras $\phi : A \longrightarrow \mathrm{End}_k(V)$ que a cada $a \in A$ le asigna el endomorfismo dado por $\phi_a(v) = va$. Si llamamos B a su imagen, entonces B es una k-álgebra finitamente generada tal que V es un B-módulo fiel. Además V es simple o absolutamente simple como A-módulo si y sólo si lo es como B-módulo.*

Demostración: Es claro que V es un B-módulo fiel. Basta probar que si K/k es una extensión de cuerpos, entonces V_K es un A_K-módulo simple si y sólo si es un B_K-módulo simple.

Fijemos una k-base $v_1, \ldots, v_n$ de V, una k-base $a_1, \ldots, a_r$ del anulador $\mathrm{An}(V)$ y completemos ésta hasta una k-base $a_1, \ldots, a_m$ de A. Entonces B tiene como k-base a $\phi_{a_{r+1}}, \ldots, \phi_{a_m}$.

Un subespacio de V_K será un A_K-submódulo si y sólo si es estable para la multiplicación por los elementos de la base $1 \otimes a_i$, mientras que será un B_K submódulo si es estable para la multiplicación por los elementos de la base $1 \otimes \phi_{a_i}$ (para $i > r$).

Ahora bien, si $i \leq r$, tenemos que $(\alpha \otimes v_j)(1 \otimes a_i) = \alpha \otimes (v_j a_i) = 0$, luego, en realidad, los A_K-submódulos de V_K son los subespacios estables para el producto por los $1 \otimes a_i$ con $i > r$. Pero resulta que, para $i > r$,

$$(\alpha \otimes v_j)(1 \otimes a_i) = \alpha \otimes v_j a_i = \alpha \otimes v_j \phi_{a_i} = (\alpha \otimes v_j)(1 \otimes \phi_{a_i})$$

luego, por linealidad, $v(1 \otimes a_i) = v(1 \otimes \phi_{a_i})$ para todo $v \in V_K$, luego los A_K-submódulos de V_K son los mismos que los B_K-submódulos y, en particular, V es simple como A_K-módulo si y sólo si lo es como B_K-módulo. ∎

Observemos que si V es un $k[G]$-módulo, el homomorfismo ϕ del teorema anterior no es sino la representación lineal $\rho : G \longrightarrow \mathrm{End}_k(V)$ asociada a V extendida por linealidad a $k[G]$.

A los módulos simples y fieles les podemos aplicar el teorema 3.14:

[4]Recordemos que los módulos simples se llaman también irreducibles y, del mismo modo, los módulos absolutamente simples se llaman también *absolutamente irreducibles*. El término "simple" es más habitual en teoría de anillos, mientras que "irreducible" es el usual en teoría de representaciones.

Teorema 3.33 *Sea k un cuerpo y A una k-álgebra de dimensión finita. Si V es un A-módulo simple y fiel, entonces tiene dimensión finita sobre k. Además $D = \mathrm{End}_A(V)$ es un anillo de división que contiene a k en su centro, también tiene dimensión finita sobre k y si $n = \dim_D V$,*

$$A \cong \mathrm{End}_D(V) \cong \mathrm{Mat}_n(D^{\mathrm{op}}).$$

Demostración: Si V es fiel, el homomorfismo $\phi : A \longrightarrow \mathrm{End}_k(V)$ es un monomorfismo de álgebras. Hemos de probar que su imagen es $\mathrm{End}_D(V)$. En primer lugar observamos que $\phi[k] \subset \mathrm{End}_A(V) = D$, porque k está en el centro de A. Así pues, identificando cada $\alpha \in k$ con la homotecia ϕ_α, podemos considerar que $k \subset D$. Las homotecias conmutan con todos los elementos de $\mathrm{End}_k(V)$, luego en particular con los elementos de D, luego k está en el centro de D.

Así pues, $k \subset D \subset \mathrm{End}_k(V)$. Todos los ideales de A son k-espacios vectoriales de dimensión finita, al igual que sus factores de composición, luego también los A-módulos simples. Si $m = \dim_k V$, entonces $\mathrm{End}_k(V)$ tiene dimensión m^2, luego $\dim_k D$ es finita. El teorema 3.14 nos da que $A \cong \mathrm{End}_D(V)$, y el segundo isomorfismo está probado en la discusión previa al teorema 3.16. ∎

Ahora podemos dar una caracterización de los A-módulos absolutamente simples:

Teorema 3.34 *Sea A una k-álgebra de dimensión finita y V un A-módulo simple. Se cumple que V es absolutamente simple si y sólo si $\mathrm{End}_A(V) = k$.*

Demostración: Sea B la imagen de A por el homomorfismo del teorema 3.32. Según dicho teorema, V es absolutamente simple como A-módulo si y sólo si lo es como B-módulo, y también es claro que $\mathrm{End}_A(V) = \mathrm{End}_B(V)$. Como V es un B-módulo fiel, cambiando A por B, no perdemos generalidad si suponemos que V es un A-módulo fiel.

A continuación demostramos que V_K es fiel, para toda extensión K/k. Fijemos una base $a_1, \ldots, a_m$ de A y una base $v_1, \ldots, v_n$ de V. Pongamos que

$$v_j a_i = \sum_l \alpha_{ijl} v_l,$$

para ciertos $\alpha_{ijl} \in k$. Así,

$$v_j \sum_i \beta_i a_i = \sum_l \Big(\sum_i \beta_i \alpha_{ijl}\Big) v_l.$$

Que V sea fiel significa que si $\sum_i \beta_i \alpha_{ijl} = 0$ para todo j y l, entonces $\beta_i = 0$ para todo i. A su vez, esto equivale a que las matrices $M_i = (\alpha_{ijl})_{jl}$ sean linealmente independientes sobre k.

Análogamente, considerando las bases $1 \otimes a_i$ y $1 \otimes v_j$, concluimos que V_K es fiel si y sólo si las matrices M_i son linealmente independientes sobre K. Considerando las matrices como vectores en k^{n^2}, las m matrices forman una matriz $m \times n^2$, y la independencia lineal de sus filas equivale a que existen m

columnas que forman una submatriz cuadrada de determinante no nulo. Esto sucede sobre k y, obviamente, sigue siendo cierto sobre K, luego las matrices siguen siendo linealmente independientes sobre K.

El teorema 3.33 nos da que, si $D = \mathrm{End}_A(V)$, entonces $A \cong \mathrm{Mat}_m(D^{\mathrm{op}})$, donde $m = \dim_D V$. Entonces

$$n = \dim_k V = (\dim_k D)(\dim_D V) = m \dim_k D$$

y, por otra parte, $\dim_k A = m^2 \dim_k D$.

Supongamos ahora que V es absolutamente irreducible y demostremos que $D = \mathrm{End}_A(V) = k$. Basta probar que $\dim_k D = 1$.

Si K es una clausura algebraica de k, sabemos que V_K es un A_K-módulo simple y fiel, luego podemos aplicarle también el teorema 3.33, según el cual $D' = \mathrm{End}_{A_K}(V_K)$ es un anillo de división que tiene dimensión finita sobre K.

Ahora bien, si $\alpha \in \mathrm{End}_{A_K}(V_K)$, entonces $K(\alpha)$ es un cuerpo y es una extensión finita de K, luego $\alpha \in K$, lo que prueba que $D' = K = D'^{\mathrm{op}}$, luego, también por 3.33, resulta que $A_K \cong \mathrm{Mat}_n(K)$, donde $n = \dim_K(V_K) = \dim_k V$.

Concluimos observando que

$$n^2 = \dim_K A_K = \dim_k A = m^2 \dim_k D,$$

lo cual, juntamente con la igualdad $n = m \dim_k D$, nos da que

$$\dim_k D = \frac{n}{m} = \frac{n^2}{m^2} = (\dim_k D)^2$$

lo cual sólo es posible si $\dim_k D = 1$.

Por último, suponemos que $\mathrm{End}_A(V) = k$ y veamos que V es absolutamente simple. El teorema 3.33 nos da ahora que $A = \mathrm{Mat}_n(k)$. Por lo tanto, si K/k es cualquier extensión, se cumple que $A_K = K \otimes_k \mathrm{Mat}_n(k) \cong \mathrm{Mat}_n(K)$ y V_K es un A_K-módulo de dimensión n, luego ha de ser simple por el teorema 3.17. ∎

En la prueba del teorema anterior se ve que la condición $\mathrm{End}_A(V) = k$ se da siempre que el cuerpo k es algebraicamente cerrado. En particular, tenemos que cualquier cuerpo algebraicamente cerrado es un cuerpo de escisión para cualquier grupo finito.

Teorema 3.35 *Sea G un grupo finito y k un cuerpo tal que $\mathrm{car}\, k \nmid |G|$ y sean $n_1, \ldots, n_h$ los grados de las representaciones irreducibles de G sobre k. Se cumple que k es un cuerpo de escisión para G si y sólo si $n_1^2 + \cdots + n_h^2 = |G|$ y, en tal caso, h es el número de clases de conjugación de G.*

Demostración: Sean $V_1, \ldots, V_h$ representantes de los $k[G]$-módulos simples de G y sea $D_i = \mathrm{End}_G(V_i)$. La hipótesis sobre la característica de k se traduce en que $k[G]$ es semisimple, por lo que el teorema de Wedderburn nos da que

$$k[G] \cong \mathrm{Mat}_{n'_1}(D_1^{\mathrm{op}}) \oplus \cdots \oplus \mathrm{Mat}_{n'_h}(D_h^{\mathrm{op}}),$$

donde cada D_i es un anillo de división que tiene a k en su centro y $\dim_{D_i} V_i = n'_i$, luego $n_i = \dim_k V_i = (\dim_k D_i)n'_i$. Tomando dimensiones sobre k en ambos miembros de la descomposición de $k[G]$, vemos que

$$|G| = n'^2_1 \dim_k D_1 + \cdots + n'^2_h \dim_k D_h = \frac{n_1^2}{m_1} + \cdots + \frac{n_h^2}{m_h},$$

donde $m_i = \dim_k D_i$.

Es claro que la igualdad del enunciado equivale a que $\dim_k D_i = 1$ para todo i, lo cual, por el teorema anterior, equivale a que todos los módulos V_i sean absolutamente simples, es decir, a que k sea un cuerpo de escisión para G. En tal caso, la descomposición de $k[G]$ se reduce a

$$k[G] \cong \mathrm{Mat}_{n_1}(k) \oplus \cdots \oplus \mathrm{Mat}_{n_h}(k).$$

El teorema 1.5 nos da que la dimensión del centro de $k[G]$ sobre k es igual al número de clases de conjugación de G. Por otra parte

$$Z(k[G]) = Z(\mathrm{Mat}_{n_1}(k)) \oplus \cdots \oplus Z(\mathrm{Mat}_{n_h}(k)) = k \oplus \cdots \oplus k = k^h,$$

luego dicha dimensión es h. ∎

En el último paso de la prueba anterior hemos usado que el centro de un anillo de matrices $A = \mathrm{Mat}_n(k)$ está formado por las matrices de la forma αI_n y, por consiguiente, es isomorfo a k. Esto puede probarse directamente sin dificultad, pero ahora podemos dar una prueba conceptual:

El teorema 3.17 nos da que $\mathrm{End}_A(k^n) = k$, donde cada $\alpha \in k$ se identifica con el endomorfismo $v \mapsto v\alpha$. Si $M \in Z(A)$, entonces $v \mapsto vM$ define un A-endomorfismo de k^n, luego existe un $\alpha \in k$ tal que $vM = v\alpha$ para todo $v \in k^n$, luego $M = \alpha I_n$. ∎

Conviene destacar una consecuencia inmediata de los resultados que hemos obtenido:

Teorema 3.36 *Sea A una k-álgebra de dimensión finita y V un A-módulo absolutamente simple. Entonces, el homomorfismo $A \longrightarrow \mathrm{End}_k(V)$ del teorema* 3.32 *es suprayectivo.*

Demostración: Si llamamos B a la imagen de A por el homomorfismo del enunciado, el teorema 3.32 nos da que B es una k-álgebra de dimensión finita y que V es un B-módulo absolutamente simple y fiel. El teorema 3.34 nos da que $\mathrm{End}_B(V) = k$, y el teorema 3.33 implica entonces que $B = \mathrm{End}_k(V)$. ∎

A partir de aquí nos restringiremos al caso de álgebras de tipo $k[G]$. Si k es un cuerpo de escisión para G cuya característica no divida al orden de G, el teorema de Wedderburn (véase la observación posterior) juntamente con el teorema 3.34, nos da el isomorfismo

$$\rho : k[G] \longrightarrow \bigoplus_{i=1}^{n} \mathrm{End}_k(V_i),$$

donde $V_1, \dots, V_n$ son representantes de las clases de isomorfía de $k[G]$-módulos simples, y en el que cada coordenada $\rho_i : k[G] \longrightarrow \mathrm{End}_k(V_i)$ no es sino la representación lineal de G asociada a V_i extendida a $k[G]$ por linealidad. Si eliminamos las hipótesis sobre k tenemos al menos el teorema siguiente:

Teorema 3.37 *Sea G un grupo finito y $\rho : k[G] \longrightarrow \mathrm{End}_k(V)$ una representación lineal irreducible de G sobre un cuerpo k (extendida a $k[G]$ de por linealidad). Para cada $x \in k[G]$, existe un $y \in k[G]$ tal que $\rho(x) = \rho(y)$ y $\rho'(y) = 0$, para toda representación lineal irreducible $\rho' : k[G] \longrightarrow \mathrm{End}_k(W)$ de G sobre k no isomorfa a ρ.*

Demostración: Sean $V_1, \dots, V_n$ representantes de las clases de isomorfía de $k[G]$-módulos simples. Pongamos que $V = V_1$. Sea $A = k[G]/J(k[G])$, que es una k-álgebra semisimple cuyos A-módulos simples son precisamente $V_1, \dots, V_n$. El teorema de Wedderburn nos da un isomorfismo

$$\rho : A \longrightarrow \bigoplus_{i=1}^{n} \mathrm{End}_{D_i}(V_i),$$

cuyas funciones coordenadas ρ_i no son sino las representaciones lineales de G asociadas a los módulos V_i. Basta tomar $y \in k[G]$ que cumpla $[y] = \rho^{-1}(\rho_1(x))$. ∎

Como consecuencia:

Teorema 3.38 *Sea G un grupo finito, sea $k \subset K$ una extensión de cuerpos y sean V, W dos $k[G]$-módulos simples. Si V_K y W_K tienen un factor de composición en común, entonces V y W son isomorfos.*

Demostración: Por el teorema anterior, si los módulos no son isomorfos, podemos tomar $y \in k[G]$ tal que la multiplicación por y sea la identidad en V y el homomorfismo nulo en W, lo cual sigue siendo cierto en V_K y W_K. Por hipótesis, V_K y W_K tienen $K[G]$-submódulos

$$V_{i-1} \subset V_i \subset V_K, \qquad W_{j-1} \subset W_j \subset W_K$$

tales que $V_i/V_{i-1} \cong W_j/W_{j-1}$. Ahora bien, la multiplicación por y en V_K induce el automorfismo identidad, luego lo mismo sucede con la multiplicación por y en V_i/V_{i-1}. Por el contrario, y anula a W_K, luego también anula a W_j/W_{j-1}, luego los factores de composición tienen anuladores distintos, luego no pueden ser isomorfos. ∎

De aquí deducimos algunas propiedades de los cuerpos de escisión:

Teorema 3.39 *Sea G un grupo finito y K/k una extensión de cuerpos. Si k es un cuerpo de escisión de G, entonces K también lo es y, si $V_1, \dots, V_h$ es un sistema de representantes de las clases de isomorfía de $k[G]$-módulos simples, entonces $V_{1K}, \dots, V_{hK}$ es un sistema de representantes de las clases de isomorfía de $K[G]$-módulos simples.*

DEMOSTRACIÓN: Como k es un cuerpo de escisión de G, los $K[G]$-módulos V_{iK} son simples, y son no isomorfos dos a dos, pues si dos de ellos fueran isomorfos, trivialmente tendrían un factor de composición en común, luego los correspondientes $k[G]$-módulos V_i serían isomorfos por el teorema anterior.

Veamos ahora que todo $K[G]$-módulo simple es isomorfo a un V_{iK}. En principio, todo $K[G]$-módulo simple es isomorfo a un factor de composición de $K[G]$, luego basta probar que todo factor de composición de $K[G]$ es isomorfo a un V_{iK}. Para ello observamos que si

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_n = k[G]$$

es una serie de composición de $k[G]$, entonces

$$0 = M_{0K} \subsetneq M_{1K} \subsetneq \cdots \subsetneq M_{nK} = K[G]$$

es una serie de composición de $K[G]$. En efecto, basta tener en cuenta que la sucesión exacta

$$0 \longrightarrow M_{i-1} \longrightarrow M_i \longrightarrow M_i/M_{i-1} \longrightarrow 0$$

sigue siendo exacta al multiplicarla por $\otimes_k K$, de modo que

$$M_{iK}/M_{i-1K} \cong (M_i/M_{i-1})_K.$$

Como M_i/M_{i-1} es isomorfo a un V_i, el miembro derecho de la fórmula anterior es isomorfo a un V_{iK}. En particular es simple. Esto prueba que la segunda serie es realmente una serie de composición de $K[G]$, y además hemos visto que los factores de composición de $K[G]$ son isomorfos a módulos de la forma V_{iK}.

Con esto tenemos probado que todos los $K[G]$-módulos simples son de la forma V_{iK}, lo que prueba a su vez que todos ellos son absolutamente simples, pues sus extensiones de coeficientes son también extensiones de coeficientes de los módulos V_i, luego son simples. Por consiguiente, K es también un cuerpo de escisión de G. ∎

Si no suponemos que k es un cuerpo de escisión de G, partiendo de una serie de composición de $k[G]$ como en la prueba del teorema anterior, obtenemos una serie de $K[G]$ que no es necesariamente una serie de composición de $K[G]$, pero que puede refinarse hasta que lo sea. Esto nos permite concluir que todo $K[G]$-módulo simple es un factor de composición de un $K[G]$-módulo V_{iK}.

Teorema 3.40 *Sea G un grupo finito y K/k una extensión de cuerpos. Si K es un cuerpo de escisión de G, entonces k lo es también si y sólo si todo $K[G]$-módulo simple es isomorfo a un $K[G]$-módulo V_K, para cierto $k[G]$-módulo simple V.*

DEMOSTRACIÓN: Una implicación es inmediata por el teorema anterior. Sea V cualquier $k[G]$-módulo simple y sea W un factor de composición de V_K. Por hipótesis, existe otro $k[G]$-módulo simple V' tal que $W \cong V'_K$. Así pues, V_K

y V'_K tienen un factor de composición en común. El teorema 3.38 nos da que $V \cong V'$, de modo que $V_K \cong W$. Así pues, V_K es absolutamente simple.

Esto implica que V también es absolutamente simple, pues si L/k es una extensión arbitraria (aunque podemos suponer que K y L están contenidos en un mismo cuerpo KL), no puede ocurrir que V_L no sea simple, ya que entonces $V_{KL} = (V_L)_{KL} = (V_K)_{KL}$ tampoco lo sería, en contra de que V_K es absolutamente simple. Por consiguiente, k es un cuerpo de escisión de G. ∎

3.4 Grupos de Grothendieck

Introducimos ahora una herramienta útil para estudiar las representaciones lineales a modo de nexo entre las representaciones propiamente dichas y sus caracteres. El punto de partida es una construcción general que conviene exponer en el contexto de una subcategoría arbitraria[5] $\mathcal{C}$ de la categoría de los A-módulos (por la derecha) finitamente generados, donde A es un anillo prefijado:

Sea $A^{(\mathbb{N})}$ la suma directa de infinitas copias de A, que es un A-módulo libre de rango infinito. Así, para todo objeto $M \in \mathcal{C}$, existe un epimorfismo $A^{(\mathbb{N})} \longrightarrow M$, luego M es isomorfo a un cociente de $A^{(\mathbb{N})}$. Llamamos $\mathcal{B}$ al conjunto[6] de todos los módulos cociente $A^{(\mathbb{N})}/I$ que pertenecen a $\mathcal{C}$. Así, $\mathcal{B} \subset \mathcal{C}$ y para cada $M \in \mathcal{C}$ existe al menos un $M' \in \mathcal{B}$ tal que $M \cong M'$. Ahora llamamos $\mathcal{L}$ al $\mathbb{Z}$-módulo libre de base $\mathcal{B}$, de modo que un elemento arbitrario de $\mathcal{L}$ se expresa de forma única como combinación lineal

$$\sum_{M\in\mathcal{B}} a_M M,$$

donde $a_M \in \mathbb{Z}$ y $a_M = 0$ para todo M salvo a lo sumo para una cantidad finita de ellos.

Consideramos el conjunto $\mathcal{R}$ de todas las ternas $(M', M, M'') \in \mathcal{B}^3$ tales que existe una sucesión exacta

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

de morfismos de $\mathcal{C}$ y

$$\mathcal{R}^* = \{M - M' - M'' \mid (M', M, M'') \in \mathcal{R}\} \subset \mathcal{L}.$$

Por último, definimos el *grupo de Grothendieck* asociado a la categoría $\mathcal{C}$ como el grupo cociente

$$R(\mathcal{C}) = \mathcal{L}/\langle \mathcal{R}^* \rangle .$$

[5]No vamos a necesitar ningún resultado de la teoría de categorías más allá de la mera definición. Si el lector no está familiarizado con ella, sólo necesita saber que cuando hablamos de un "objeto" de $\mathcal{C}$ queremos decir "un A-módulo finitamente generado", o un "A-módulo proyectivo finitamente generado", etc., y que cuando hablamos de un "morfismo" de $\mathcal{C}$ queremos decir un homomorfismo de A-módulos finitamente generados, o de A-módulos proyectivos finitamente generados, etc., según los objetos que compongan $\mathcal{C}$.

[6]Tomamos $\mathcal{B}$ por una cuestión técnica conjuntista: en general el universo de una categoría es una clase propia (que no es un conjunto), y así $\mathcal{B}$ es un conjunto que contiene representantes de todas las clases de isomorfía de los objetos de $\mathcal{C}$.

En primer lugar observamos que si $M \in \mathcal{B}$ es el módulo trivial, entonces tenemos una sucesión exacta

$$0 \longrightarrow M \longrightarrow M \longrightarrow M \longrightarrow 0,$$

luego $M - M - M = -M \in \mathcal{R}^*$, luego $M \in \langle \mathcal{R}^* \rangle$, luego la clase de M en $R(\mathcal{C})$ es la clase nula.

Más en general, si M, $N \in \mathcal{B}$ cumplen que $M \cong N$, entonces tenemos una sucesión exacta

$$0 \longrightarrow 0 \longrightarrow M \longrightarrow N \longrightarrow 0,$$

luego $N - M - 0 \in \mathcal{R}^*$, luego $N - M \in \langle \mathcal{R}^* \rangle$ (porque $0 \in \langle \mathcal{R}^* \rangle$), luego M y N determinan la misma clase de congruencia en el cociente $R(\mathcal{C})$.

En conclusión, cada $M \in \mathcal{C}$ es isomorfo a al menos un módulo $M' \in \mathcal{B}$, que no es necesariamente único, pero dos cualesquiera de ellos determinan la misma clase de congruencia en $R(\mathcal{C})$, luego podemos definir $[M] \in R(\mathcal{C})$ como la única clase de congruencia que contiene módulos isomorfos a M. El teorema siguiente recoge las propiedades básicas del grupo $R(\mathcal{C})$:

Teorema 3.41 *Sea A un anillo y $\mathcal{C}$ una subcategoría de la categoría de los A-módulos finitamente generados.*

a) El grupo de Grothendieck $R(\mathcal{C})$ es un grupo abeliano.

b) Existe una aplicación $[\ ] : \mathcal{C} \longrightarrow R(\mathcal{C})$ cuya imagen es un sistema generador de $R(\mathcal{C})$ y tal que, para toda sucesión exacta en $\mathcal{C}$

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0,$$

se cumple que $[M] = [M'] + [M'']$.

c) Si R es un grupo abeliano y $f : \mathcal{C} \longrightarrow R$ es una aplicación tal que, para toda sucesión exacta en $\mathcal{C}$

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0,$$

se cumple que $f(M) = f(M') + f(M'')$, entonces existe un único homomorfismo de grupos $i : R(\mathcal{C}) \longrightarrow R$ tal que, para todo $M \in \mathcal{C}$, se cumple que $i([M]) = f(M)$.

Demostración: a) es evidente, para probar b) tomamos módulos M_1', M_1, $M_1'' \in \mathcal{B}$ tales que $M' \cong M_1'$, $M \cong M_1$, $M'' \cong M_1''$. Claramente existe una sucesión exacta

$$0 \longrightarrow M_1' \longrightarrow M_1 \longrightarrow M_1'' \longrightarrow 0,$$

luego $M_1 - M_1' - M_1'' \in \mathcal{R}^*$, luego $[M] = [M_1] = [M_1'] + [M_1''] = [M'] + [M'']$.

Para probar c) usamos que $\mathcal{L}$ es un $\mathbb{Z}$-módulo libre de base $\mathcal{B}$, luego podemos definir un homomorfismo de grupos $j : \mathcal{L} \longrightarrow R$ mediante $j(M) = f(M)$. Si $(M', M, M'') \in \mathcal{R}$, entonces

$$j(M - M' - M'') = f(M) - f(M') - f(M'') = 0,$$

luego $\langle \mathcal{R}^* \rangle$ está contenido en el núcleo de j y, por consiguiente, j induce un homomorfismo de grupos $i : R(\mathcal{C}) \longrightarrow R$ que cumple $i([M]) = f(M)$ para todo $M \in \mathcal{B}$.

El mismo razonamiento que hemos empleado con $R(\mathcal{C})$ prueba que si M, $N \in \mathcal{C}$ cumplen $M \cong N$, entonces $f(M) = f(N)$. Por lo tanto, si $M \in \mathcal{C}$, tomamos $M' \in \mathcal{B}$ tal que $M \cong M'$ y sucede que

$$i([M]) = i([M']) = f(M') = f(M).$$

Como los elementos $[M]$ generan $R(\mathcal{C})$, es claro que el homomorfismo i es único. ∎

Las funciones f que cumplen la propiedad c) del teorema anterior se llaman *funciones aditivas.*

Es claro que el grupo $R(\mathcal{C})$ está determinado salvo isomorfismo por las propiedades del teorema anterior. En lo sucesivo no volveremos a mencionar los objetos $\mathcal{L}$, $\mathcal{R}$, etc. que hemos usado en la construcción de $R(\mathcal{C})$. Veamos otras propiedades elementales, cuya prueba no ofrece ninguna dificultad:

Teorema 3.42 *Sea A un anillo y $\mathcal{C}$ una subcategoría de la categoría de los A-módulos finitamente generados. Consideremos el grupo de Grothendieck $R(\mathcal{C})$ y la aplicación canónica $[\ ] : \mathcal{C} \longrightarrow R(\mathcal{C})$. Entonces*

a) $[0] = 0$.

b) Si M, $N \in \mathcal{C}$ cumplen $M \cong N$, entonces $[M] = [N]$.

c) Todo elemento de $R(\mathcal{C})$ se expresa como combinación lineal finita

$$n_1[M_1] + \cdots + n_r[M_r],$$

donde $n_i \in \mathbb{Z}$, $M_i \in \mathcal{C}$.

d) Si M, N, $M \oplus N \in \mathcal{C}$, entonces $[M \oplus N] = [M] + [N]$.

Observemos que si $\mathcal{C}$ es estable para sumas directas (es decir, si la suma directa de dos módulos de $\mathcal{C}$ está también en $\mathcal{C}$) entonces, en la combinación lineal de c), todos los sumandos con coeficiente positivo pueden agruparse en una única suma directa, e igualmente con los de coeficiente negativo, por lo que todo elemento de $R(\mathcal{C})$ es de la forma $[M] - [N]$, con M, $N \in \mathcal{C}$.

El principal ejemplo concreto de grupos de Grothendieck que nos va a interesar es el siguiente:

Definición 3.43 Sea G un grupo finito y k un cuerpo. Llamaremos $R_k(G)$ al grupo de Grothendieck asociado a la categoría de los $k[G]$-módulos finitamente generados. Definimos

$$R_k^+(G) = \{[M] \in R_k(G) \mid M \text{ es un } k[G]\text{-módulo finitamente generado}\},$$

$$S_k(G) = \{[M] \in R_k(G) \mid M \text{ es un } k[G]\text{-módulo simple}\}.$$

Teorema 3.44 *Sea G un grupo finito y k un cuerpo. Entonces:*

a) Si M y N son dos $k[G]$-módulos simples, entonces $[M] = [N]$ en $R_k(G)$ si y sólo si $M \cong N$.

b) $R_k(G)$ es un $\mathbb{Z}$-módulo libre de base $S_k(G)$.

DEMOSTRACIÓN: Observemos en primer lugar que $S_k(G)$ genera $R_k(G)$. Para ello basta observar que si M es un $k[G]$-módulo finitamente generado no nulo y

$$0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$$

es una serie de composición, la sucesión exacta

$$0 \longrightarrow M_{n-1} \longrightarrow M \longrightarrow M/M_{n-1} \longrightarrow 0$$

nos da la relación

$$[M] = [M/M_{n-1}] + [M_{n-1}],$$

donde $[M/M_{n-1}] \in S_k(G)$. Razonamos igualmente con M_{n-1} y, tras un numero finito de pasos, llegamos a que

$$[M] = [M_n/M_{n-1}] + [M_{n-1}/M_{n-2}] + \cdots + [M_1] \in \langle S_k(G) \rangle .$$

Sea $V_1, \ldots, V_h$ un sistema de representantes de los $k[G]$-módulos simples y sea R el $\mathbb{Z}$-módulo libre de base $\{V_1, \ldots, V_h\}$. La aplicación $V_i \mapsto [V_i]$ se extiende a un epimorfismo de grupos $f : R \longrightarrow R_k(G)$. Vamos a probar que es un isomorfismo construyendo su inverso. Esto prueba al mismo tiempo a) y b).

Para cada $k[G]$-módulo finitamente generado M, sea $m_i(M)$ la multiplicidad de V_i como factor de composición de M (es decir, el número de factores de composición de V isomorfos a V_i). Si tenemos una sucesión exacta de $k[G]$-módulos

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0,$$

es claro que una serie de composición de M se obtiene "enlazando" una serie de composición de M' con una serie de composición de $M/M' \cong M''$, por lo que $m_i(M) = m_i(M') + m_i(M'')$. Así pues, la función m_i es aditiva y, por consiguiente, induce un homomorfismo de grupos $m_i : R_k(G) \longrightarrow \mathbb{Z}$ que cumple $m_i([M]) = m_i(M)$. El homomorfismo $g : R_k(G) \longrightarrow R$ dado por

$$g(x) = \sum_{i=1}^{h} m_i(x) V_i$$

cumple que $g([V_i]) = V_i$, luego es el inverso de f. ∎

De este modo, los elementos de $S_k(G) = \{[V_1], \ldots, [V_h]\}$ se corresponden biunívocamente con las clases de isomorfía de $k[G]$-módulos simples y, para todo $k[G]$-módulo no nulo finitamente generado M, el elemento $[M] \in R_k(G)$ se expresa de forma única como

$$[M] = \sum_{i=1}^{h} m_i(M)[V_i],$$

donde $m_i(M)$ es el número de veces que V_i aparece como factor de composición de M.

Así, para dos $k[G]$-módulos M y N, se cumple que $[M] = [N]$ si y sólo si M y N tienen los mismos factores de composición (con las mismas multiplicidades). En particular, si $\operatorname{car} k \nmid |G|$ (con lo que $k[G]$ es semisimple), podemos concluir que $[M] = [N]$ si y sólo si $M \cong N$, ya que cada $k[G]$-módulo finitamente generado y no nulo es la suma directa de sus factores de composición.

Veamos ahora un resultado general para definir formas bilineales sobre grupos de Grothendieck:

Teorema 3.45 *Sea A un anillo y sean $\mathcal{C}$ y $\mathcal{C}'$ dos subcategorías de la categoría de los A-módulos finitamente generados, sea R un grupo abeliano y sea*

$$F : \mathcal{C} \times \mathcal{C}' \longrightarrow R$$

una aplicación tal que, para cada par de sucesiones exactas

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0, \qquad 0 \longrightarrow N' \longrightarrow N \longrightarrow N'' \longrightarrow 0$$

en $\mathcal{C}$ y $\mathcal{C}'$ respectivamente, se cumpla que

$$F(M,N) = F(M',N) + F(M'',N), \qquad F(M,N) = F(M,N') + F(M,N'').$$

Entonces existe una única forma bilineal $b : R(\mathcal{C}) \times R(\mathcal{C}') \longrightarrow R$ tal que

$$b([M],[N]) = F(M,N).$$

Demostración: Fijemos un objeto $N \in \mathcal{C}'$ y consideremos la aplicación $f_N : \mathcal{C} \longrightarrow R$ dada por $f_N(M) = F(M,N)$. Claramente es aditiva, luego induce un homomorfismo de grupos $i_N : R(\mathcal{C}) \longrightarrow R$ que cumple $i_N([M]) = F(M,N)$.

Tomemos ahora $x \in R(\mathcal{C})$ y consideremos la aplicación $g_x : \mathcal{C}' \longrightarrow R$ dada por $g_x(N) = i_N(x)$. Vamos a probar que es aditiva. Consideramos una sucesión exacta

$$0 \longrightarrow N' \longrightarrow N \longrightarrow N'' \longrightarrow 0$$

y observamos que, para cada $M \in \mathcal{C}$, se cumple que

$$i_N([M]) = F(M,N) = F(M,N') + F(M,N'') = i_{N'}([M]) + i_{N''}([M]).$$

Como i_N, $i_{N'}$ e $i_{N''}$ son homomorfismos de grupos y los elementos $[M]$ generan $R(\mathcal{C})$, esto implica que $i_N(x) = i_{N'}(x) + i_{N''}(x)$ para todo $x \in R(\mathcal{C})$, luego $g_x(N) = g_x(N') + g_x(N'')$. Así pues, g_x es aditiva y define un homomorfismo de grupos $j_x : R(\mathcal{C}') \longrightarrow R$ que cumple $j_x([N]) = i_N(x)$.

Finalmente, definimos $b(x,y) = j_x(y)$. Claramente, si

$$x = \sum_i m_i[M_i], \qquad y = \sum_j n_j[N_j],$$

entonces

$$b(x,y) = \sum_j n_j j_x([N_j]) = \sum_j n_j i_{N_j}(x) = \sum_{i,j} m_i n_j i_{N_j}([M_i]) = \sum_{i,j} m_i n_j F(M_i, N_j).$$

De aquí se sigue inmediatamente que b es bilineal y que cumple lo pedido. La unicidad es inmediata. ∎

De momento veremos dos aplicaciones de este teorema. En primer lugar consideramos la aplicación que a cada par de $k[G]$-módulos M y N les asigna $F(M,N) = [M \otimes_k N] \in R_k(G)$. Claramente es aditiva en M y N, por lo que induce una forma bilineal en $R_k(G)$:

Teorema 3.46 *Si G es un grupo finito y k es un cuerpo, el grupo $R_k(G)$ adquiere estructura de anillo conmutativo con el producto determinado por*

$$[M] \cdot [N] = [M \otimes_k N],$$

para todo par de $k[G]$-módulos finitamente generados M y N.

Demostración: El producto está bien definido por el teorema anterior, y es bilineal, es decir, que cumple la propiedad distributiva. Las propiedades del producto tensorial implican trivialmente las propiedades de la definición de anillo. Observemos que el elemento neutro es $1 = [k]$, considerando a k como $k[G]$-módulo trivial (el $k[G]$-módulo asociado a la representación trivial de G sobre k). ∎

La segunda forma bilineal que podemos definir en $R_k(G)$ (esta vez bajo la hipótesis de que $\operatorname{car} k \nmid |G|$) está asociada a

$$\langle M, N\rangle = \dim_k \operatorname{Hom}_G(M,N) \in \mathbb{Z}.$$

(Obviamente, la dimensión es un número natural, pero vamos a aplicar el teorema 3.45 con $R = \mathbb{Z}$).

Observemos que $\langle M, N\rangle$ es aditiva en las dos componentes, pues si tenemos una sucesión exacta de $k[G]$-módulos finitamente generados

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0,$$

el hecho de que $k[G]$ sea semisimple se traduce en que $M \cong M' \oplus M''$, por lo que todo homomorfismo de $k[G]$-módulos $M \longrightarrow N$ está determinado por sus restricciones a M' y M'', es decir,

$$\operatorname{Hom}_G(M,N) \cong \operatorname{Hom}_G(M',N) \oplus \operatorname{Hom}_G(M'',N),$$

luego $\langle M, N\rangle = \langle M', N\rangle + \langle M'', N\rangle$. Similarmente se razona con la segunda componente. Por lo tanto:

Teorema 3.47 *Sea G un grupo finito y k un cuerpo tal que $\operatorname{car} k \nmid |G|$. Entonces existe una forma bilineal $\langle\ ,\ \rangle : R_k(G) \times R_k(G) \longrightarrow \mathbb{Z}$ determinada por*

que, para todo par de $k[G]$-módulos finitamente generados M y N, se cumple que

$$\langle [M], [N] \rangle = \dim_k \mathrm{Hom}_G(M, N).$$

Respecto a ella, la base $S_k(G)$ es ortogonal (y es ortonormal si k es un cuerpo de escisión para G).

DEMOSTRACIÓN: La ortogonalidad de la base significa que $\langle [M], [N] \rangle = 0$ si $[M] \neq [N]$, lo cual es consecuencia del lema de Schur 3.12. La ortonormalidad significa que, además, $\langle [M], [M] \rangle = 1$, lo cual se cumple si k es un cuerpo de escisión, por el teorema 3.34. ∎

3.5 Caracteres

En esta sección deduciremos las propiedades básicas de los caracteres de las representaciones de grupos finitos a partir de los resultados precedentes.

Definición 3.48 Si G es un grupo finito y k es un cuerpo, definimos k^G como el k-espacio vectorial de todas las funciones $G \longrightarrow k$. Llamaremos $F_k(G)$ al subespacio de k^G generado por los caracteres de las representaciones de G en k. Notemos que todos los elementos de $F_k(G)$ son *funciones de clases,* es decir, que son constantes en cada clase de conjugación de G.

Teniendo en cuenta que el producto de caracteres es de nuevo un carácter (teorema 1.16), es claro que $F_k(G)$ tiene estructura de k-álgebra con el producto definido puntualmente. Llamaremos $R'_k(G)$ al subgrupo de $F_k(G)$ generado por los caracteres de G sobre k, que claramente es un subanillo de $F_k(G)$, a cuyos elementos llamaremos *caracteres virtuales* de G sobre k.

La notación $R'_k(G)$ se debe que vamos a demostrar que este anillo es isomorfo al anillo de Grothendieck $R_k(G)$. Para probarlo necesitaremos un resultado previo sobre extensión de coeficientes. Observemos que si

$$0 \longrightarrow V' \longrightarrow V \longrightarrow V'' \longrightarrow 0$$

es una sucesión exacta de $k[G]$-módulos, entonces

$$0 \longrightarrow V'_K \longrightarrow V_K \longrightarrow V''_K \longrightarrow 0$$

es también una sucesión exacta (porque K es libre sobre k), luego podemos definir un homomorfismo de grupos $R_k(G) \longrightarrow R_K(G)$ mediante $[V] \mapsto [V_K]$.

Teorema 3.49 *Sea G un grupo finito y $k \subset K$ una extensión de cuerpos. El homomorfismo natural $R_k(G) \longrightarrow R_K(G)$ es inyectivo, y es un isomorfismo si k es un cuerpo de escisión de G.*

DEMOSTRACIÓN: La imagen de cada elemento $[V] \in S_k(G)$ se expresa como combinación lineal de un subconjunto $I_{[V]} \subset S_K(G)$, y el teorema 3.38 implica que los conjuntos $I_{[V]}$ son disjuntos dos a dos. Esto prueba que la imagen de $S_k(G)$ es linealmente independiente en $R_K(G)$, y esto implica a su vez la inyectividad. Si k es un cuerpo de escisión de G, el teorema 3.39 implica que la imagen de $S_k(G)$ es $S_K(G)$, luego el homomorfismo es un isomorfismo. ∎

Teorema 3.50 *Si G es un grupo finito y k es un cuerpo, existe un isomorfismo de anillos $R_k(G) \longrightarrow R'_k(G)$ dado por $[V] \mapsto \chi_V$, donde χ_V es el carácter asociado al $k[G]$-módulo V. En particular, el grupo $R'_k(G)$ es un $\mathbb{Z}$-módulo libre que tiene por base a los caracteres irreducibles de G sobre k.*

DEMOSTRACIÓN: Consideremos una sucesión exacta de $k[G]$-módulos finitamente generados

$$0 \longrightarrow V' \longrightarrow V \longrightarrow V'' \longrightarrow 0.$$

Fijemos una base $v_1, \ldots, v_r$ de V' como k-espacio vectorial y completémosla hasta una base $v_1, \ldots, v_n$ de V. Entonces, las imágenes de $v_{r+1}, \ldots, v_n$ son una base de V''. Consideremos las representaciones matriciales ρ', ρ, ρ'' asociadas a los tres módulos en dichas bases. Es claro que, para todo $\sigma \in G$, se cumple que

$$\rho(\sigma) = \left(\begin{array}{c|c} \rho'(\sigma) & 0 \\ \hline * & \rho''(\sigma) \end{array}\right),$$

luego los caracteres correspondientes cumplen la relación $\chi_V = \chi_{V'} + \chi_{V''}$. Esto implica que existe un homomorfismo de grupos en las condiciones del enunciado. Como el producto en $R_k(G)$ está inducido por el producto tensorial, es claro que se trata de un homomorfismo de anillos, obviamente suprayectivo.

En particular, hemos probado que el carácter de un módulo es la suma de los caracteres de sus factores de composición, luego todo carácter es suma de caracteres irreducibles, y éstos generan $R'_k(G)$.

Vamos a probar que el homomorfismo del enunciado es un isomorfismo suponiendo en primer lugar que k es un cuerpo de escisión de G. Para ello bastará probar que si $S_k(G) = \{[V_1], \ldots, [V_h]\}$, los caracteres χ_{V_i} son linealmente independientes sobre $\mathbb{Z}$ (en particular, distintos dos a dos). Probaremos, de hecho, que son linealmente independientes sobre k (es decir, como elementos del espacio $F_k(G)$).

Si ρ_i es la representación lineal asociada a V_i, podemos extenderla por linealidad hasta un homomorfismo de k-álgebras $\rho_i : k[G] \longrightarrow \mathrm{End}_k(V_i)$. Como k es un cuerpo de escisión, los $k[G]$-módulos V_i son absolutamente simples, y el teorema 3.36 nos da que cada ρ_i es suprayectiva.

Igualmente podemos extender linealmente los caracteres hasta funciones $\chi_{V_i} : k[G] \longrightarrow k$, de modo que $\chi_{V_i}(x)$ sigue siendo la traza de $\rho_i(x)$, para todo $x \in k[G]$.

La suprayectividad de ρ_i hace que podamos tomar un elemento $x_i \in k[G]$ tal que $\chi_{V_i}(x_i) = 1$. El teorema 3.37 nos da otro elemento $y_i \in k[G]$ tal que $\chi_{V_i}(y_i) = \chi_{V_i}(x_i) = 1$ y $\chi_{V_j}(y_i) = 0$, para todo $j \neq i$. De aquí se sigue inmediatamente que los caracteres son linealmente independientes sobre k considerados

como funciones definidas sobre $k[G]$, pero, como las extensiones a $k[G]$ están determinadas por linealidad por sus restricciones a G, es evidente que también son linealmente independientes considerados como funciones sobre G, es decir, como elementos de $F_k(G)$.

Supongamos ahora que k es un cuerpo arbitrario y sea K un cuerpo de escisión de G que contenga a k. Por la parte ya probada, tenemos un isomorfismo $R'_K(G) \cong F_K(G)$ que biyecta la base $S_K(G)$ con el conjunto I de los caracteres irreducibles de G sobre K. Si V es un $k[G]$-módulo simple, su carácter es el mismo que el de V_K y, como $[V_K]$ es combinación lineal (no nula) de los elementos de un subconjunto $I_{[V]} \subset S_K(G)$ (véase la prueba de 3.49), resulta que χ_V es combinación lineal (no nula) de los caracteres de la imagen $I'_{[V]} \subset I$ de $I_{[V]}$. Como los conjuntos $I_{[V]}$ son disjuntos dos a dos, lo mismo sucede con los conjuntos $I'_{[V]}$ y, como I es una K-base de $F_K(G)$, es claro que los caracteres irreducibles de G sobre k son linealmente independientes sobre K, luego también son linealmente independientes sobre k y forman, por consiguiente, una k-base de $F_k(G)$ y una $\mathbb{Z}$-base de $R'_k(G)$. Esto prueba que el homomorfismo del enunciado es un isomorfismo. ∎

Conviene destacar que hemos probado que los caracteres irreducibles de G sobre k son una k-base de $F_k(G)$. El teorema anterior implica que dos $k[G]$-módulos finitamente generados tienen el mismo carácter si y sólo si tienen los mismos factores de composición (con las mismas multiplicidades).

Ahora probaremos que los valores que toman los caracteres son sumas de raíces de la unidad. Para ello necesitamos unos resultados previos que nos reduzcan el problema al caso semisimple:

Teorema 3.51 *Sea k un cuerpo de característica prima p y sea $G = P \times H$ un grupo finito, donde P tiene orden potencia de p y H tiene orden primo con p. Entonces, un $k[G]$-módulo finitamente generado V es semisimple si y sólo si P actúa trivialmente sobre V.*

Demostración: Si P actúa trivialmente sobre V, podemos considerar a V como $k[H]$-módulo finitamente generado y, como $k[H]$ es semisimple, vemos que V es un $k[H]$-módulo semisimple, y esto implica que también es semisimple como $k[G]$-módulo.

Para probar el recíproco no perdemos generalidad si suponemos que V es simple. El teorema 1.14 nos da que el $k[P]$-submódulo

$$V_P = \{v \in V \mid v\pi = v \text{ para todo } \pi \in P\}$$

no es nulo. Ahora bien, el hecho de que $P \trianglelefteq G$ implica que V_P es un $k[G]$-submódulo de V, pues si $v \in V_P$, $\sigma \in G$ y $\pi \in P$, tenemos que $\sigma\pi\sigma^{-1} \in P$, luego

$$(v\sigma)\pi = v(\sigma\pi\sigma^{-1})\sigma = v\sigma,$$

luego $v\sigma \in V_P$. Como V es un $k[G]$-módulo simple, esto implica que $V_P = V$, es decir, que P actúa trivialmente sobre V. ∎

Teorema 3.52 *Sea G un grupo finito, sea k un cuerpo de característica p y sea $\sigma = \pi\sigma' \in G$, donde π tiene orden potencia de p y σ' tienen orden primo con p. Entonces, para todo carácter χ de G sobre k, se cumple que $\chi(\sigma) = \chi(\sigma')$.*

DEMOSTRACIÓN: No perdemos generalidad si suponemos que $G = \langle\sigma\rangle$ (notemos que π y σ' son potencias de σ). De este modo, $G = P \times H$, donde $P = \langle\pi\rangle$ y $H = \langle\sigma'\rangle$. Sea V un $k[G]$-módulo irreducible que determine el carácter χ, sea

$$0 = V_0 \subset V_1 \subset \cdots \subset V_n = V$$

una serie de composición de V y formemos una base de V extendiendo una base de V_0 a una base de V_1 y así sucesivamente hasta llegar a V. Consideremos la representación matricial de G asociada a esta base. Para cada $\tau \in G$, la matriz $\rho(\tau)$ tiene la forma

$$\rho(\tau) = \left(\begin{array}{c|c|c} \rho_1(\tau) & 0 & 0 \\ \hline * & \ddots & 0 \\ \hline * & * & \rho_n(\tau) \end{array}\right)$$

donde ρ_i es la representación asociada al factor de composición V_i/V_{i-1}. Como los factores de composición son simples, el teorema 3.51 implica que $\rho_i(\pi)$ es la matriz identidad. Por consiguiente $\rho(\sigma)$ tiene los mismos bloques diagonales que $\rho(\sigma')$, luego $\chi(\sigma) = \chi(\sigma')$. ∎

Teorema 3.53 *Sea k un cuerpo, sea G un grupo finito, sea m el mínimo común múltiplo de los órdenes de los elementos de G no divisibles entre la característica de k (si es que es no nula). Entonces, los valores que toman los caracteres de G sobre k son sumas de raíces m-simas de la unidad (en una clausura algebraica de k).*

DEMOSTRACIÓN: Sea V un $k[G]$-módulo finitamente generado y sea χ su carácter y sea $\sigma \in G$. Hemos de probar que $\chi(\sigma)$ es suma de raíces m-simas de la unidad. Si k tiene característica prima p, el teorema anterior nos permite suponer que el orden de σ no es divisible entre p. Sea $H = \langle\sigma\rangle$. El carácter de V como $k[H]$-módulo es la restricción $\chi|_H$, luego no perdemos generalidad si suponemos que $G = \langle\sigma\rangle$, de modo que G es abeliano y $k[G]$ es semisimple (y ahora $m = |G|$). También podemos sustituir k por una clausura algebraica $\bar{k}$ (y V por $V \otimes_k \bar{k}$) sin modificar el carácter, luego podemos suponer que k es algebraicamente cerrado.

Es claro que las representaciones irreducibles de G son lineales, luego coinciden con los caracteres irreducibles de G y son, concretamente, las que asignan a σ cada una de las m raíces de la unidad en k. Como χ es suma de caracteres irreducibles, $\chi(\sigma)$ es suma de raíces m-simas de la unidad. ∎

A partir de aquí nos restringimos al caso en que $\operatorname{car} k \nmid |G|$.

Definición 3.54 Sea G un grupo finito y k un cuerpo tal que $\operatorname{car} k \nmid |G|$. Definimos en $F_k(G)$ la forma bilineal dada por

$$\langle f, g\rangle = \frac{1}{|G|}\sum_{\sigma\in G} f(\sigma)g(\sigma^{-1}).$$

Recordemos que el carácter regular de G es el asociado al $k[G]$-módulo $k[G]$ y, según el ejemplo de la página 10, viene dado por

$$r_G(\sigma) = \begin{cases} |G| & \text{si } \sigma = 1, \\ 0 & \text{si } \sigma \neq 1. \end{cases}$$

Vamos a calcular su expresión como combinación lineal de los caracteres irreducibles. Sea $k[G] = A_1 \oplus \cdots \oplus A_h$ la descomposición de $k[G]$ dada por el teorema de Wedderburn 3.16, de modo que $A_i \cong \mathrm{Mat}_{n_i}(D_i^{\mathrm{op}})$, $D_i = \mathrm{End}(V_i)$. Sea χ_i el carácter de V_i. En la demostración del teorema 3.17 se ve que el número de veces que V_i aparece como sumando directo de A_i es $n_i = \dim_{D_i} V_i$. Como

$$\chi_i(1) = \dim_k V_i = (\dim_k D_i)(\dim_{D_i} V_i),$$

concluimos que la multiplicidad de V_i en $k[G]$ (o, equivalentemente, la multiplicidad de χ_i en el carácter regular r_G asociado a $k[G]$) es $\chi_i(1)/m_i$, donde $m_i = \dim_k D_i$. Explícitamente:

$$r_G = \sum_i \frac{\chi_i(1)}{m_i}\chi_i.$$

Teorema 3.55 *Sea G un grupo finito y k un cuerpo tal que $\mathrm{car}\, k \nmid |G|$. Sea $k[G] = A_1 \oplus \cdots \oplus A_h$ la descomposición de $k[G]$ dada por el teorema de Wedderburn* 3.16, *de modo que $A_i \cong \mathrm{Mat}_{n_i}(D_i^{\mathrm{op}})$, $D_i = \mathrm{End}(V_i)$, y sea $1 = e_1 + \cdots + e_h$ la descomposición correspondiente de la unidad de $k[G]$. Sea χ_i el carácter de V_i y sea $m_i = \dim_k D_i$. Entonces*

$$e_i = \frac{\chi_i(1)}{|G|m_i} \sum_{\sigma\in G} \chi_i(\sigma^{-1})\sigma.$$

Demostración: En principio,

$$e_i = \sum_{\sigma\in G} a_\sigma \sigma,$$

para ciertos $a_\sigma \in k$, que hemos de determinar. Para ello observamos que

$$r_G(e_i\sigma^{-1}) = \sum_{\tau\in G} a_\sigma r_G(\tau\sigma^{-1}) = |G|a_\sigma.$$

Por otra parte, usando la expresión de r_G que hemos obtenido justo antes de este teorema,

$$|G|a_\sigma = \sum_j \frac{\chi_j(1)}{m_j}\chi_j(e_i\sigma^{-1}).$$

Si llamamos $\rho_j : k[G] \longrightarrow k$ a la representación que origina a χ_j, tenemos que

$$\rho_j(e_i\sigma^{-1}) = \rho_j(e_i)\rho_j(\sigma^{-1}) = \begin{cases} 0 & \text{si } i \neq j, \\ \rho_j(\sigma^{-1}) & \text{si } i = j. \end{cases}$$

Por lo tanto, $\chi_j(e_i\sigma^{-1}) = \chi_j(\sigma^{-1})\delta_{ij}$, donde (δ_{ij}) es la matriz identidad. En definitiva, llegamos a que $|G|a_\sigma = \chi_i(1)\chi_i(\sigma^{-1})/m_i$, que es lo que afirma el enunciado. ∎

Notemos que $\chi_i(1)/m_i \in \mathbb{Z}$, luego el cociente tiene sentido como elemento de k. Más aún, es no nulo en k, pues de lo contrario sería $e_j = 0$. De aquí deducimos las relaciones de ortogonalidad:

Teorema 3.56 (Relaciones de ortogonalidad) *Sea G un grupo finito y k un cuerpo tal que* $\operatorname{car} k \nmid |G|$. *Sean χ, ψ dos caracteres irreducibles de G sobre k. Entonces*

$$\langle \chi, \psi \rangle = \begin{cases} m & \text{si } \chi = \psi, \\ 0 & \text{si } \chi \neq \psi, \end{cases}$$

donde $m = \dim_k \operatorname{End}_k(V)$, para cualquier $k[G]$-módulo irreducible V de carácter χ.

Demostración: Continuando con la notación del teorema anterior, consideramos dos caracteres irreducibles χ_i y χ_j. Puesto que $e_ie_j = e_i\delta_{ij}$, sustituyendo en esta igualdad las expresiones que hemos obtenido para los e_i resulta

$$\frac{\chi_j(1)}{m_j}\frac{1}{|G|}\sum_{\sigma,\tau\in G}\chi_i(\sigma^{-1})\chi_j(\tau^{-1})\sigma\tau = \delta_{ij}\sum_{\sigma\in G}\chi_i(\sigma^{-1})\sigma$$

Igualamos el coeficiente de 1 en ambos miembros:

$$\frac{\chi_j(1)}{m_j}\frac{1}{|G|}\sum_{\tau\in G}\chi_i(\tau)\chi_j(\tau^{-1}) = \delta_{ij}\chi_i(1),$$

lo que equivale a

$$\frac{\chi_j(1)}{m_j}\langle \chi_i, \chi_j \rangle = \delta_{ij}\chi_i(1).$$

Si $i \neq j$, teniendo en cuenta que $\chi_j(1)/m_j \neq 0$ en k, concluimos que $\langle \chi_i, \chi_j \rangle = 0$. Si $i = j$, la expresión se reduce a

$$\frac{\chi_i(1)}{m_i}\langle \chi_i, \chi_i \rangle = \chi_i(1) = \frac{\chi_i(1)}{m_i}m_i$$

luego, dividiendo entre $\chi_i(1)/m_i$, llegamos a que $\langle \chi_i, \chi_i \rangle = m_i$. ∎

El teorema siguiente termina de probar la equivalencia entre los anillos $R_k(G)$ y $R'_k(G)$:

Teorema 3.57 *Sea G un grupo finito y k un cuerpo tal que* $\operatorname{car} k \nmid |G|$. *A través del isomorfismo $R_k(G) \cong R'_k(G)$ dado por el teorema* 3.50 *hace corresponder la forma bilineal definida en el teorema* 3.47 *con la definida en* 3.54.

Demostración: Antes de probar el teorema, debemos señalar que la correspondencia entre las formas bilineales requiere una matización. En efecto, la forma bilineal en $R_k(G)$ es una aplicación

$$\langle\ ,\ \rangle : R_k(G) \times R_k(G) \longrightarrow \mathbb{Z},$$

mientras que la forma bilineal en $R'_k(G)$ es una aplicación

$$\langle\ ,\ \rangle : R'_k(G) \times R'_k(G) \longrightarrow k.$$

La correspondencia consiste en que la segunda es igual a la primera compuesta con el homomorfismo natural $\mathbb{Z} \longrightarrow k$.

El isomorfismo dado por el teorema 3.50 hace corresponder la base $S_k(G)$ de $R_k(G)$ con la base de $R'_k(G)$ formada por los caracteres irreducibles de G sobre k, y ambas son ortogonales para las formas bilineales respectivas, luego la matriz de ambas en las bases respectivas es diagonal. Como

$$\langle [V], [V] \rangle = \dim_k \operatorname{End}(V) = \langle \chi_V, \chi_V \rangle,$$

(entendiendo que el miembro derecho es la imagen en k del miembro izquierdo), concluimos que ambas matrices se corresponden (a través del homomorfismo $\mathbb{Z} \longrightarrow k$), luego las dos formas bilineales se corresponden a través del isomorfismo. ∎

3.6 Extensiones de coeficientes

En esta sección vamos a estudiar con más detenimiento el monomorfismo del teorema 3.49 o, equivalentemente, la inclusión $R'_k(G) \subset R'_K(G)$. En principio, sabemos que cada carácter irreducible de G sobre k se expresa como combinación lineal (con coeficientes naturales) de ciertos caracteres irreducibles de G sobre K. Vamos a ver qué podemos decir de estos caracteres y de los coeficientes de la combinación. La situación para cuerpos de característica prima es bastante más simple que en el caso de cuerpos de característica cero, y ello es consecuencia del teorema siguiente:

Teorema 3.58 *Sea G un grupo finito, K/k una extensión de cuerpos de característica prima y $\rho : G \longrightarrow \operatorname{Aut}(V)$ una representación lineal absolutamente irreducible de G sobre K cuyo carácter asociado tome valores en k. Entonces $V = W_K$, para cierto $k[G]$-módulo absolutamente simple W.*

Demostración: Consideramos en primer lugar el caso en que K es finito. Razonando por inducción sobre el cardinal de K, no perdemos generalidad si suponemos que no hay cuerpos intermedios entre k y K.

Fijemos una representación matricial $\rho : K[G] \longrightarrow \operatorname{Mat}_m(K)$. Por el teorema 3.36 sabemos que ρ es suprayectiva. Llamemos $A \subset \operatorname{Mat}_m(K)$ al k-espacio vectorial generado por $\rho[G]$, que claramente es una k-subálgebra del anillo de matrices. Consideremos su centro $Z(A)$.

Una matriz $a \in Z(A)$ conmuta con todas las matrices de $\rho[G]$, luego también conmuta con todas las matrices de $\rho[K[G]]$, luego $a \in Z(\operatorname{Mat}_m(K)) = K$ (donde identificamos a K con el espacio de matrices escalares). Así pues, tenemos que $k \subset Z(A) \subset K$. Es claro que $Z(A)$ es un cuerpo (por ejemplo, porque es la adjunción a k de elementos algebraicos), luego, por la hipótesis de que

la extensión K/k no tiene cuerpos intermedios, ha de ser $Z(A) = k$ o bien $Z(A) = K$. Vamos a descartar esta segunda posibilidad.

Si $Z(A) = K$, entonces A contendría al K-espacio vectorial generado por $\rho[G]$, es decir, sería $A = \rho[K[G]] = \mathrm{Mat}_m(K)$. En particular, si $\alpha \in K \setminus k$, podríamos tomar una matriz en A de traza igual a α, pero, por otra parte, como las trazas de las matrices de $\rho[G]$ están todas en k, lo mismo sucede con las trazas de las matrices de A, y tenemos una contradicción.

Así pues, tenemos que $Z(A) = k$. Ahora demostraremos que A es semisimple, para lo cual basta probar que $J(A) = 0$ y a su vez, basta probar que A no tiene ideales nilpotentes no nulos. Si I es un ideal nilpotente de A, entonces KI es un ideal nilpotente de $KA = \rho[K[G]] = \mathrm{Mat}_m(K)$, luego $KI = 0$, porque los anillos de matrices son semisimples (teorema 3.17). Así pues, $I = 0$ y A es semisimple.

Podemos considerar entonces la descomposición de A dada por el teorema de Wedderburn 3.16, donde cada $A_i \cong \mathrm{Mat}_{n_i}(D_i^{\mathrm{op}})$ ha de contener en su centro un k-subespacio vectorial isomorfo a k (pues $D_i = \mathrm{End}_A(V_i)$ contiene a k en su centro, identificado con el espacio de las homotecias en V_i). Puesto que $\dim_k Z(A) = 1$, la descomposición de A sólo puede tener un sumando, es decir, que $A \cong \mathrm{Mat}_n(D^{\mathrm{op}})$, donde $D = \mathrm{End}_A(W)$, para cierto A-módulo simple W finitamente generado. Como W tiene dimensión finita sobre k, es un conjunto finito, luego D también es finito, y todo anillo de división finito es un cuerpo.[7] Por consiguiente, $D = Z(\mathrm{Mat}_n(D)) = Z(A) = k$. Como $\mathrm{End}_A(W) = D = k$, el teorema 3.34 nos da que W es un A-módulo absolutamente simple.

El epimorfismo natural $k[G] \longrightarrow A$ convierte a W en un $k[G]$-módulo simple, que, de hecho, es absolutamente simple, pues $\mathrm{End}_{k[G]}(W) = \mathrm{End}_A(W) = k$. Nos falta probar que $V \cong W_K$.

Por la observación tras el teorema 3.39, existe un $k[G]$-módulo simple M tal que V es un factor de composición de M_K. Basta probar que $M \cong W$, pues entonces V será un factor de composición de W_K, que es simple, luego será $V \cong W_K$.

Si no se diera el isomorfismo $M \cong W$, el teorema 3.37 nos da un $y \in k[G]$ que anula a M pero no anula a W. Como V es un factor de composición de M_K, es claro que y también anula a V, pero esto significa que la imagen de y por el epimorfismo $k[G] \longrightarrow A$ (inducido por la representación matricial de V) es nula, luego y también anula a W, ya que el producto de y por los elementos de W se define a través de su imagen en A. Esta contradicción prueba que $V \cong W_K$ y el teorema está demostrado en el caso en que el cuerpo K es finito.

Para el caso general, observamos que no perdemos generalidad si sustituimos el cuerpo K por una extensión. (Hemos de probar que una representación matricial sobre K con trazas en k es isomorfa a una representación matricial sobre k.) Así pues, podemos suponer que K es algebraicamente cerrado. Sea F el cuerpo primo de K, sea $\overline{F} \subset K$ la clausura algebraica de F. Sabemos que es un cuerpo de escisión de G. El teorema 3.40 nos asegura la existencia de un subcuerpo finito L de K que es también un cuerpo de escisión para G. (Basta tomar un sistema de representantes de las representaciones matriciales

[7] Esto es el teorema de Wedderburn. Está probado en mi libro de *Geometría,* teorema 7.28.

irreducibles de G sobre $\overline{F}$ y adjuntar a F los coeficientes de todas las matrices imágenes de los elementos de G, que son un número finito. De este modo, todo $\overline{F}[G]$-módulo simple está inducido por un $L[G]$-módulo simple.)

Como L es un cuerpo de escisión de G, tenemos que $V = M_K$, para cierto $L[G]$-módulo simple M. Como M y V tienen el mismo carácter, tenemos que éste toma valores en $L \cap k$. Por la parte ya probada, $M = N_L$, para cierto $(L \cap k)[G]$-módulo simple N. Entonces $V = M_K = N_K = (N_k)_K$. El $k[G]$-módulo $W = N_k$ cumple lo pedido. (El hecho de que V sea absolutamente simple y $V = W_K$ implica que W también es absolutamente simple.) ∎

Para extraer la principal consecuencia del teorema anterior conviene dar la definición siguiente:

Definición 3.59 Sea G un grupo finito y m su exponente, es decir, el mínimo común múltiplo de los órdenes de los elementos de G. Diremos que un cuerpo es *suficientemente grande* para G si contiene todas las raíces m-simas de la unidad.

Teorema 3.60 *Si K es un cuerpo suficientemente grande para un grupo finito G, entonces es un cuerpo de escisión para G.*

Demostración: Si K tiene característica 0 y $k \subset K$ es la adjunción a $\mathbb{Q}$ de las raíces m-simas de la unidad (donde m es el exponente de G), el teorema 2.62 nos da que k es un cuerpo de escisión de G, luego K también lo es.

Supongamos ahora que K tiene característica prima y sea $\overline{K}$ su clausura algebraica (que es un cuerpo de escisión de G). El teorema 3.53 nos da que los valores que toman los caracteres de G sobre $\overline{K}$ son sumas de raíces m-simas de la unidad, luego todos ellos toman valores en K. Por el teorema 3.58, todo $\overline{K}[G]$-módulo simple es de la forma $V_{\overline{K}}$, para cierto $K[G]$-módulo absolutamente simple V. El teorema 3.40 implica que K es un cuerpo de escisión de G. ∎

Notemos que la prueba del teorema anterior es completamente distinta para cuerpos de característica 0 y para cuerpos de característica prima, pues en el primer caso se basa en el teorema de Brauer sobre caracteres inducidos y en el segundo en el teorema 3.58.

Entre otras cosas, hemos de probar que los caracteres que aparecen en la descomposición de un carácter irreducible tras una extensión de coeficientes forman una clase de conjugación en el sentido que vamos a definir a continuación.

Definición 3.61 Sea G un grupo finito, K un cuerpo y $\rho : G \longrightarrow \mathrm{LG}(n, K)$ una representación matricial de G sobre K. Cada automorfismo $\tau : K \longrightarrow K$ induce un automorfismo de grupos $\bar{\tau} : \mathrm{LG}(n, K) \longrightarrow \mathrm{LG}(n, K)$. Llamaremos $\rho^\tau = \rho \circ \bar{\tau}$, que es claramente una representación matricial de G sobre K.

Es inmediato comprobar que si ρ_2 y ρ_2 son representaciones matriciales isomorfas, entonces ρ_1^τ y ρ_2^τ también son isomorfas, por lo que, si V es un $K[G]$-módulo finitamente generado, podemos llamar V^τ al $K[G]$-módulo asociado a cualquier representación matricial ρ^τ, donde ρ es cualquier representación matricial asociada a V.

Si $f : G \longrightarrow K$ es una función cualquiera, podemos definir $f^\tau : G \longrightarrow K$ como la función dada por $f^\tau(\sigma) = \tau(f(\sigma))$. En estos términos, si una representación matricial ρ tiene carácter χ, es claro que ρ^τ tiene carácter χ^τ.

Teorema 3.62 *Sea G un grupo finito, K un cuerpo de escisión de G y sea $\chi : G \longrightarrow k$ un carácter (irreducible) de G sobre K que tome valores en un subcuerpo $k \subset K$. Si $\tau : k \longrightarrow k$ es un automorfismo, entonces χ^τ es también un carácter (irreducible) de G sobre K.*

DEMOSTRACIÓN: Sea $\overline{K}$ la clausura algebraica de K y sea $\overline{k} \subset \overline{K}$ la clausura algebraica de k. El teorema 3.49 implica que los caracteres irreducibles de G sobre K son los mismos que los caracteres irreducibles de G sobre $\overline{K}$ y éstos, a su vez, son los mismos que los caracteres irreducibles de G sobre $\overline{k}$. Por otra parte, τ se extiende a un automorfismo de $\overline{k}$. Por consiguiente, viendo a χ como carácter de una representación irreducible ρ de G sobre $\overline{k}$, tenemos que χ^τ es el carácter de ρ^τ y, claramente, es también irreducible. Por lo tanto, χ^τ es también el carácter de una representación irreducible de G sobre K. Como todo carácter es suma de caracteres irreducibles, el conjugado de un carácter arbitrario es también un carácter. ∎

Definición 3.63 Sea K/k una extensión de cuerpos. Si $\chi : G \longrightarrow K$ es un carácter de G sobre K, llamaremos $k(\chi)$ a la adjunción a k de la imagen de χ. Por 3.60 tenemos que $k(\chi)$ está contenido en una extensión ciclotómica de K, luego la extensión $k(\chi)/k$ es finita de Galois con grupo de Galois $\mathcal{G}_\chi = G(k(\chi)/k)$ abeliano. Diremos que dos caracteres irreducibles ψ, χ de G sobre K son *conjugados* sobre k si $k(\psi) = k(\chi)$ y existe un $\tau \in \mathcal{G}_\chi$ tal que $\chi^\tau = \psi$.

Es claro que la conjugación sobre k es una relación de equivalencia en el conjunto de los caracteres irreducibles de G sobre K. Observemos que si χ es un carácter irreducible cualquiera y $\tau \in \mathcal{G}_\chi$, entonces χ^τ es también un carácter irreducible (por el teorema 3.62) y claramente $k(\chi) = k(\chi^\tau)$, luego χ^τ es un carácter conjugado con χ sobre k. Esto significa que el grupo $\mathcal{G}_\chi$ actúa sobre la clase de conjugación de χ (y determina en ella una única órbita). Además el estabilizador de χ es trivial, pues si $\chi^\tau = \chi$, entonces τ fija a $k(\chi)$, luego ha de ser $\tau = 1$. El teorema 1.18 implica entonces que el número de conjugados de χ sobre k es $|\mathcal{G}_\chi| = |k(\chi) : k|$.

Por otra parte, vamos a necesitar el siguiente resultado técnico:

Teorema 3.64 *Sea K/k una extensión de cuerpos finita de grado n, sea V un $K[G]$-módulo simple y sea V_k el mismo espacio V considerado como $k[G]$-módulo.*

a) V_k tiene un único factor de composición W (con cierta multiplicidad), que es, concretamente, el único $k[G]$-módulo simple tal que W_K tiene a V como factor de composición.

b) Si el carácter χ de V toma valores en k, entonces el carácter de V_k es $n\chi$.

DEMOSTRACIÓN: Llamemos W al único $k[G]$-módulo simple tal que W_K tiene a V como factor de composición. (Véase la observación tras 3.39.) El teorema 3.37 nos da un $x \in k[G]$ tal que la multiplicación por x en W es el automorfismo identidad, mientras que x anula a cualquier $k[G]$-módulo simple no isomorfo a W.

Es claro que la multiplicación por x en W_K es también la identidad, y lo mismo vale para la multiplicación por x en V, ya que es un factor de composición de W_K. Por consiguiente, la multiplicación por x en V_k también es la identidad, y lo mismo vale para todos los factores de composición de V_k, luego todos ellos han de ser isomorfos a W. Esto prueba a)

Fijemos una K-base $v_1, \dots, v_m$ de V, y sea $e_1, \dots, e_n$ una k-base de K. Es claro entonces que los elementos $e_i v_j$ forman una k-base de V_k. Dado $\sigma \in G$, sea $v_j\sigma = \sum_r \alpha_{jr} v_r$, con $\alpha_{jr} \in K$. Sea, a su vez,

$$e_i \alpha_{jr} = \sum_s \beta_{ijrs} e_s, \qquad \text{con } \beta_{ijrs} \in k.$$

De este modo,

$$e_i v_j \sigma = \sum_r e_i \alpha_{jr} v_r = \sum_s \beta_{ijrs} e_s v_r.$$

Entonces:

$$e_i \chi(\sigma) = e_i \sum_j \alpha_{jj} = \sum_{j,s} \beta_{ijjs} e_s.$$

Como $\chi(\sigma) \in k$, la unicidad de las coordenadas implica que

$$\chi(\sigma) = \sum_j \beta_{ijji},$$

luego, si llamamos ψ al carácter de V_k, tenemos que

$$\psi(\sigma) = \sum_{ij} \beta_{ijji} = n\chi(\sigma).$$

Así pues, $\psi = n\chi$. ∎

Ahora ya podemos estudiar la descomposición de un $k[G]$-módulo tras una extensión de coeficientes:

Teorema 3.65 *Sea G un grupo finito, sea K/k una extensión de cuerpos tal que K sea un cuerpo de escisión de G y sea V un $k[G]$-módulo simple.*

a) Los factores de composición del $K[G]$-módulo V_K tienen todos la misma multiplicidad m.

b) Si $\operatorname{car} k \neq 0$, entonces $m = 1$.

c) Los caracteres χ_i asociados a los factores de composición de V_K forman una clase de conjugación sobre k. En particular, todos determinan el mismo cuerpo $L = k(\chi_i) \subset K$.

d) Los factores de composición de V_L tienen todos multiplicidad 1.

e) Si Z es un factor de composición de V_L, entonces Z_K tiene un único factor de composición, con multiplicidad m.

f) Los módulos V_L y V_K son semisimples.

DEMOSTRACIÓN: Sea W un factor de composición de V_K, sea χ su carácter y sea $L = k(\chi)$. Los factores de composición de V son factores de composición de las extensiones de coeficientes de los factores de composición de V_L, luego podemos tomar un factor de composición Z de V_L tal que W sea un factor de composición de Z_K.

Veamos que W es el único factor de composición de Z_K (con cierta multiplicidad m). Notemos que esto implica que el carácter de Z (que es el mismo que el de Z_K) es $m\chi$.

Si k tiene característica prima, esto es consecuencia inmediata del teorema 3.58, pues (combinado con 3.38) nos da que $W = Z_K$, luego en este caso tenemos además que $m = 1$. Supongamos ahora que $\operatorname{car} k = 0$.

Sea L_0/L una extensión finita tal que L_0 sea un cuerpo de escisión de G. Podemos suponer que L_0 y K están contenidos en un mismo cuerpo L_0K (por ejemplo, podemos tomar una extensión ciclotómica adecuada de L en la clausura algebraica de K). Como L_0, K y L_0K son todos cuerpos de escisión de G, el teorema 3.39 nos da que χ —que en principio es un carácter irreducible de G sobre K— es también un carácter irreducible de G sobre L_0K y también sobre L_0.

Si tomamos un $L_0[G]$-módulo Z' con carácter χ y lo consideramos como $L[G]$-módulo, el teorema anterior nos da que su carácter sobre L pasa a ser $n\chi$. Entonces, Z'_K también tiene carácter $n\chi$, luego tiene a W como factor de composición, al igual que Z_K, luego $Z = Z'$, por 3.38, luego el carácter de Z_K es $m\chi$, y esto significa que su único factor de composición es W, como queríamos probar.

Sea $\mathcal{G} = G(L/k)$ y sean $\chi = \chi_1, \ldots, \chi_n$ los caracteres conjugados de χ sobre k, donde $n = |L : k| = |\mathcal{G}|$. Pongamos que $\mathcal{G} = \{\tau_1, \ldots, \tau_n\}$, de manera que $\chi_i = \chi^{\tau_i}$. El $L[G]$-módulo Z^{τ_i} tiene carácter $m\chi_i$, luego los $L[G]$-módulos Z^{τ_i} son no isomorfos dos a dos, pues tienen caracteres distintos. También es claro que los $K[G]$-módulos $(Z^{\tau_i})_K$ tienen cada uno un único factor de composición distinto, aunque siempre con multiplicidad m.

Ahora demostraremos que los $L[G]$-módulos Z^{τ_i} son los factores de composición de V_L, y que todos ellos tienen multiplicidad 1 en V_L. Con esto serán inmediatas todas las afirmaciones del enunciado excepto la última.

Como Z es un factor de composición de V_L y $(V_L)^{\tau_i} = V_L$ (porque podemos tomar como representación matricial de V_L una de V, con coeficientes en k), resulta que todos los Z^{τ_i} son factores de composición de V_L. Por consiguiente,

$$n \dim_L Z \leq \dim_L V_L.$$

Por otra parte, si Z_k es el $L[G]$-módulo Z considerado como $k[G]$-módulo, el teorema anterior implica que Z_k tiene a V como único factor de composición, luego

$$\dim_L V_L = \dim_k V \leq \dim_k Z_k = n \dim_L Z.$$

Así pues, se da la igualdad $\dim_L V_L = n \dim_L Z$, de la que se sigue que V_L no puede tener más factores de composición que los n módulos Z^{τ_i}, y que todos ellos han de tener multiplicidad 1.

Sólo falta probar que V_L y V_K son completamente reducibles, lo cual es trivial si $\operatorname{car} k = 0$. Supongamos, pues, que k tiene característica prima. Teniendo en cuenta la parte del teorema ya probada, es claro que Z es un factor de composición arbitrario de V_L. Podemos tomar concretamente como Z un factor de composición que aparezca en primer lugar en una serie de composición de V_L, es decir, un submódulo simple de V_L. Si fijamos una L-base de Z y la extendemos hasta una L-base de V_L, la representación matricial asociada a V_L cumple, para todo $\sigma \in G$:

$$\rho_{V_L}(\sigma) = \left(\begin{array}{c|c} \rho_Z(\sigma) & 0 \\ \hline * & * \end{array}\right).$$

Las matrices de $\rho_{V_L}^{\tau_i}$ tienen la misma estructura, con $\rho_{Z^{\tau_i}}$ en el primer bloque, lo cual se traduce en que $V_L^{\tau_i} = V_L$ tiene un $L[G]$-submódulo isomorfo a Z^{τ_i}. Por consiguiente, si llamamos S a la suma de un $L[G]$-submódulo simple de V_L isomorfo a cada Z^{τ_i}, tenemos que S es un $L[G]$-módulo semisimple (teorema 3.3) que tiene los mismos factores de composición que V_L. Como éstos tienen multiplicidad 1 en V_L, ha de ser $V_L = S$, luego V_L es semisimple.

La prueba para V_K es análoga: considerando a Z^{τ_i} como submódulo de V_L, vemos que $(Z^{\tau_i})_K$ es un submódulo de V_K (simple, por la propiedad e). Como los factores de composición de V_K son los $(Z^{\tau_i})_K$ y todos tienen multiplicidad 1, concluimos igualmente que V_K es semisimple. ∎

Definición 3.66 Sea G un grupo finito y K/k una extensión de cuerpos tal que K sea un cuerpo de escisión de G. Sea W un $K[G]$-módulo simple y sea V el único $k[G]$-módulo simple tal que V_K tiene a W como factor de composición. La multiplicidad $m = m_k(V)$ dada por el teorema anterior para el $k[G]$-módulo V se llama *índice de Schur* de V sobre k. Si χ es el carácter de W, se dice también que $m = m_k(\chi)$ es el *índice de Schur* de χ sobre k.

Hemos probado que si K tiene característica prima, todos los $K[G]$-módulos irreducibles (o todos los caracteres irreducibles) tienen índice de Schur igual a 1 sobre cualquier subcuerpo.

Como aplicación, probamos un resultado sobre radicales de Jacobson:

Teorema 3.67 *Sea G un grupo finito y K/k una extensión de cuerpos tal que K sea un cuerpo de escisión de G. Entonces $J(K[G]) = KJ(k(G))$.*

DEMOSTRACIÓN: Si $x \in J(k[G])$, entonces x anula a todos los $k[G]$-módulos simples. Si V es un $K[G]$-módulo simple, entonces existe un $k[G]$-módulo simple W tal que V es un factor de composición de W_K. El hecho de que x anule a W implica que también anula a W_K, y esto a su vez implica que anula a V. Por lo tanto, $x \in J(K[G])$. Como $J(K[G])$ es un ideal, concluimos que $KJ(k[G]) \subset J(K[G])$.

Por otra parte, hemos probado que las extensiones de coeficientes de los $k[G]$-módulos simples son semisimples, luego lo mismo vale para $k[G]$-módulos semisimples. En particular, el $K[G]$-módulo $(k[G]/J(k[G]) \otimes_k K$ es semisimple. Teniendo en cuenta la sucesión exacta

$$0 \longrightarrow J(k[G]) \otimes_k K \longrightarrow K[G] \longrightarrow (k[G]/J(k[G]) \otimes_k K \longrightarrow 0,$$

vemos que $KJ(k[G])$ es un ideal de $K[G]$ cuyo cociente es semisimple. Según las observaciones posteriores a 3.25, podemos concluir que $J(K[G]) \subset KJ(k[G])$. ∎

Capítulo IV

Representaciones modulares

En este capítulo relacionaremos las representaciones de grupos finitos en cuerpos de característica 0 con las representaciones en cuerpos de característica prima p a través de los cuerpos locales, es decir, las extensiones finitas K de los cuerpos de números p-ádicos $\mathbb{Q}_p$, de modo que podemos considerar las representaciones sobre el propio K, que es un cuerpo de característica 0, y sobre su cuerpo de restos, que es un cuerpo de característica prima. Dedicamos la primera sección a presentar una variante de los anillos de Grothendieck $R_k(G)$ que será más adecuada para tratar el caso en que la característica del cuerpo divide al orden del grupo.

4.1 Representaciones proyectivas

Entre las diferencias que presenta la teoría de representaciones lineales en el caso en que la característica del grupo no divide al orden del grupo y el caso opuesto en que sí que la divide —aparte del hecho fundamental de que el álgebra $k[G]$ es semisimple en el primer caso y no en el segundo— cabe destacar que en el caso de las representaciones ordinarias podemos definir una forma bilineal en el anillo de caracteres virtuales o, equivalentemente, en el anillo de Grothendieck, de forma que se cumplen las relaciones de ortogonalidad.

Si intentamos trasladar esto al caso en que la característica del cuerpo divide al orden del grupo, nos encontramos, para empezar, con que no podemos dividir entre $|G|$ para definir la forma bilineal en el anillo de caracteres virtuales y, si eliminamos esta división, obtenemos la forma bilineal nula. En el anillo de Grothendieck tampoco podemos definir la forma bilineal como en el teorema 3.47 porque los anillos de homomorfismos no son aditivos respecto a sucesiones exactas. No obstante, esto puede remediarse si nos restringimos a la categoría de $k[G]$-módulos proyectivos:

Definición 4.1 Sea G un grupo finito y k un cuerpo. Llamaremos $P_k(G)$ al grupo de Grothendieck asociado a la categoría de los $k[G]$-módulos proyectivos

finitamente generados. Definimos

$$P_k^+(G) = \{[M] \in P_k(G) \mid M \text{ es un } k[G]\text{-módulo proyectivo f.g.}\},$$

Si $\operatorname{car} k \nmid |G|$, entonces todo $k[G]$-módulo finitamente generado es proyectivo, pues es suma directa de $k[G]$-módulos simples y cada $k[G]$-módulo simple es un sumando directo de $k[G]$. Por consiguiente, en este caso $P_k(G) = R_k(G)$.

Vamos a investigar la estructura de $P_k(G)$. Para cada $k[G]$-módulo semisimple V finitamente generado, llamemos $f : P_V \longrightarrow V$ a su envoltura proyectiva (definición 1.56). Si N es el núcleo de f, el hecho de que f sea esencial implica que $N \subset P_V J(k[G])$ (por los teoremas 3.29 y 3.30), y el hecho de que V sea semisimple implica que $P_V J(k[G]) \subset N$ (por las observaciones tras 3.25). Por lo tanto, $N = P_V J(k[G])$, luego

$$V \cong P_V / P_V J(k[G]).$$

Vemos, pues, que dos $k[G]$-módulos semisimples son isomorfos si y sólo si sus envolturas proyectivas son isomorfas. Por otra parte, todo $k[G]$-módulo proyectivo finitamente generado P es la envoltura proyectiva de un $k[G]$-módulo semisimple, a saber, de $V = P/PJ(k[G])$.

En definitiva, vemos que, a través de las envolturas proyectivas, las clases de isomorfía de $k[G]$-módulos semisimples se corresponden biunívocamente con las clases de isomorfía de $k[G]$-módulos proyectivos finitamente generados. Veamos ahora que los $k[G]$-módulos simples se corresponden con los $k[G]$-módulos proyectivos indescomponibles, en el sentido siguiente:

Definición 4.2 Si A es un anillo, un A-módulo $M \neq 0$ es *indescomponible* si no puede descomponerse en suma directa de dos submódulos propios.

Es claro que todo A-módulo simple es indescomponible y, si A es un anillo semisimple, un A-módulo finitamente generado es indescomponible si y sólo si es simple. En general, si A tiene longitud finita, entonces todo A-módulo finitamente generado se descompone en suma directa de A-submódulos indescomponibles.

Volviendo al caso de los $k[G]$-módulos, observemos que si $P_i \longrightarrow V_i$, para $i = 1, \ldots, n$, son las envolturas proyectivas de los $k[G]$-módulos V_i, entonces

$$P_1 \oplus \cdots \oplus P_h \longrightarrow V_1 \oplus \cdots \oplus V_h$$

es la envoltura proyectiva de $V_1 \oplus \cdots \oplus V_h$. En efecto, si N_i es el núcleo de la envoltura proyectiva de V_i, entonces $N_i = P_i J(k[G])$, luego

$$N = N_1 \oplus \cdots \oplus N_h \subset (P_1 \oplus \cdots \oplus P_h) J(k[G]),$$

lo que prueba que la suma de las envolturas proyectivas es un homomorfismo esencial y, por consiguiente, es la envoltura proyectiva de la suma de los módulos dados.

Así pues, si V es un $k[G]$-módulo tal que P_V no es indescomponible, podemos expresar $P_V = P_1 \oplus P_2$, para ciertos $k[G]$-submódulos propios P_i. Llamamos $V_i = P_i/P_iJ(k[G])$, que son $k[G]$-módulos semisimples cuya envoltura proyectiva es P_i. Según hemos visto, P_V es entonces la envoltura proyectiva de $V_1 \oplus V_2$, luego

$$V_1 \oplus V_2 \cong P_V/PJ(k[G]) \cong V.$$

Así pues, V no es simple. Recíprocamente, si $V = V_1 \oplus V_2$ no es simple, entonces $P_V \cong P_{V_1} \oplus P_{V_2}$ no es indescomponible. Ahora es inmediato el teorema siguiente:

Teorema 4.3 *Sea G un grupo finito y k un cuerpo. Entonces, todo $k[G]$-módulo proyectivo finitamente generado P se descompone de forma única (salvo isomorfismo y reordenación de sumandos) como suma directa de submódulos proyectivos indescomponibles. Concretamente, si la descomposición del $k[G]$-módulo semisimple*

$$V = P/PJ(k[G])$$

en suma de submódulos simples es $V = V_1 \oplus \cdots \oplus V_h$, entonces la única descomposición de P en submódulos proyectivos indescomponibles es $P = P_{V_1} \oplus \cdots \oplus P_{V_h}$, donde P_{V_i} es la envoltura proyectiva de V_i.

A su vez, de aquí se sigue trivialmente:

Teorema 4.4 *Sea G un grupo finito y k un cuerpo. Entonces:*

a) Si P_1 y P_2 son dos $k[G]$-módulos proyectivos finitamente generados, entonces $[P_1] = [P_2]$ en $P_k(G)$ si y sólo si $P_1 \cong P_2$.

b) $P_k(G)$ es un $\mathbb{Z}$-módulo libre de base

$$I_k(G) = \{[M] \in P_k(G) \mid M \text{ es indescomponible } \}.$$

Demostración: Como todo $k[G]$-módulo proyectivo finitamente generado es suma directa de submódulos proyectivos indescomponibles, es claro que $I_k(G)$ es un sistema generador de $P_k(G)$. Puesto que el número de $k[G]$-módulos simples no isomorfos dos a dos es finito, lo mismo sucede con el de $k[G]$-módulos proyectivos indescomponibles finitamente generados. Sea $P_1, \ldots, P_h$ un sistema de representantes de las clases de isomorfía.

Para cada $k[G]$-módulo proyectivo finitamente generado P, definimos $m_i(P)$ como el número de sumandos isomorfos a V_i en la descomposición de P en suma de $k[G]$-módulos indescomponibles. Observemos que todas las sucesiones exactas de $k[G]$-módulos proyectivos se escinden, por lo que la aditividad requerida para que una función f induzca un homomorfismo sobre $P_k(G)$ se reduce a que

$$f(P \oplus Q) = f(P) + f(Q).$$

En el caso concreto de las funciones m_i, tenemos ciertamente que

$$m_i(P \oplus Q) = m_i(P) + m_i(Q),$$

luego inducen homomorfismos $m_i : P_k(G) \longrightarrow \mathbb{Z}$ tales que $m_i([P]) = m_i(P)$. En particular, $m_i([P_j]) = \delta_{ij}$, donde (δ_{ij}) es la matriz identidad. Esto prueba el apartado a) para módulos indescomponibles. Los m_i determina un isomorfismo $P_k(G) \cong \mathbb{Z}^h$ que hace corresponder $I_k(G)$ con la base canónica de $\mathbb{Z}^h$, lo cual prueba el apartado b).

Por último, la igualdad $[P_1] = [P_2]$ equivale a que $m_i(P_1) = m_i(P_2)$ para todo i, lo cual equivale claramente a que $P_1 \cong P_2$. ∎

El teorema 1.58 nos permite dotar a $P_k(G)$ de estructura de anillo.

Teorema 4.5 *Si G es un grupo finito y k es un cuerpo, el grupo $P_k(G)$ adquiere estructura de anillo conmutativo con el producto determinado por*

$$[P] \cdot [Q] = [P \otimes_k Q],$$

para todo par de $k[G]$-módulos proyectivos finitamente generados P y Q, así como estructura de $R_k(G)$-álgebra con el producto determinado por

$$[P] \cdot [V] = [P \otimes_k V],$$

donde P y V son $k[G]$-módulos finitamente generados y P es proyectivo.

Si $\mathcal{C}$ es la categoría de los $k[G]$-módulos finitamente generados y $\mathcal{C}'$ la de los $k[G]$-módulos proyectivos finitamente generados, consideramos la aplicación

$$\langle \ , \ \rangle : \mathcal{C}' \times \mathcal{C} \longrightarrow \mathbb{Z}$$

dada por

$$\langle P, V\rangle = \dim_k \operatorname{Hom}(P, V).$$

Vamos a ver que, al restringir el primer argumento a módulos proyectivos, esta aplicación sí que define una forma bilineal sobre los grupos de Grothendieck respectivos. En efecto, por una parte, una sucesión exacta en $\mathcal{C}'$ es de la forma

$$0 \longrightarrow P_1 \longrightarrow P_1 \oplus P_2 \longrightarrow P_2 \longrightarrow 0,$$

de modo que, como en el caso de $R_k(G)$, se cumple que

$$\operatorname{Hom}(P_1 \oplus P_2, V) \cong \operatorname{Hom}(P_1, V) \oplus \operatorname{Hom}(P_2, V),$$

luego

$$\langle P_1 \oplus P_2, V\rangle = \langle P_1, V\rangle + \langle P_2, V\rangle .$$

Por otra parte, dada una sucesión exacta

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

en $\mathcal{C}$ y $P \in \mathcal{C}'$, el teorema 1.51 nos da la sucesión exacta

$$0 \longrightarrow \operatorname{Hom}(P, M') \longrightarrow \operatorname{Hom}(P, M) \longrightarrow \operatorname{Hom}(P, M'') \longrightarrow 0.$$

Tomando dimensiones sobre k, llegamos a que

$$\langle P, M\rangle = \langle P, M'\rangle + \langle P, M''\rangle .$$

El teorema 3.45 nos da ahora:

Teorema 4.6 *Sea G un grupo finito y k un cuerpo. Entonces existe una forma bilineal $\langle\ ,\ \rangle : P_k(G) \times R_k(G) \longrightarrow \mathbb{Z}$ determinada por que, para todo par de $k[G]$-módulos finitamente generados P y M (con P proyectivo), se cumple que*

$$\langle [P], [M] \rangle = \dim_k \mathrm{Hom}(P, M).$$

Observemos ahora que si $[V], [V'] \in S_k(G)$ y $f : P_V \longrightarrow V$ es la envoltura proyectiva de V, entonces tenemos un isomorfismo canónico de k-espacios vectoriales

$$\mathrm{Hom}(V, V') \cong \mathrm{Hom}(P_V, V')$$

dado por $g \mapsto f \circ g$. En efecto, es claro que se trata de un monomorfismo y, dado $h : P_V \longrightarrow V'$ no nulo, como V' es simple, ha de ser suprayectivo, luego el núcleo de h está contenido en $J(P_V)$, que es el núcleo de f, luego h induce un homomorfismo $g : V \longrightarrow V'$ tal que $f \circ g = h$.

Así pues, $\langle [P_V], [V'] \rangle = \dim_k \mathrm{Hom}(V, V')$ y, en particular, si

$$S_k(G) = \{[V_1], \ldots, [V_h]\}, \qquad I_k(G) = \{[P_{V_1}], \ldots, [P_{V_h}]\},$$

entonces

$$\langle [P_{V_i}], [V_j] \rangle = \begin{cases} \dim_k \mathrm{End}(V_i) & \text{si } i = j, \\ 0 & \text{si } i \neq j. \end{cases}$$

Si k es un cuerpo de escisión de G, el teorema 3.34 nos da que $S_k(G)$ e $I_k(G)$ son bases duales respecto de la forma bilineal dada por el teorema anterior. En tal caso, $\langle [P], [V_j] \rangle$ es el número de veces que P_{V_j} aparece en la descomposición de P en $k[G]$-módulos proyectivos indescomponibles.

Teorema 4.7 *Sea G un grupo finito, k un cuerpo de escisión para G, sean $V_1, \ldots, V_h$ un sistema de representantes de los $k[G]$-módulos simples y sean $P_{V_1}, \ldots, P_{V_h}$ sus envolturas proyectivas. Entonces*

$$k[G] = \bigoplus_{j=1}^{h} P_{V_j}^{n_j},$$

donde $n_j = \dim_k V_j$. En particular, si $N_j = \dim_k P_{V_j}$, tenemos que

$$\sum_{j=1}^{h} N_j n_j = |G|.$$

Demostración: Basta observar que

$$\langle [k[G], [V_j] \rangle = \dim_k \mathrm{Hom}(k[G], V_j) = \dim_k V_j = n_j,$$

luego P_{V_j} aparece n_j veces en la descomposición de G. ∎

Una última relación elemental entre $R_k(G)$ y $P_k(G)$ es que entre ambos podemos definir el homomorfismo siguiente:

Definición 4.8 Sea G un grupo finito y k un cuerpo. El *homomorfismo de Cartan* de G es el homomorfismo $c : P_k(G) \longrightarrow R_k(G)$ determinado por que $c([P]) = [P]$, para todo $k[G]$-módulo proyectivo finitamente generado P. La matriz de c en las bases $I_k(G)$, $S_k(G)$ se llama *matriz de Cartan* de G sobre k.

Concretamente, si V y W son dos $k[G]$-módulos simples, podemos considerar $[P_V] \in I_k(G)$, $[W] \in S_k(G)$. Representamos por $C_{V,W} = C_{[P_V],[W]} \in \mathbb{N}$ el coeficiente correspondiente de la matriz de Cartan. Se trata del coeficiente de $[W]$ en la descomposición de $[P_V]$ como elemento de $R_k(G)$, es decir, el número de veces que W aparece en una serie de composición de P_V.

Teorema 4.9 *Sea G un grupo finito, k un cuerpo y V, W dos $k[G]$-módulos simples. Sea $m_V = \dim_k \operatorname{End}(V)$, $m_W = \dim_k \operatorname{End}(W)$. Entonces*

$$m_W C_{V,W} = m_V C_{W,V}.$$

Demostración: En virtud del teorema 1.66, basta probar que

$$m_V C_{W,V} = \dim_k \operatorname{Hom}(P_V, P_W).$$

Para ello tomamos una serie de composición

$$0 = M_0 \subset M_1 \subset \cdots \subset M_n = P_W,$$

con la que formamos la sucesión exacta

$$0 \longrightarrow M_{n-1} \longrightarrow M_n \longrightarrow M_n/M_{n-1} \longrightarrow 0.$$

El teorema 1.51 nos da la sucesión exacta

$$0 \longrightarrow \operatorname{Hom}(P_V, M_{n-1}) \longrightarrow \operatorname{Hom}(P_V, M_n) \longrightarrow \operatorname{Hom}(P_V, M_n/M_{n-1}) \longrightarrow 0.$$

De aquí deducimos que

$$\dim_k \operatorname{Hom}(P_V, M_n) = \dim_k \operatorname{Hom}(P_V, M_n/M_{n-1}) + \dim_k \operatorname{Hom}(P_V, M_{n-1}).$$

Ahora consideramos la sucesión exacta

$$0 \longrightarrow M_{n-2} \longrightarrow M_{n-1} \longrightarrow M_{n-1}/M_{n-1} \longrightarrow 0$$

y, tras un número finito de pasos, llegamos a que

$$\dim_k \operatorname{Hom}(P_V, P_W) = \dim_k \operatorname{Hom}(P_V, M_n) = \sum_{i=1}^{n} \dim_k \operatorname{Hom}(P_V, M_i/M_{i-1})$$

$$= \sum_{i=1}^{n} \dim_k \operatorname{Hom}(V, M_i/M_{i-1})$$

(por la observación tras el teorema 4.6). El lema de Schur 3.12 implica que el último sumatorio es igual a $m_V C_{WV}$. ∎

Si k es un cuerpo de escisión de G, el teorema 3.34 implica que $m_V = 1$ para todo $K[G]$-módulo simple. Por lo tanto:

Teorema 4.10 *Si G es un grupo finito y k es un cuerpo de escisión de G, entonces la matriz de Cartan de G sobre k es simétrica.*

Otra propiedad de la matriz de Cartan que podemos probar fácilmente es la siguiente:

Teorema 4.11 *Si G es un grupo finito y V es un $k[G]$-módulo simple, V es proyectivo si y sólo si $c_{VV} = 1$.*

DEMOSTRACIÓN: Obviamente, si V es proyectivo, $P_V = V$ y $c_{VV} = 1$. Por otra parte, el teorema 1.66 nos da que

$$\dim_k \mathrm{Hom}_G(V, P_V) = \dim_k \mathrm{Hom}_G(P_V, V) \geq 1,$$

luego existe un homomorfismo no nulo $V \longrightarrow P_V$. Como V es simple, ha de ser un monomorfismo, luego P_V tiene un submódulo isomorfo a V. Por consiguiente, podemos formar una serie de composición

$$0 = V_0 \subset V_1 \subset \cdots \subset V_{n-1} \subset V_n = P_V$$

con $V_1 \cong V$. Si V no es proyectivo, entonces $n \geq 2$. Como P_V/V_{n-1} es simple, ha de ser $P_V J(k[G]) \subset V_{n-1}$, pero, como

$$P_V/P_V J(k[G]) \cong V,$$

ha de ser $P_V/V_{n-1} \cong V$, luego P_V tiene al menos dos factores de composición isomorfos a V, a saber, V_1/V_0 y V_n/V_{n-1}, luego $c_{VV} \geq 2$. ∎

4.2 Representaciones en anillos locales

Vamos a ver que si K es un cuerpo local cuyo cuerpo de restos k tiene característica p, cada representación lineal de G sobre K determina una "reducción módulo p", que es una representación lineal de G sobre k. Ello exige pasar primero a una representación de G sobre el anillo de enteros de K y, desde ésta, pasar a una representación sobre k. En realidad, los resultados de esta sección son válidos cuando K es el cuerpo de cocientes de un anillo de valoración discreta de característica 0, sin que sea necesario exigir completitud.

Teorema 4.12 *Sea A un anillo conmutativo, G un grupo finito y P un $A[G]$-módulo finitamente generado. Entonces, P es un $A[G]$-módulo proyectivo si y sólo si es un A-módulo proyectivo y existe un A-endomorfismo $u : P \longrightarrow P$ tal que, para todo $v \in P$,*

$$\sum_{\sigma \in G} u(v\sigma^{-1})\sigma = v.$$

DEMOSTRACIÓN: Como $A[G]$ es un A-módulo libre, todo $A[G]$-módulo libre es también un A-módulo libre, luego todo $A[G]$-módulo proyectivo es también un A-módulo proyectivo.

Supongamos ahora que P es proyectivo como A-módulo y sea $Q = P \otimes_A A[G]$, considerado como $A[G]$-módulo con el producto derivado de la estructura de $A[G]$-bimódulo de $A[G]$, es decir, de modo que

$$(v \otimes x)y = v \otimes xy \quad (\text{y no } (v \otimes x)y = vy \otimes xy).$$

Se cumple entonces que Q es un $A[G]$-módulo proyectivo, pues si P' es un A-módulo tal que $P \oplus P' \cong A^n$, entonces tenemos los isomorfismos de $A[G]$-módulos

$$Q \oplus (P' \otimes_A A[G]) \cong A^n \otimes_A A[G] \cong A[G]^n.$$

Sea $q : Q \longrightarrow P$ el epimorfismo de $A[G]$-módulos dado por $q(v \otimes \sigma) = v\sigma$. Tenemos una sucesión exacta de homomorfismos de $A[G]$-módulos

$$0 \longrightarrow N \longrightarrow Q \longrightarrow P \longrightarrow 0,$$

que se escinde si y sólo si P es proyectivo. (Una implicación por el teorema 1.52, la otra porque si la sucesión se escinde, entonces P es un sumando directo de Q, que es proyectivo.) Teniendo en cuenta el teorema 1.35, llegamos a que P es un $A[G]$-módulo proyectivo si y sólo si existe un $A[G]$-homomorfismo $f : P \longrightarrow Q$ tal que $f \circ q = 1$.

Un $A[G]$-homomorfismo $f : P \longrightarrow Q$ arbitrario es de la forma

$$f(v) = \sum_{\sigma \in G} u_\sigma(v) \otimes \sigma,$$

donde $u_\sigma \in \mathrm{End}_A(P)$. La ecuación $f(v\sigma^{-1}) = f(v)\sigma^{-1}$ nos da la relación $u_\sigma(v) = u_1(v\sigma^{-1})$, luego, llamado $u = u_1$, vemos que todo $A[G]$-homomorfismo $f : P \longrightarrow Q$ es de la forma

$$f(v) = \sum_{\sigma \in G} u(v\sigma^{-1}) \otimes \sigma,$$

para cierto $u \in \mathrm{End}_A(P)$. La condición $f \circ q = 1$ equivale a que

$$\sum_{\sigma \in G} u(v\sigma^{-1})\sigma = v$$

para todo $v \in P$. ∎

A partir de aquí consideraremos un dominio íntegro local D con ideal maximal $\mathfrak{m}$ y cuerpo de restos $k = D/\mathfrak{m}$. Para cada $D[G]$-módulo V, podemos considerar el k-espacio vectorial $\overline{V} = V \otimes_D k$, al que podemos dotar de estructura de $k[G]$-módulo mediante

$$(v \otimes \alpha)\sigma = (v\sigma) \otimes \alpha.$$

Si V es libre de rango finito sobre D, una base $v_1, \ldots, v_n$ de V determina una representación matricial $\rho : G \longrightarrow \mathrm{Mat}_n(D)$. Entonces, $v_i \otimes 1$ es una base de $\overline{V}$ sobre k, y la representación matricial de G sobre k asociada a esta base es la *reducción módulo* $\mathfrak{m}$ de ρ, es decir, la representación $\bar{\rho}$ en la que $\bar{\rho}(\sigma)$ es

la matriz cuyos coeficientes son las clases módulo $\mathfrak{m}$ de los coeficientes de $\rho(\sigma)$. Por ello, al módulo $\overline{V}$ lo llamaremos *reducción módulo* $\mathfrak{m}$ de V.

Observemos que, si V es libre sobre D, el producto $V\otimes_D$ conserva la exactitud de la sucesión

$$0 \longrightarrow \mathfrak{m} \longrightarrow D \longrightarrow k \longrightarrow 0,$$

con lo que obtenemos que $\overline{V} \cong V/V\mathfrak{m}$.

Teorema 4.13 *Sea D un dominio íntegro local, sea $\mathfrak{m}$ su ideal maximal y sea $k = D/\mathfrak{m}$ su cuerpo de restos.*

a) Si P es un $D[G]$-módulo finitamente generado que es libre como D-módulo, entonces P es proyectivo como $D[G]$-módulo si y sólo si el $k[G]$-módulo $\overline{P} = P \otimes_D k$ es proyectivo.

b) Dos $D[G]$-módulos proyectivos finitamente generados P y P' libres sobre D son isomorfos si y sólo si los son los $k[G]$-módulos $\overline{P}$ y $\overline{P}'$.

Demostración: a) Si P es proyectivo, existe un $D[G]$-módulo P' tal que $P \oplus P'$ es libre. Teniendo en cuenta que $D[G] \otimes_D k \cong k[G]$, es claro que $\overline{P} \oplus \overline{P}'$ es un $k[G]$-módulo libre, luego $\overline{P}$ es proyectivo.

Supongamos ahora que $\overline{P}$ es proyectivo. El teorema 4.12 nos da un k-endomorfismo $\bar{u} : \overline{P} \longrightarrow \overline{P}$ tal que

$$\sum_{\sigma\in G} \bar{u}(v\sigma^{-1})\sigma = v,$$

para todo $v \in \overline{P}$. Como P es un D-módulo libre, podemos definir un D-endomorfismo $u : P \longrightarrow P$ que haga conmutativo el diagrama siguiente:

$$\begin{array}{ccc} P & \xrightarrow{u} & P \\ \downarrow & & \downarrow \\ \overline{P} & \xrightarrow[\bar{u}]{} & \overline{P} \end{array}$$

donde las flechas verticales se identifican con el epimorfismo $P \longrightarrow P/V\mathfrak{m}$. Si llamamos $u' : P \longrightarrow P$ al D-homomorfismo dado por

$$u'(v) = \sum_{\sigma\in G} u(v\sigma^{-1})\sigma,$$

tenemos claramente un diagrama conmutativo análogo con u' y la identidad en $\overline{P}$, es decir, que $u'(v) \equiv v$ (mód $V\mathfrak{m}$) para todo $v \in V$. En particular, el determinante de la matriz de u' respecto de una base de V es $\equiv 1$ (mód $\mathfrak{m}$), luego es una unidad de D, luego u' es un D-automorfismo de P. Más aún, es claro que se trata de un $D[G]$-automorfismo. Por consiguiente:

$$\sum_{\sigma\in G} (u'^{-1}u)(v\sigma^{-1})\sigma = \sum_{\sigma\in G} u(u'^{-1}(v)\sigma^{-1})\sigma = u'(u'^{-1}(v)) = v.$$

Así pues, el D-endomorfismo $u'^{-1}u$ nos permite aplicar el teorema 4.12 para concluir que P es un $D[G]$-módulo proyectivo.

b) Una implicación es obvia. Si $\bar{w} : \overline{P} \longrightarrow \overline{P}'$ es un $k[G]$-homomorfismo, la proyectividad de P nos da un $k[G]$-homomorfismo $w : P \longrightarrow P'$ que hace conmutativo el diagrama

$$\begin{array}{ccc} P & \xrightarrow{w} & P \\ \downarrow & & \downarrow \\ \overline{P} & \xrightarrow[\bar{w}]{} & \overline{P} \end{array}$$

Si $\bar{w}$ es un isomorfismo, el determinante de w en una D-base de P es congruente módulo $\mathfrak{m}$ con el determinante de $\bar{w}$ en la base de $\overline{P}$ inducida por la base dada. En particular, es no nulo módulo $\mathfrak{m}$, luego es una unidad en D, luego w es un isomorfismo. ∎

En adelante supondremos que D es un anillo de valoración discreta. Como antes, llamaremos $\mathfrak{m}$ a su ideal maximal y $k = D/\mathfrak{m}$ a su cuerpo de restos. Además, llamaremos K a su cuerpo de cocientes.

Definición 4.14 En las condiciones anteriores, si V es un K-espacio vectorial de dimensión finita, llamaremos *retículo* en V a todo D-submódulo de V finitamente generados que sea un sistema generador de V como K-espacio vectorial.

Equivalentemente, un retículo $R \subset V$ es el D-módulo generado por un sistema generador finito de V. El hecho de que V es un espacio vectorial implica que R es un D-módulo libre de torsión, luego es un D-módulo libre.[1] Es fácil ver que una D-base de R es también una K-base de V, por lo que el rango de R como D-módulo coincide con la dimensión de V.

Sea G un grupo finito y supongamos que V es un $K[G]$-módulo finitamente generado, con lo que también es un K-espacio vectorial de dimensión finita. Diremos que un retículo $R \subset V$ es *estable* si $R\sigma \subset R$ para todo $\sigma \in G$ (lo cual implica que, de hecho, $R\sigma = R$).

Es claro que todo $K[G]$-módulo V tiene retículos estables: basta tomar un sistema generador finito B de V como K-espacio vectorial y considerar el D-módulo generado por el conjunto finito $\bigcup_{\sigma\in G} B\sigma$.

Si R es un retículo estable, entonces es un $D[G]$-módulo y es libre como D-módulo, luego podemos considerar su reducción $\overline{R} = R \otimes_D k$ módulo $\mathfrak{m}$, que es un $k[G]$-módulo finitamente generado. A su vez, podemos considerar su imagen $[\overline{R}] \in R_k(G)$ en el anillo de Grothendieck de G sobre k.

Teorema 4.15 *Sea D un anillo de valoración discreta con cuerpo de cocientes K y cuerpo de restos k. Sea G un grupo finito. Si V es un $K[G]$-módulo finitamente generado y R_1, R_2 son dos retículos estables en V, entonces se cumple que $[\overline{R}_1] = [\overline{R}_2]$ en $R_k(G)$.*

[1] Por el teorema 16.8 de mi libro de *Álgebra*. Nótese que todo anillo de valoración discreta es un dominio euclídeo.

DEMOSTRACIÓN: Consideremos primero el caso en que $R_1\mathfrak{m} \subset R_2 \subset R_1$. Entonces $T = R_1/R_2$ es un $D[G]$-módulo tal que $T\mathfrak{m} = 0$, luego tiene una estructura natural de $k[G]$-módulo (pues $k[G] = D[G]/D[G]\mathfrak{m}$). El epimorfismo canónico $R_1 \longrightarrow T$ tiene a $R_1\mathfrak{m}$ en su núcleo, luego induce un epimorfismo $\overline{R}_1 \longrightarrow T$, cuyo núcleo es $\overline{R}_2$, con lo que podemos forma la sucesión exacta

$$0 \longrightarrow T \longrightarrow \overline{R}_2 \longrightarrow \overline{R}_1 \longrightarrow T \longrightarrow 0,$$

en la que el primer monomorfismo es la multiplicación por un generador de $\mathfrak{m}$. De aquí se sigue fácilmente que, al pasar a $R_k(G)$, obtenemos la relación

$$[T] - [\overline{R}_2] + [\overline{R}_1] - [T] = 0,$$

luego $[\overline{R}_1] = [\overline{R}_2]$.

Consideramos ahora el caso general. Si tomamos sendas bases de R_1 y R_2 como D-módulos, ambas son bases de V como K-espacio vectorial, luego cada elemento de la base de R_2 puede expresarse como combinación lineal de la base de R_1 con coeficientes en K. Estos coeficientes son fracciones de D, luego, llamando $m \neq 0$ al producto de los denominadores de todos ellos, tenemos que mR_2 tiene una base cuyos elementos son combinaciones lineales en D de una base de R_1. Equivalentemente, $mR_2 \subset R_1$.

Como $R_2 \cong mR_2$ (como D-módulos), también $\overline{R}_1 \cong \overline{mR_2}$ (como k-espacios vectoriales), luego no perdemos generalidad si suponemos que $R_2 \subset R_1$. Por el mismo razonamiento anterior, existe un $m \in D$ no nulo tal que $mR_1 \subset R_2$. Existe un $n \geq 0$ tal que $m \in \mathfrak{m}^n$, luego $R_1\mathfrak{m}^n \subset R_2$.

Así pues, basta probar por inducción sobre n que si dos retículos estables cumplen

$$R_1\mathfrak{m}^n \subset R_2 \subset R_1,$$

entonces $[\overline{R}_1] = [\overline{R}_2]$. Si $n = 0$ tenemos que $R_1 = R_2$ y el resultado es obvio. Supuesto cierto para $n-1$, llamamos $R_3 = R_1\mathfrak{m}^{n-1} + R_2$, que es otro retículo estable de V que cumple

$$R_1\mathfrak{m}^{n-1} \subset R_3 \subset R_1, \qquad R_3\mathfrak{m} \subset E_2 \subset E_3.$$

Por hipótesis de inducción y por el caso ya probado, $[\overline{R}_1] = [\overline{R}_3] = [\overline{R}_2]$. ∎

Ahora suponemos que D (y, por lo tanto, K) tiene característica 0, de modo que $K[G]$ es semisimple, por lo que toda sucesión exacta de $K[G]$-módulos finitamente generados

$$0 \longrightarrow V' \longrightarrow V \longrightarrow V'' \longrightarrow 0$$

se escinde, es decir, $V = V' \oplus V''$. Por consiguiente, si tomamos retículos estables $R' \subset V'$ y $R'' \subset V''$, resulta que $R = R' \oplus R''$ es un retículo estable en V, y claramente $\overline{R} = \overline{R}' \oplus \overline{R}''$, luego $[\overline{R}] = [\overline{R}'] + [\overline{R}'']$ en $R_k(G)$.

Así pues, la aplicación que a cada $k[G]$-módulo finitamente generado V le asigna $[\overline{R}] \in R_k(G)$, donde R es un retículo estable en V, está bien definida por el teorema anterior, y acabamos de probar que induce un homomorfismo de grupos $R_K(G) \longrightarrow R_k(G)$.

Definición 4.16 Sea D un anillo de valoración discreta de característica 0, sea K su cuerpo de cocientes y k su cuerpo de restos. Si G es un grupo finito, llamaremos *homomorfismo de descomposición* de G respecto a D al homomorfismo $d : R_K(G) \longrightarrow R_k(G)$ determinado por que $d([V]) = [\overline{R}]$, donde $R \subset V$ es cualquier retículo estable. La matriz de d en las bases $S_K(G)$ y $S_k(G)$ se llama *matriz de descomposición* de G (respecto a D).

Teorema 4.17 *En las condiciones anteriores, el homomorfismo de descomposición $d : R_K(G) \longrightarrow R_k(G)$ es un homomorfismo de anillos.*

Demostración: Dados dos $K[G]$-módulos finitamente generados V y V' y sendos retículos estables $R \subset V$ y $R' \subset V'$, es claro que $R \otimes_D R'$ es un retículo estable en $V \otimes_K V'$. (La inclusión natural es inyectiva porque transforma una D-base de $R \otimes_D R'$ en una K-base de $V \otimes_K V'$). Además, existe un isomorfismo natural de $k[G]$-módulos

$$(R \otimes_D R') \otimes_D k \cong (R \otimes_D k) \otimes_k (R' \otimes_D k),$$

dado por

$$(v \otimes v') \otimes 1 \mapsto (v \otimes 1) \otimes (v' \otimes 1).$$

Por consiguiente:

$$d([V] \cdot [V']) = d([V \otimes_K V']) = [\overline{R \otimes_D R'}] = [\overline{R} \otimes_k \overline{R}'] = [\overline{R}] \cdot [\overline{R}'] = d(V) \cdot d(V')$$

y, por linealidad, lo mismo vale para un producto de elementos arbitrarios de $R_K(G)$. ∎

4.3 Representaciones en cuerpos completos

En esta sección supondremos que K es un cuerpo métrico discreto completo de característica 0 y que D es su anillo de enteros (con lo que D sigue siendo un anillo de valoración discreta y se cumplen todas las hipótesis que hemos supuesto en la sección anterior). Si $\mathfrak{m}$ es el ideal maximal de D, entonces los únicos ideales de D son las potencias de $\mathfrak{m}$. Llamemos $D_n = D/\mathfrak{m}^n$, de modo que el cuerpo de restos es $k = D_1$. Necesitaremos el hecho de que D es el límite proyectivo de los anillos D_n. Recordemos la definición de límite proyectivo:

Definición 4.18 Si A es un anillo conmutativo, un *sistema proyectivo* de A-módulos es una sucesión $\{M_n\}_{n=1}^{\infty}$ de A-módulos junto con una sucesión de homomorfismos $\phi_n : M_n \longrightarrow M_{n-1}$. Definimos el *límite proyectivo* del sistema como el submódulo $M = \varprojlim_n M_n$ del producto $\prod_n M_n$ formado por las sucesiones

$$x = (x_1, x_2, x_3, \dots)$$

tales que $\phi_n(x_n) = x_{n-1}$, para todo $n > 1$. Llamaremos $\pi_n : M \longrightarrow M_n$ a las restricciones de las proyecciones. Obviamente $\pi_{n+1} \circ \phi_{n+1} = \pi_n$.

Notemos que si los M_n son anillos y los ϕ_n son homomorfismos de anillos, entonces el límite proyectivo es también un anillo y los homomorfismos π_n son homomorfismos de anillos.

Teorema 4.19 *Los anillos $D_n = D/\mathfrak{m}^n$ forman un sistema proyectivo con los epimorfismos naturales $D_n \longrightarrow D_{n-1}$ inducidos por la identidad en D, y se cumple que*

$$D \cong \varprojlim_n D_n.$$

DEMOSTRACIÓN: Definimos un homomorfismo de anillos $f : D \longrightarrow \varprojlim_n D_n$ asignando a cada $d \in D$ la sucesión de sus clases módulo $\mathfrak{m}^n$.

Se trata de un monomorfismo, pues si $d \in D$ cumple que $f(d) = 0$ entonces $d \in \bigcap_n \mathfrak{m}^n = 0$. Falta probar que también es suprayectivo. Para ello fijamos un primo $\pi \in D$, de modo que $\mathfrak{m} = (\pi)$. Dado $x \in \varprojlim_n D_n$, tenemos que $x_1 = [d_0]$, para un cierto $d_0 \in D$, $x_2 = [c_1]$, para un cierto $c_1 \cong d_0 \pmod{\mathfrak{m}}$, de modo que $c_1 = d_0 + d_1\pi$, para cierto $d_1 \in D$. Similarmente, $x_3 = [c_2]$, para cierto $c_2 = d_0 + d_1\pi + d_2\pi^2$. De este modo construimos una sucesión $d_n \in D$ tal que $x_n = [d_0 + d_1\pi + \cdots + d_{n-1}\pi^{n-1}] \in D/\mathfrak{m}^n$. La completitud de K nos permite definir

$$d = \sum_{n=0}^{\infty} d_n\pi^n \in D,$$

que claramente cumple $f(d) = x$. ∎

Ahora estamos en condiciones de completar el teorema 4.13 con un teorema de existencia:

Teorema 4.20 *Para cada $k[G]$-módulo proyectivo finitamente generado Q, existe un $D[G]$-módulo proyectivo P, único salvo isomorfismo, tal que $Q \cong P \otimes_D k$.*

DEMOSTRACIÓN: Observemos que si P es un $D[G]$-módulo proyectivo finitamente generado, entonces es también un D-módulo proyectivo finitamente generado (por 4.12), luego en particular es un submódulo de un D-módulo libre (finitamente generado), luego P es un D-módulo libre.[2] Por lo tanto, la hipótesis de que P y P' sean libres sobre D en el apartado b) de 4.13 es redundante, y tenemos la unicidad.

Sea $\mathfrak{m}$ el ideal maximal de D y consideremos los anillos $D_n = D/\mathfrak{m}^n$. Los únicos ideales de D son 0 y las potencias de $\mathfrak{m}$, luego los únicos ideales de D_n son las potencias de $\mathfrak{m}$ hasta $\mathfrak{m}^n = 0$. Así pues, D_n tiene un número finito de ideales, luego es noetheriano y artiniano, luego tiene longitud finita.

Como $D_n[G]$ es un D_n-módulo finitamente generado, también tiene longitud finita como D_n-módulo, y esto implica que la tiene como anillo. El epimorfismo natural $D_n \longrightarrow D_1 = k$ induce un epimorfismo $D_n[G] \longrightarrow k[G]$, que nos permite considerar a Q como $D_n[G]$-módulo finitamente generado. Puesto que $D_n[G]$ es artiniano, podemos considerar la envoltura proyectiva $f_n : P_n \longrightarrow Q$. Notemos

[2]Por el teorema 7.29 de mi libro de Álgebra. Notemos que todo anillo de valoración discreta es un dominio de ideales principales.

que $D_1[G] = k[G]$, con lo que $P_1 = Q$ y f_1 es la identidad. El diagrama conmutativo

$$\begin{array}{ccc} D_{n-1}[G] & \longrightarrow & k[G] \\ \uparrow & \nearrow & \\ D_n[G] & & \end{array}$$

nos permite considerar a P_{n-1} y a Q como $D_n[G]$-módulos y a f_{n-1} como un epimorfismo de $D_n[G]$-módulos. La proyectividad de P_n implica entonces la existencia de un homomorfismo de $D_n[G]$-módulos que cierra el diagrama siguiente:

$$\begin{array}{ccc} P_{n-1} & \xrightarrow{f_{n-1}} & Q \\ \uparrow p_n & \nearrow_{f_n} & \\ P_n & & \end{array}$$

Notemos que p_n es suprayectiva porque $f_{n-1}[p_n[P_n]] = Q$ y f_{n-1} es esencial. Más aún, p_n es esencial, pues si $M \subset P_n$ cumple que $p_n[M] = P_{n-1}$, entonces $f_n[M] = Q$, luego $M = P_n$ porque f_n es esencial.

Como P_{n-1} es en realidad un $D_{n-1}[G]$-módulo, el núcleo de p_n ha de contener a $P_n\mathfrak{m}^{n-1}$, luego tenemos un diagrama conmutativo

$$\begin{array}{ccc} P_n & \xrightarrow{p_n} & P_{n-1} \\ \downarrow & \nearrow & \\ P_n/P_n\mathfrak{m}^{n-1} & & \end{array}$$

Ahora bien, $P_n/P_n\mathfrak{m}^{n-1}$ tiene una estructura natural de $D_{n-1}[G]$-módulo, para la cual, la flecha oblicua es un epimorfismo de $D_{n-1}[G]$-módulos. Como P_{n-1} es proyectivo, el teorema 1.52 implica que $P_n/P_n\mathfrak{m}^{n-1}$ tiene un sumando directo M isomorfo a P_{n-1}. Su antiimagen M' en P_n cumple que $p_n[M'] = P_{n-1}$, luego $M' = P_n$, luego $M = P_n/P_n\mathfrak{m}^{n-1}$. Concluimos que p_n induce un isomorfismo $P_n/P_n\mathfrak{m}^{n-1} \cong P_n$ o, lo que es lo mismo, que el núcleo de p_n es $P_n\mathfrak{m}^{n-1}$.

Esto implica a su vez que el núcleo de la composición $P_n \longrightarrow P_{n-1} \longrightarrow P_{n-2}$ es $P_n\mathfrak{m}^{n-2}$ y, por lo tanto, el núcleo de $f_n = p_n \circ p_{n-1} \circ \cdots \circ p_1$ es $P_n\mathfrak{m}$, de modo que $P_n/P_n\mathfrak{m} \cong Q$.

Cada P_n es un $D_n[G]$-módulo, luego en particular es un D_n-módulo y, más en particular, un D-módulo. El hecho de que p_n sea un homomorfismo de $D_n[G]$-módulos implica en particular que es un homomorfismo de D-módulos, luego podemos considerar el D-módulo

$$P = \varprojlim_n P_n.$$

Vamos a probar que es un D-módulo libre de rango finito. Como P_n es un $D_n[G]$-módulo proyectivo finitamente generado, el teorema 4.12 implica que

también es un D_n-módulo proyectivo finitamente generado, y como D_n es un anillo (noetheriano) local, esto implica que P_n es un D_n-módulo libre[3] (de rango finito). Fijando una base de P_n obtenemos un isomorfismo $P_n \cong D_n^r$, y entonces

$$P_{n-1} \cong P_n/P_n\mathfrak{m}^{n-1} \cong (D_n/D_n\mathfrak{m}^{n-1})^r \cong D_{n-1}^r,$$

luego todos los módulos P_n tienen el mismo rango r como D_n-módulos. Más aún, los isomorfismos precedentes muestran que $p_n : P_n \longrightarrow P_{n-1}$ transforma cada D_n-base de P_n en una D_{n-1}-base de P_{n-1}. Más aún, toda base de P_{n-1} puede refinarse hasta una base de P_n. En efecto, si B_n es una D_n-base de P_n y B_{n-1} es su imagen en P_{n-1}, dada cualquier otra D_{n-1}-base B' de P_{n-1}, la matriz de cambio de base entre B_{n-1} y B' tiene determinante unitario en D_{n-1} (es decir, que no está en $D_{n-1}\mathfrak{m}$. Refinando la matriz hasta una matriz con coeficientes en D_n, su determinante tampoco estará en $D_n\mathfrak{m}$, luego define un cambio de base que transforma B_n en una D_n-base de P_n cuya imagen en P_{n-1} es la base B'.

De este modo, si $(v_1^1, \ldots, v_r^1)$ es una D_1-base de P_1, podemos tomar una D_2-base $(v_1^2, \ldots, v_r^2)$ de P_2 tal que $p_2(v_i^2) = v_i^1$, y de este modo podemos construir una sucesión $(v_1^n, \ldots, v_r^n)$ de bases de P_n que determina elementos $v_1, \ldots, v_r \in P$ que resultan ser una D-base de P. En efecto, dado $x \in P$, podemos expresar

$$x_n = d_1^n v_1^n + \cdots + d_r^n v_r^n,$$

para ciertos $d_i^n \in D_n$ unívocamente determinados. Aplicando p_n y teniendo en cuenta la unicidad, vemos que las sucesiones $\{d_i^n\}_n$ determinan elementos $d_i \in D$ —y aquí usamos el teorema anterior— tales que $x = d_1v_1 + \cdots + d_nv_n$. Esto prueba que $v_1, \ldots, v_n$ es un sistema generador de P, y similarmente se prueba que es libre.

El hecho de que los homomorfismos p_n sean homomorfismos de $D_n[G]$-módulos se traduce en que podemos definir una representación de G sobre D mediante $(x_n)\sigma = (x_n\sigma)$, para todo $x = (x_n) \in P$ y todo $\sigma \in G$. Equivalentemente, P tiene una estructura natural de $D[G]$-módulo. Los homomorfismos $f_n : P_n \longrightarrow Q$ conmutan con los p_n, por lo que definen un homomorfismo de $D[G]$-módulos $f : P \longrightarrow Q$. El hecho de que el núcleo de cada f_n sea $P_n\mathfrak{m}$ se traduce inmediatamente en que el núcleo de f es $P\mathfrak{m}$, de modo que $P/P\mathfrak{m} \cong Q$ es un $k[G]$-módulo proyectivo. El teorema 4.13 implica entonces que P es un $D[G]$-módulo proyectivo. (Notemos que el isomorfismo $P/P\mathfrak{m} \cong P \otimes_D k$ es consecuencia de que P es un D-módulo libre, como se observa justo antes del teorema 4.13.) Así pues, P es el $D[G]$-módulo buscado. ∎

Para extraer consecuencias de este teorema conviene introducir un nuevo grupo de Grothendieck:

Definición 4.21 Si D es un anillo y G es un grupo finito, llamaremos $P_D(G)$ al grupo de Grothendieck asociado a la categoría de los $D[G]$-módulos proyectivos finitamente generados.

[3]Por el teorema 5.47 de mi libro de *Álgebra conmutativa.*

En realidad (bajo las hipótesis de esta sección) $P_D(G)$ se identifica con $P_k(G)$ a través de la reducción módulo $\mathfrak{m}$:

Teorema 4.22 *El homomorfismo $P_D(G) \longrightarrow P_k(G)$ dado por $[P] \mapsto [P \otimes_D k]$ es un isomorfismo de grupos.*

DEMOSTRACIÓN: En primer lugar observamos que si

$$0 \longrightarrow P' \longrightarrow P \longrightarrow P'' \longrightarrow 0$$

es una sucesión exacta de $D[G]$-módulos proyectivos finitamente generados, entonces $P \cong P' \oplus P''$, luego

$$P \otimes_D k \cong (P' \otimes_D k) \oplus (P'' \otimes_D k),$$

luego, en $P_k(G)$, tenemos que $[P \otimes_D k] = [P' \otimes_D k] + [P'' \otimes_D k]$. Por lo tanto, la asignación $[P] \mapsto [P \otimes_D k]$ induce ciertamente un homomorfismo de grupos. Recíprocamente, si tenemos una sucesión exacta

$$0 \longrightarrow Q' \longrightarrow Q \longrightarrow Q'' \longrightarrow 0$$

de $k[G]$-módulos proyectivos finitamente generados, ha de ser $Q = Q' \oplus Q''$, luego, si $Q' \cong P' \otimes_D k$ y $Q'' \cong P'' \otimes_D k$, entonces $Q \cong (P' \oplus P'') \otimes_D k$, luego la correspondencia $Q \cong P \otimes_D k \mapsto [P]$ se extiende a un homomorfismo de grupos $P_k(G) \longrightarrow P_D(G)$ que cumple $[P \otimes_D k] \mapsto [P]$, por lo que es claramente el inverso del homomorfismo del enunciado. ∎

Teorema 4.23 *Si P y Q son dos $D[G]$-módulos proyectivos finitamente generados, entonces $P \cong Q$ si y sólo si $[P] = [Q]$ en $P_D(G)$.*

DEMOSTRACIÓN: Si $[P] = [Q]$, entonces, aplicando el isomorfismo del teorema anterior, $[P \otimes_D k] \cong [Q \otimes_D k]$ en $P_k(G)$, luego $P \otimes_D k \cong Q \otimes_D k$, por el teorema 4.4, luego $P \cong Q$, por la unicidad del teorema 4.20. ∎

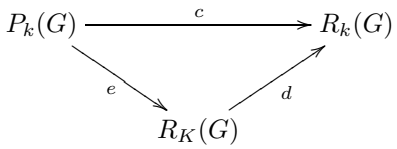
En las condiciones precedentes, si P es un $D[G]$-módulo proyectivo finitamente generado, entonces $P \otimes_D K$ es un $K[G]$-módulo finitamente generado con el producto dado por $(v \otimes \alpha)\sigma = (v\sigma) \otimes \alpha$, y es claro que existe un único homomorfismo de grupos $P_D(G) \longrightarrow R_K(G)$ determinado por que $[P] \mapsto [P \otimes_D K]$.

Definición 4.24 Definimos el homomorfismo $e : P_k(G) \longrightarrow R_K(G)$ como la composición del isomorfismo $P_k(G) \longrightarrow P_D(G)$ inverso del dado por el teorema 4.22 con el homomorfismo $P_D(G) \longrightarrow R_K(G)$ que acabamos de describir.

Explícitamente, e está determinado por que, para todo $D[G]$-módulo proyectivo finitamente generado P, se cumple que $e([P \otimes_D k]) = [P \otimes_D K]$.

En total, tenemos definidos tres homomorfismos entre grupos de Grothendieck, que dan lugar a un triángulo conmutativo:

Teorema 4.25 *El diagrama siguiente es conmutativo:*



DEMOSTRACIÓN: Basta comprobar que coinciden sobre un generador de $P_k(G)$ de la forma $[P \otimes_D k]$, donde P es un $D[G]$-módulo proyectivo finitamente generado. Tenemos que $e([P \otimes_D k]) = [P \otimes_D K]$. Ahora observamos que $P \otimes 1$ es un retículo estable en $P \otimes_D K$ isomorfo a P como D-módulo. Por consiguiente, $d(e([P \otimes_D k])) = [P \otimes_D k] = c([P \otimes_D k])$. ∎

Otra propiedad relevante es que los homomorfismos d y e son adjuntos respecto de las formas bilineales

$$\langle\ ,\ \rangle_K : R_K(G) \times R_K(G) \longrightarrow \mathbb{Z}, \qquad \langle\ ,\ \rangle_k : P_k(G) \times R_k(G) \longrightarrow \mathbb{Z}$$

definidas en 3.47 y 4.6:

Teorema 4.26 *Si $x \in P_k(G)$, $y \in R_K(G)$, entonces*

$$\langle x, d(y)\rangle_k = \langle e(x), y\rangle_K .$$

DEMOSTRACIÓN: Podemos tomar como x un generador de $P_k(G)$, de la forma $x = [P \otimes_D k]$, donde P es un $D[G]$-módulo proyectivo, así como que $y = [V]$, donde V es un $K[G]$-módulo finitamente generado. Podemos tomar un retículo estable R en V, con lo que $V \cong R \otimes_D K$. Equivalentemente, podemos suponer que $y = [R \otimes_D K]$, donde R es un $D[G]$-módulo finitamente generado que es libre como D-módulo.

Tenemos entonces que $e(x) = [P \otimes_D K]$, $d(y) = [R \otimes_D k]$, luego

$$\langle x, d(y)\rangle_k = \dim_k \mathrm{Hom}_G(P \otimes_D k, R \otimes_D k),$$

$$\langle x, e(y)\rangle_K = \dim_K \mathrm{Hom}_G(P \otimes_D K, R \otimes_D K).$$

Al ser proyectivo, P es un $K[G]$-submódulo de un $K[G]$-módulo libre (finitamente generado), que también será un D-módulo libre finitamente generado. Como D es un dominio de ideales principales, P es un D-módulo libre de rango finito. Es claro entonces que $\mathrm{Hom}_D(P, R)$ es también un D-módulo libre de rango finito, luego lo mismo vale para el D-submódulo $\mathrm{Hom}_G(P, R)$. Llamemos r a su rango. Ahora basta observar que, según el teorema 1.53, tenemos isomorfismos canónicos

$$\mathrm{Hom}_G(P, R) \otimes_D K \cong \mathrm{Hom}_G(P \otimes_D K, R \otimes_D K),$$

$$\mathrm{Hom}_G(P, R) \otimes_D k \cong \mathrm{Hom}_G(P \otimes_D k, R \otimes_D k).$$

Por consiguiente, $\langle x, d(y)\rangle_k = r = \langle e(x), y\rangle_K$. ∎

En las condiciones del teorema anterior, si K es un cuerpo suficientemente grande para G (y, por consiguiente, k también) tenemos que la matriz de la forma bilineal $\langle\ ,\ \rangle_K$ respecto de la base $S_K(G)$ es la identidad, al igual que la matriz de la forma bilineal $\langle\ ,\ \rangle_k$ respecto de las bases $I_k(G)$, $S_k(G)$ (por las observaciones posteriores al teorema 4.6). Por consiguiente, si llamamos D y E a las matrices de los homomorfismos d y e respecto de las bases correspondientes, el teorema anterior implica que $E = D^t$.

Así, si C es la matriz del homomorfismo de Cartan $c : P_k(G) \longrightarrow R_k(G)$ respecto de las bases $I_k(G)$, $S_k(G)$, tenemos que $C = D^t D$, lo que implica en particular que C es simétrica. Esto es un caso particular del teorema 4.10.

Cuando la característica del cuerpo de restos no divide al orden del grupo, la situación es trivial:

Teorema 4.27 *Sea K un cuerpo métrico discreto completo de característica 0 cuyo cuerpo de restos k tenga característica prima p, y sea G un grupo finito cuyo orden no sea divisible entre p. Entonces los homomorfismos c, d, e son isomorfismos.*

Demostración: Como $k[G]$ es semisimple, es claro que $P_k(G) = R_k(G)$ y que el homomorfismo c es la identidad. Como $e \circ d = c = 1$, tenemos que e es inyectivo y d suprayectivo. Esto implica a su vez que $R_K(G)$ es un $\mathbb{Z}$-módulo libre del mismo rango que $R_k(G)$.

Observemos que si $x \in R_k(G)$ cumple $d(e(x)) = 0$, entonces, por el teorema anterior,

$$\langle e(x), e(x)\rangle_K = \langle x, 0\rangle_k = 0,$$

y esto implica que $e(x) = 0$. Con esto hemos probado que $\operatorname{Im} e \cap \operatorname{N} d = 0$, y la inclusión $\operatorname{Im} e \oplus \operatorname{N} d \subset R_K(G)$ obliga entonces a que el núcleo de d sea nulo, ya que el rango de $\operatorname{Im} e$ es igual al de $R_K(G)$. Por consiguiente, d es un isomorfismo y e es su inverso. ∎

Si G es un grupo finito y p es un primo que no divida a su orden, ahora podemos concluir que la teoría de representaciones lineales de G sobre cuerpos de característica p es equivalente a la teoría de representaciones lineales de G sobre cuerpos de característica 0. Esto se debe a que todo cuerpo de característica prima k es isomorfo[4] al cuerpo de restos de un cuerpo métrico discreto completo de característica 0, y el teorema anterior nos da los isomorfismos

$$d : R_K(G) \longrightarrow R_k(G), \qquad e : R_k(G) \longrightarrow R_K(G).$$

Teniendo en cuenta además que las álgebras $k[G]$ y $K[G]$ son semisimples, esto significa que las representaciones lineales de G sobre K se corresponden biunívocamente de forma natural con las representaciones lineales de G sobre k.

El caso es más sencillo si nos restringimos a cuerpos de escisión, pues entonces las representaciones de G sobre cualquier cuerpo de escisión de característica 0 se

[4]Véase el teorema 2.15 de mi libro de *Superficies algebraicas,* que proporciona un anillo de valoración discreta de característica 0 con cuerpo de restos k. Basta tomar la compleción K de su cuerpo de cocientes.

corresponden biunívocamente de forma natural con las representaciones sobre el cuerpo local K que resulta de adjuntarle a $\mathbb{Q}_p$ las raíces de la unidad de orden igual al exponente de G, las cuales se corresponden a su vez con las representaciones de G sobre su cuerpo de restos k, que es un cuerpo finito de característica p suficientemente grande para G, luego las representaciones de G sobre k se corresponden biunívocamente de forma natural con las de cualquier cuerpo de escisión de G de característica p.

4.4 Algunos resultados técnicos

Dedicamos esta sección a probar algunos resultados generales que necesitamos para estudiar las propiedades de los homomorfismos c, d, e definidos en las secciones precedentes.

Restricción e inducción Si k es un cuerpo, G es un grupo finito y H es un subgrupo, cada $k[G]$-módulo es también un $k[H]$-módulo, y toda sucesión exacta de $k[G]$-módulos es también una sucesión exacta de $k[H]$-módulos, lo cual nos permite definir un homomorfismo de grupos $\mathrm{Res}^G_H : R_k(G) \longrightarrow R_k(H)$, determinado por que $\mathrm{Res}^G_H([V]) = [V]$.

Además, si V es un $k[G]$-módulo proyectivo, entonces es un sumando directo de un $k[G]$-módulo libre, el cual es también un $k[H]$-módulo libre (porque $k[G]$ es un $k[H]$-módulo libre), luego V también es un $k[H]$-módulo proyectivo. Esto nos permite definir también un homomorfismo de grupos $\mathrm{Res}^G_H : P_k(G) \longrightarrow P_k(H)$.

Por otra parte, si V es un $k[H]$-módulo finitamente generado, entonces $V \otimes_{k[H]} k[G]$ es un $k[G]$-módulo finitamente generado y, como $k[G]$ es libre sobre $k[H]$ (en particular, proyectivo) al multiplicar por $\otimes_{k[H]} k[G]$ una sucesión exacta de $k[H]$-módulos, obtenemos una sucesión exacta de $k[G]$-módulos. Esto implica que podemos definir un homomorfismo de grupos $\mathrm{Ind}^G_H : R_k(H) \longrightarrow R_k(G)$ dado por $\mathrm{Ind}^G_H([V]) = [V \otimes_{k[H]} k[G]]$.

Similarmente a lo que sucede con la restricción, si V es un $k[H]$-módulo proyectivo, entonces es sumando directo de un $k[H]$-módulo libre L, luego $V \otimes_{k[H]} k[G]$ es un sumando directo de $L \otimes_{k[H]} k[G]$, que es un $k[G]$-módulo libre, luego $V \otimes_{k[H]} k[G]$ es un $k[G]$-módulo proyectivo, y esto nos permite definir un homomorfismo de grupos $\mathrm{Ind}^G_H : P_k(H) \longrightarrow P_k(G)$.

Entre la restricción y la inducción se da la relación siguiente:

Teorema 4.28 *Si G es un grupo finito, H es un subgrupo y k es un cuerpo, se cumple la relación*

$$\mathrm{Ind}^G_H(x \cdot \mathrm{Res}^G_H y) = \mathrm{Ind}^G_H(x) \cdot y$$

para todo $x \in R_k(H)$, $y \in R_k(G)$, en cuyo caso ambos miembros están en $R_k(G)$, y también para todo $x \in R_k(H)$, $y \in P_k(G)$, en cuyo caso la identidad se da en $P_k(G)$.

DEMOSTRACIÓN: Por linealidad, basta probarlo cuando $x = [V]$, donde V es un $k[H]$-módulo finitamente generado, e $y = [W]$, donde W es un $k[G]$-módulo (proyectivo) finitamente generado. Basta probar el isomorfismo

$$(V \otimes_k W) \otimes_{k[H]} k[G] \cong (V \otimes_{k[H]} k[G]) \otimes_k W.$$

Para ello consideramos el homomorfismo $\phi : V \otimes_k W \longrightarrow (V \otimes_{k[H]} k[G]) \otimes_k W$ dado por $\phi(v \otimes w) = (v \otimes 1) \otimes w$, que es un homomorfismo de $k[H]$-módulos, a partir del cual definimos $\psi : (V \otimes_k W) \otimes_{k[H]} k[G] \longrightarrow (V \otimes_{k[H]} k[G]) \otimes_k W$ mediante $\psi(u \otimes v) = \phi(u)v$, que es un isomorfismo porque una k-base del primer espacio está formada por los elementos de la forma $v_i \otimes w_j \otimes \sigma_l$, donde v_i recorre una k-base de V, w_j recorre una k-base de W y σ_l recorre un sistema de representantes de las clases a derecha de G/H, y ψ transforma esta base en la k-base $v_i \otimes \sigma_l \otimes w_j$ del espacio de la derecha. ∎

También se cumple que las inducciones y las restricciones conmutan con los homomorfismos c, d, e definidos en las secciones precedentes. Sólo vamos a necesitar el caso de la inducción y los homomorfismos d y e:

Teorema 4.29 *Sea G un grupo finito, H un subgrupo, D un anillo de valoración discreta de característica 0, sea K su cuerpo de cocientes y k su cuerpo de restos. El diagrama siguiente es conmutativo:*

$$\begin{array}{ccc} R_K(G) & \xrightarrow{d} & R_k(G) \\ {\scriptstyle \mathrm{Ind}}\uparrow & & \uparrow{\scriptstyle \mathrm{Ind}} \\ R_K(H) & \xrightarrow[d]{} & R_k(H) \end{array}$$

DEMOSTRACIÓN: Basta probar que ambas composiciones coinciden sobre un elemento de la forma $[V] \in R_K(H)$, donde V es un $K[H]$-módulo finitamente generado. Tomamos un retículo estable R en V, de modo que $d([V]) = [R \otimes_D k]$.

Por otra parte, $\mathrm{Ind}_H^G([V]) = [V \otimes_{K[H]} K[G]]$. Si $\sigma_1, \ldots, \sigma_r$ es un sistema de representantes de las clases a derecha de G/H (es decir, una $K[H]$-base de $K[G]$), entonces

$$V \otimes_{K[H]} K[G] = \bigoplus_i V \otimes \sigma_i,$$

de donde se sigue que

$$R \otimes_{D[H]} D[G] = \bigoplus_i R \otimes \sigma_i$$

es un retículo estable en $V \otimes_{K[H]} K[G]$. Así pues, todo se reduce a probar que

$$(R \otimes_{D[H]} D[G]) \otimes_D k \cong (R \otimes_D k) \otimes_{k[H]} k[G].$$

En efecto:

$$(R \otimes_D k) \otimes_{k[H]} k[G] \cong (R \otimes_{D[H]} D[H] \otimes_D k) \otimes_{k[H]} k[G]$$
$$\cong R \otimes_{D[H]} k[H] \otimes_{k[H]} k[G] \cong R \otimes_{D[H]} k[G] \cong R \otimes_{D[H]} (D[G] \otimes_D k)$$
$$\cong (R \otimes_{D[H]} D[G]) \otimes_D k.$$

∎

Teorema 4.30 *Sea G un grupo finito, H un subgrupo, D un anillo de valoración discreta de característica 0, sea K su cuerpo de cocientes y k su cuerpo de restos. El diagrama siguiente es conmutativo:*

$$\begin{array}{ccc} P_k(G) & \xrightarrow{e} & R_K(G) \\ {\scriptstyle \mathrm{Ind}}\uparrow & & \uparrow{\scriptstyle \mathrm{Ind}} \\ P_k(H) & \xrightarrow[e]{} & R_K(H) \end{array}$$

Demostración: Tenemos que $P_k(H)$ está generado por los elementos de la forma $x = [V \otimes_D k]$, donde V es un $D[H]$-módulo proyectivo finitamente generado.

$$\mathrm{Ind}_H^G(x) = [(V \otimes_D k) \otimes_{k[H]} k[G]] = [V \otimes_{D[H]} k[H] \otimes_{k[H]} k[G]]$$

$$= [V \otimes_{D[H]} k[G]] = [(V \otimes_{D[H]} D[G]) \otimes_D k],$$

donde $V \otimes_{D[H]} D[G]$ es un $D[G]$-módulo proyectivo finitamente generado. Por consiguiente,

$$e(\mathrm{Ind}_H^G(x)) = [V \otimes_{D[H]} D[G] \otimes_D K] = [V \otimes_{D[H]} K[G]].$$

Por otra parte:

$$\mathrm{Ind}_H^G(e(x)) = [(V \otimes_D K) \otimes_{K[H]} K[G]]$$

$$= [V \otimes_{D[H]} K[H] \otimes_{K[H]} K[G]] = [V \otimes_{D[H]} K[G]].$$

■

Vamos a demostrar ahora una versión abstracta del teorema de Brauer 2.41. Para ello, consideramos el conjunto X de todos los subgrupos elementales de G (definición 2.42), así como los homomorfismos de grupos

$$\mathrm{Ind} : \bigoplus_{H\in X} R_k(H) \longrightarrow R_k(G), \qquad \mathrm{Ind} : \bigoplus_{H\in X} P_k(H) \longrightarrow P_k(G)$$

determinados por los homomorfismos Ind_H^G.

Teorema 4.31 *Sea G un grupo finito y k un cuerpo suficientemente grande para G. Entonces, los homomorfismos*

$$\mathrm{Ind} : \bigoplus_{H\in X} R_k(H) \longrightarrow R_k(G), \qquad \mathrm{Ind} : \bigoplus_{H\in X} P_k(H) \longrightarrow P_k(G)$$

donde X es el conjunto de los subgrupos elementales de G, son suprayectivos.

Demostración: Observemos en primer lugar que si $k_0 \subset k_1$ son dos cuerpos suficientemente grandes para G, entonces el teorema es cierto para k_0 si y sólo si lo es para k_1. En efecto, es claro que también son suficientemente grandes

para todos los subgrupos de G, luego son cuerpos de escisión para todos ellos. Tenemos entonces diagramas conmutativos

$$\begin{array}{ccc} R_{k_1}(H) & \xrightarrow{\mathrm{Ind}_H^G} & R_{k_1}(G) \\ \uparrow & & \uparrow \\ R_{k_0}(H) & \xrightarrow[\mathrm{Ind}_H^G]{} & R_{k_1}(G) \end{array}$$

donde las flechas verticales son los isomorfismos dados por el teorema 3.49. Para ello basta observar que si V es un $k_0[H]$-módulo, la imagen de $[V]$ por cada camino del diagrama es la asociada a los $k_1[G]$-módulos

$$(V \otimes_{k_0} k_1) \otimes_{k_1[H]} k_1[G] \cong (V \otimes_{k_0[H]} k_0[H] \otimes k_1) \otimes_{k_1[H]} k_1[G]$$

$$\cong V \otimes_{k_0[H]} k_1[H] \otimes_{k_1[H]} k_1[G] \cong V \otimes_{k_0[H]} k_1[G]$$

y

$$(V \otimes_{k_0[H]} k_0[G]) \otimes_{k_0} k_1 \cong V \otimes_{k_0[H]} (k_0[G] \otimes_{k_0} k_1) \cong V \otimes_{k_0[H]} k_1[G].$$

Los diagramas conmutativos para cada subgrupo H dan lugar a un diagrama conmutativo

$$\begin{array}{ccc} \bigoplus_{H\in X} R_{k_1}(H) & \xrightarrow{\mathrm{Ind}} & R_{k_1}(G) \\ \uparrow & & \uparrow \\ \bigoplus_{H\in X} R_{k_0}(H) & \xrightarrow[\mathrm{Ind}]{} & R_{k_0}(G) \end{array}$$

donde las flechas verticales son isomorfismos. Concluimos que una flecha horizontal es suprayectiva si y sólo si lo es la otra. Todo el razonamiento es válido igualmente si cambiamos $R_k(G)$ por $P_k(G)$.

Ahora observamos que, cuando $k = \mathbb{C}$, el teorema es consecuencia inmediata del teorema 2.45, sin más que tener en cuenta que, a través del isomorfismo 3.57, el subgrupo V_p considerado en 2.45 se identifica con la imagen de la restricción de Ind a la suma directa de los grupos $R_k(H)$, donde H es p-elemental. Concluimos entonces que la imagen de Ind es un subgrupo de $R_k(G)$ cuyo índice es finito, pero no es divisible entre ningún primo. (Notemos que, para cuerpos de característica 0, se cumple que $R_k(G) = P_k(G)$, luego no hemos de preocuparnos del segundo homomorfismo del enunciado.)

De aquí obtenemos que el teorema es cierto para el cuerpo $k_0 \subset \mathbb{C}$ que resulta de adjuntar a $\mathbb{Q}$ las raíces m-simas de la unidad, donde m es el exponente de G, y esto a su vez implica que el teorema también se cumple para todo cuerpo de característica 0 suficientemente grande para G (pues todo cuerpo suficientemente grande para G de característica 0 contiene a k_0).

Similarmente, para probar el teorema sobre cuerpos de característica prima p basta probarlo para el cuerpo k que resulta de adjuntar a $\mathbb{Z}/p\mathbb{Z}$ las raíces

m-simas de la unidad. Si llamamos K a la adjunción de las raíces m-simas de la unidad al cuerpo $\mathbb{Q}_p$ de los números p-ádicos, es claro que k es el cuerpo de restos de K y, como K tiene característica 0, el teorema se cumple para K.

Sea 1_K (resp. 1_k) la identidad del anillo $R_K(G)$ (resp. $R_k(G)$). Concretamente, $1_K = [K]$, donde consideramos a K como $K[G]$-módulo trivial y, análogamente, $1_k = [k]$. Es claro que $d(1_K) = 1_k$. Por la parte ya probada sabemos que

$$1_K = \sum_{H\in X} \mathrm{Ind}_H^G(x_H),$$

para ciertos $x_H \in R_K(H)$. Aplicando d y teniendo en cuenta el teorema 4.29, obtenemos que

$$1_k = \sum_{H\in X} \mathrm{Ind}_H^G(x'_H),$$

donde $x'_H = d(x_H) \in R_k(H)$. Para cada $y \in R_k(G)$ (resp. $P_k(G)$), tenemos que

$$y = 1_k \cdot y = \sum_{H\in X} \mathrm{Ind}_H^G(x'_H \cdot \mathrm{Res}_H^G(y)),$$

y esto completa la prueba. ∎

Extensiones de coeficientes Vamos a necesitar el análogo del teorema 3.49 para los anillos $P_k(G)$ y un hecho adicional para cuerpos de característica prima:

Teorema 4.32 *Si K/k es una extensión de cuerpos y G es un grupo finito, el homomorfismo $P_k(G) \longrightarrow P_K(G)$ dado por $[P] \mapsto [P \otimes_k K]$ es inyectivo. Además, identificando a $P_k(G)$ con un subgrupo de $P_K(G)$ a través de este monomorfismo:*

a) Si los cuerpos tienen característica prima, entonces $P_k(G)$ es un sumando directo de $P_K(G)$.

b) Si k es un cuerpo de escisión de G, entonces $P_k(G) = P_K(G)$.

Demostración: Es evidente que, si P es un $k[G]$-módulo proyectivo, entonces $P \otimes_k K$ es un $K[G]$-módulo proyectivo, así como que la asignación $P \mapsto P \otimes_k K$ induce un homomorfismo entre los grupos de Grothendieck.

Para probar que es inyectivo, no perdemos generalidad si suponemos que K es un cuerpo de escisión de G, pues siempre podemos tomar una extensión L/K tal que L lo sea, y la inyectividad del homomorfismo $P_k(G) \longrightarrow P_L(G)$ implica la inyectividad del correspondiente a K.

Si V es un $k[G]$-módulo simple y P_V es su envoltura proyectiva, tenemos una sucesión exacta

$$0 \longrightarrow P_V J(k[G]) \longrightarrow P_V \longrightarrow V \longrightarrow 0,$$

la cual, teniendo en cuenta el teorema 3.67, da lugar a una sucesión exacta

$$0 \longrightarrow (P_V \otimes_k K)J(K[G]) \longrightarrow P_V \otimes_k K \longrightarrow V \otimes_k K \longrightarrow 0.$$

Esto implica que $P_V \otimes_k K$ es la envoltura proyectiva de $V \otimes_k K$, que es un $K[G]$-módulo semisimple por el teorema 3.65. De este modo, si $V_1, \dots, V_h$ son representantes de las clases de isomorfía de $k[G]$-módulos simples, tenemos que $I_k(G) = \{[P_{V_1}], \dots, [P_{V_h}]\}$ es una base de $P_k(G)$ y su imagen en $P_K(G)$ está formada por los elementos $[P_{V_i \otimes_k K}]$, cada uno de los cuales se expresa como combinación lineal de un subconjunto $S_i \subset I_K(G)$, concretamente, según el teorema 4.3, tenemos que S_i está formado por los elementos $[P_W]$, donde W recorre los factores de composición de $V_i \otimes_k K$. Ahora bien, el teorema 3.38 implica que los módulos $V_i \otimes_k K$ no tienen factores de composición en común, luego los conjuntos S_i son disjuntos dos a dos, y esto implica que el homomorfismo del enunciado es inyectivo.

a) Si los cuerpos tienen característica prima, el teorema 3.65 nos da que cada $W \in S_i$ tiene multiplicidad 1 como factor de composición de $V_i \otimes_k K$, luego la imagen de $[P_{V_i}]$ es simplemente la suma de los elementos de S_i. Es claro entonces que $P_k(G)$ está complementado en $P_K(G)$. Un complemento es, por ejemplo, el subgrupo generado por todos los elementos de la base $I_K(G)$ menos uno elegido arbitrariamente en cada conjunto S_i.

b) Si k es un cuerpo de escisión de G, los $K[G]$-módulos $V_i \otimes_k K$ son simples, luego concluimos que el homomorfismo del enunciado biyecta $I_k(G)$ con $I_K(G)$. ∎

Restricciones de coeficientes Si K/k es una extensión finita de cuerpos y G es un grupo finito, cada $K[G]$-módulo V tiene una estructura natural de $k[G]$-módulo. Usaremos la notación V_k para referirnos a V como $k[G]$-módulo. Como toda sucesión exacta de $K[G]$-módulos es también una sucesión exacta de $k[G]$-módulos, podemos definir un homomorfismo de grupos $\pi : R_K(G) \longrightarrow R_k(G)$ mediante $\pi([V]) = [V_k]$. Vamos a estudiarlo en el caso en el que los cuerpos tienen característica 0. Puesto que cada elemento de $R_K(G)$ y $R_k(G)$ está determinado por su carácter virtual asociado (teorema 3.50), basta determinar el carácter virtual de $\pi(x)$ en función del carácter virtual de x.

Teorema 4.33 *Sea K/k una extensión finita de cuerpos de característica 0, sea G un grupo finito y sea $\pi : R_K(G) \longrightarrow R_k(G)$ la restricción de coeficientes que acabamos de definir. Si un elemento $x \in R_K(G)$ tiene asociado el carácter virtual $\chi : G \longrightarrow K$, entonces el carácter virtual de $\pi(x)$ es $\chi \circ \mathrm{Tr}_k^K$, donde $\mathrm{Tr}_k^K : K \longrightarrow k$ es la traza de la extensión.*

Demostración: Basta probar que el diagrama siguiente es conmutativo:

$$\begin{array}{ccc} R_K(G) & \xrightarrow{\chi} & R'_K(G) \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi'} \\ R_k(G) & \xrightarrow[\chi]{} & R'_k(G) \end{array}$$

donde las flechas horizontales son los isomorfismos $x \mapsto \chi_x$ que a cada elemento del grupo de Grothendieck respectivo le asignan su carácter virtual, y la flecha vertical derecha viene dada por $\pi'(f) = f \circ \mathrm{Tr}_k^K$.

Como las cuatro flechas son homomorfismos de grupos, basta ver que coinciden sobre un generador de $R_K(G)$, es decir, sobre un elemento de la forma $[V]$, donde V es un $K[G]$-módulo simple. En primer lugar supondremos que la extensión K/k es finita de Galois.

Según el teorema 3.64, sabemos que $\pi([V]) = n[W]$, para cierto natural $n \geq 1$, donde W es el único $k[G]$-módulo simple tal que W_K tiene a V como factor de composición. Según 3.65, los caracteres de los factores de composición de W_K son los conjugados del carácter χ de V por los automorfismos de la extensión $k(\chi)/k$, y todos aparecen con la misma multiplicidad m. Así pues, el carácter de $\pi([V])$ es $nm(\chi_1 + \cdots + \chi_h)$, donde $h = |k(\chi)/k|$. Ahora bien, si $\dim_K V = d$, entonces $\dim_k V_k = d|K : k|$, luego, evaluando los caracteres en 1, obtenemos la igualdad $d|K : k| = nmhd$, y de aquí que $|K : k(\chi)| = nm$.

A través de la restricción $G(K/k) \longrightarrow G(k(\chi)/k)$, cada automorfismo de $k(\chi)/k$ tiene nm antiimágenes, luego, si en lugar de aplicarle a χ los automorfismos de $k(\chi)/k$ le aplicamos todos los automorfismos de K/k, cada conjugado χ_i aparecerá nm veces, luego podemos afirmar que el carácter de $\pi([V])$ es

$$\sum_{\sigma \in G(K/k)} \chi^\sigma = \chi \circ \mathrm{Tr}_k^K .$$

Esto prueba el teorema para extensiones de Galois. En el caso general, tomamos una extensión $k \subset K \subset L$ de modo que L/k (y, por consiguiente, también L/K) sea finita de Galois. Dado $x \in R_K(G)$, sea $x_L \in R_L(G)$ el elemento obtenido por extensión de coeficientes, que tiene el mismo carácter virtual χ. Por la parte ya probada, el carácter virtual de $\pi_K^L(x_L)$ es

$$\chi \circ \mathrm{Tr}_K^L = |L : K|\chi,$$

puesto que χ toma valores en K. Por consiguiente, $\pi_K^L(x_L) = |L : K|x$. Por otra parte, es claro que $\pi_k^L = \pi_K^L \circ \pi_k^K$, luego

$$\pi_k^L(x_L) = |L : K|\pi_k^K(x).$$

Aplicando de nuevo la parte ya probada, vemos que el carácter virtual del miembro izquierdo es

$$\chi \circ \mathrm{Tr}_k^L = \chi \circ \mathrm{Tr}_K^L \circ \mathrm{Tr}_k^K = |L : K|(\chi \circ \mathrm{Tr}_k^K),$$

de donde concluimos que el carácter virtual de $\pi_k^K(x)$ es $\chi \circ \mathrm{Tr}_k^K$, como queríamos probar. ∎

Observemos que si, en las condiciones del teorema anterior, el carácter virtual de x toma valores en k, entonces el carácter virtual de $\pi(x)$ es $|K : k|\chi$, luego $\pi(x) = |K : k|x$ (donde identificamos $\pi(x) \in R_k(G)$ con su extensión de coeficientes en $R_K(G)$).

Productos de p-grupos y p′-grupos Consideramos ahora un cuerpo k de característica prima p y un grupo finito de la forma $G = H \times P$, donde P es un p-grupo y H es un grupo de orden no divisible entre p.

En primer lugar observamos que $k[G] \cong k[H] \otimes_k k[P]$. El isomorfismo como k-espacios vectoriales es inmediato y, además, teniendo en cuenta que los elementos de P conmutan con los de H, es claro que también es un isomorfismo de k-álgebras.

> *Un $k[G]$-módulo finitamente generado V es proyectivo si y sólo si es isomorfo a $W \otimes_k k[P]$, donde W es un $k[H]$-módulo finitamente generado.*

En efecto, dado W, como $k[H]$ es semisimple, tenemos que W es un $k[H]$-módulo proyectivo, de donde se sigue que $W \otimes_k k[P]$ es un $k[G]$-módulo proyectivo. (Si W es sumando directo de un $k[H]$-módulo libre L, entonces $W \otimes_k k[P]$ es sumando directo de $L \otimes_k k[P]$, que es un $k[G]$-módulo libre debido al isomorfismo $k[H] \otimes_k k[P] \cong k[G]$.)

Ahora vamos a probar que $W \otimes_k k[P]$ es la envoltura proyectiva de W considerado como $k[G]$-módulo (de modo que P actúa trivialmente sobre él). Esto implica el recíproco, pues todo $k[G]$-módulo proyectivo es la envoltura proyectiva de un $k[G]$-módulo semisimple W (sobre el que P actúa trivialmente, por el teorema 3.51, luego W es también un $k[H]$-módulo), luego ha de ser isomorfo a $W \otimes_k k[P]$.

Tenemos ciertamente un epimorfismo de $k[G]$-módulos $W \otimes_k k[P] \longrightarrow W$ dado por $w \otimes \sigma \mapsto w$. Hemos de probar que es esencial o, equivalentemente, que su núcleo está contenido en $N = (W \otimes_k k[P])J(k[G])$. Sea $V = (W \otimes_k k[P])/N$, que es un $k[G]$-módulo semisimple, luego P actúa trivialmente sobre él, de nuevo por 3.51. Esto hace que la aplicación $W \longrightarrow V$ dada por $w \mapsto [w \otimes 1]$ sea un homomorfismo de $k[G]$-módulos que hace conmutativo el diagrama

$$\begin{array}{ccc} W \otimes_k k[P] & \longrightarrow & W \\ & \searrow & \downarrow \\ & & V \end{array}$$

(La clave es que $[w \otimes \pi] = [w \otimes 1]\pi = [w \otimes 1]$.) Es claro entonces que el núcleo de la flecha horizontal está contenido en el núcleo de la oblicua, que es N. ∎

Teorema 4.34 *Sea K un cuerpo métrico discreto completo de característica 0, sea D su anillo de enteros y k su cuerpo de restos, de característica prima p. Sea $G = H \times P$ un grupo finito, donde P es un p-grupo y H un grupo de orden no divisible entre p. Un $D[G]$-módulo finitamente generado V es proyectivo si y sólo si es isomorfo a $W \otimes_D D[P]$, donde W es un $D[H]$-módulo finitamente generado y libre como D-módulo.*

DEMOSTRACIÓN: El teorema 4.13 nos da que un $D[H]$-módulo W en las condiciones del enunciado es proyectivo, pues todos los $k[H]$-módulos finitamente generados son proyectivos. Nuevamente tenemos que $D[G] = D[H] \otimes_D D[P]$, de donde se sigue todo $D[G]$-módulo de la forma $W \otimes_D D[P]$ es proyectivo (por el mismo argumento empleado antes con $k[G]$-módulos).

Si V es un $D[G]$-módulo proyectivo finitamente generado, entonces $V \otimes_D k$ es un $k[G]$-módulo proyectivo finitamente generado y, por 4.13, es de la forma $V \otimes_D k \cong W_0 \otimes_k k[P]$, donde W_0 es un $k[H]$-módulo finitamente generado. Como todo $k[H]$-módulo es proyectivo, el teorema 4.20 nos da que existe un $D[H]$-módulo proyectivo finitamente generado W tal que $W_0 \cong W \otimes_D k$. Notemos que W también es proyectivo sobre D y, como D es local, W es un D-módulo libre. Ahora observamos que

$$(W \otimes_D D[P]) \otimes_D k \cong (W \otimes_D k) \otimes_k (D[P] \otimes_D k) \cong W_0 \otimes_k k[P] \cong V \otimes_D k,$$

luego $W \otimes_D D[P] \cong V$ por el teorema 4.13. ∎

4.5 Propiedades de los homomorfismos c, d, e

A lo largo de esta sección K será un cuerpo local, es decir, una extensión finita de un cuerpo de números p-ádicos $\mathbb{Q}_p$. Llamaremos D a su anillo de enteros y k a su cuerpo de restos (que es un cuerpo finito de característica p).

Teorema 4.35 *Si G es un grupo finito y K es suficientemente grande*[5] *para G, el homomorfismo $d : R_K(G) \longrightarrow R_k(G)$ es suprayectivo.*

DEMOSTRACIÓN: Por el teorema 4.31 sólo hemos de probar que los elementos de $R_k(G)$ inducidos desde un subgrupo q-elemental H de G tienen antiimagen por d. Como d conmuta con la inducción, no perdemos generalidad si suponemos que G es q-elemental, es decir, que $G = Q \times C$, donde Q es un q-grupo y C es un subgrupo cíclico de orden primo con q.

Si $p \neq q$, podemos descomponer $C = P \times C_0$, donde P es un p-grupo y C_0 es un grupo de orden primo con p. Si $q = p$ llamamos $P = Q$ y así, en ambos casos, podemos descomponer $G = P \times H$, donde P es un p-grupo y H es un grupo de orden primo con p.

Basta probar que si V es un $k[G]$-módulo simple, entonces $[V] \in R_k(G)$ tiene una antiimagen por d. El teorema 3.51 nos da que P actúa trivialmente sobre V, lo cual nos permite considerar a V como $k[H]$-módulo simple. Basta encontrar un $K[H]$-módulo W tal que $d([W]) = [V]$ en $R_k(H)$, pues entonces tenemos la misma igualdad en $R_K(G)$ sin más que considerar a W como $K[G]$-módulo. Equivalentemente (cambiando G por H), podemos suponer que p no divide al orden de G. En tal caso $k[G]$ es semisimple, luego $P_k(G) = R_k(G)$ y el homomorfismo de Cartan c es la identidad. Puesto que $e \circ d = c$, es claro que

[5]Esta hipótesis no es necesaria en realidad, pero para probar el teorema sin ella necesitaríamos una versión más general del teorema de Brauer.

d es suprayectiva. (De hecho, sabemos que es un isomorfismo por el teorema 4.27.) ∎

Teorema 4.36 *El homomorfismo $e : P_k(G) \longrightarrow R_K(G)$ es inyectivo.*

DEMOSTRACIÓN: Supongamos en primer lugar que K es suficientemente grande. Si $x \in P_k(G)$ cumple que $e(x) = 0$, el teorema 4.26 nos da que

$$\langle x, d(y)\rangle_k = \langle e(x), y\rangle_K = 0$$

para todo $y \in R_K(G)$. Como d es suprayectivo, esto implica que $\langle x, z\rangle_k = 0$ para todo $z \in R_k(G)$, lo cual implica que $x = 0$.

En el caso general, sea K'/K una extensión finita de cuerpos locales tal que K' sea suficientemente grande. Es fácil ver que tenemos un diagrama conmutativo

$$\begin{array}{ccc} P_{k'}(G) & \xrightarrow{e'} & R_{K'}(G) \\ \uparrow & & \uparrow \\ P_k(G) & \xrightarrow[e]{} & R_K(G) \end{array}$$

en el que las flechas verticales son los monomorfismos del teorema 3.49. La inyectividad de e' implica la de e. ∎

Explícitamente, el teorema anterior afirma lo siguiente:

Teorema 4.37 *Si P y P' son $D[G]$-módulos proyectivos finitamente generados y $P \otimes_D K \cong P' \otimes_D K$, entonces $P \cong P'$.*

DEMOSTRACIÓN: En efecto, tenemos que $e([P \otimes_D k]) = e([P' \otimes_D k])$, luego $[P \otimes_D k] = [P' \otimes_D k]$, luego $P \otimes_D k \cong P' \otimes_D k$ por el teorema 4.4, luego $P \cong P'$ por 4.13. ∎

Teorema 4.38 *El homomorfismo $c : P_k(G) \longrightarrow R_k(G)$ es inyectivo.*

DEMOSTRACIÓN: Si K es suficientemente grande y $x \in P_k(G)$ cumple que $c(x) = 0$, entonces $d(e(x)) = 0$, luego

$$\langle e(x), e(x)\rangle_K = \langle x, d(e(x))\rangle_k = 0,$$

luego $e(x) = 0$, luego $x = 0$. En el caso general consideramos una extensión K'/K de cuerpos locales tal que K' sea suficientemente grande y formamos el diagrama conmutativo

$$\begin{array}{ccc} P_{k'}(G) & \xrightarrow{c'} & R_{k'}(G) \\ \uparrow & & \uparrow \\ P_k(G) & \xrightarrow[c]{} & R_k(G) \end{array}$$

donde las flechas verticales son monomorfismos por el teorema 4.32. Así pues, la inyectividad de c' implica la de c. ∎

Equivalentemente:

Teorema 4.39 *Si dos $k[G]$-módulos proyectivos tienen los mismos factores de composición (contando sus multiplicidades), entonces son isomorfos.*

Ahora vamos a dar una caracterización de la imagen del homomorfismo e en $R_K(G)$. Recordemos que, según el teorema 3.50, el anillo $R_K(G)$ es isomorfo al anillo $R'_K(G)$ de los caracteres virtuales de G sobre K.

Teorema 4.40 *La imagen del homomorfismo $e : P_k(G) \longrightarrow R_K(G)$ está formada por los elementos de $R_K(G)$ cuyo carácter virtual asociado se anula sobre los elementos p-singulares de G (es decir, de orden divisible entre p).*

Por razones técnicas, demostraremos un resultado ligeramente más general:

Teorema 4.41 *Sea K'/K una extensión finita. Para que un elemento de $R_{K'}(G)$ esté en la imagen del homomorfismo $e : P_k(G) \longrightarrow R_K(G) \subset R_{K'}(G)$ es necesario y suficiente que su carácter virtual tome valores en K y se anule sobre los elementos p-singulares de G.*

Demostración: El carácter virtual de un elemento de $R_K(G)$ es el mismo que el de su imagen en $R_{K'}(G)$, luego no perdemos generalidad si suponemos que K' es suficientemente grande para G y que la extensión K'/K es de Galois.

El anillo $P_k(G)$ está generado por los elementos de la forma $[V \otimes_D k]$, donde V es un $D[G]$-módulo proyectivo finitamente generado. Su imagen por e es $[V \otimes_D K]$ y, vista como elemento de $R_{K'}(G)$, es $[V \otimes_D K']$. Llamemos χ al carácter asociado a $V \otimes_D K'$, que es el mismo asociado a $V \otimes_D K$, luego es una aplicación $\chi : G \longrightarrow K$. Hemos de probar que si $\sigma \in G$ es p-singular, entonces $\chi(\sigma) = 0$. Si llamamos G_0 al subgrupo generado por σ, entonces V es también un $D[G_0]$-módulo proyectivo finitamente generado, y el carácter asociado a $V \otimes_D K$ como $K[G_0]$-módulo es $\chi|_{G_0}$, luego, cambiando G por G_0, podemos suponer que G es cíclico.

Descompongamos $G = H \times P$, donde P es un p-grupo y H es un grupo de orden no divisible entre p. El teorema 4.34 nos da que $V \cong W \otimes_D D[P]$, donde W es un $D[G]$-módulo proyectivo finitamente generado. Por consiguiente, $V \otimes_D K \cong (W \otimes_D K) \otimes_K K[P]$, luego $\chi = \psi r$, donde ψ es un carácter de H y r es el carácter regular de P (extendidos ambos a G de forma natural). Como σ es p-singular, su descomposición $\sigma = \tau\pi$, con $\tau \in H$, $\pi \in P$, cumple $\pi \neq 1$, luego $\chi(\sigma) = 0$ (pues $r(\pi) = 0$).

Tomemos ahora un elemento $y \in R_{K'}(G)$ tal que su carácter virtual asociado χ se anule sobre los elementos p-singulares de G. Vamos a probar que y está en la imagen del homomorfismo $e' : P_{k'}(G) \longrightarrow R_{K'}(G)$.

Por el teorema 4.31 podemos expresar

$$1_{K'} = \sum \mathrm{Ind}_H^G(x_H),$$

donde $x_H \in R_{K'}(H)$ y H recorre el conjunto de los subgrupos elementales de G. Multiplicando por y, el teorema 4.28 nos da que

$$y = \sum \mathrm{Ind}_H^G(y_H), \qquad y_H = x_H \cdot \mathrm{Res}_H^G(y).$$

Vemos así que, al expresar y como suma de elementos y_H inducidos desde subgrupos elementales de G, éstos conservan la propiedad de que su carácter virtual asociado en $R'_{K'}(H)$ se anula en los elementos p-singulares de H. Si probamos que cada y_H está en la imagen de e'_H, el teorema 4.30 nos dará que y está en la imagen de e'. Así pues, no perdemos generalidad si suponemos que G es elemental. Esto, a su vez, nos permite descomponerlo como $G = H \times P$, donde P es un p-grupo y H es un grupo de orden no divisible entre p.

Como χ se anula fuera de H, podemos expresarlo como $\chi = fr$, donde $f \in F(H)$ y r es el carácter regular de P (ambos extendidos a G de forma natural). Si ψ un carácter irreducible de H sobre K', tenemos que

$$\langle f, \psi\rangle = \langle f, \psi\rangle \langle r, 1_P\rangle = \langle \chi, \psi\rangle \in \mathbb{Z}.$$

Este valor es el coeficiente de ψ en la expresión de f como combinación lineal de los caracteres irreducibles de H. Como todas las coordenadas son enteras, concluimos que $f \in R'_{K'}(H)$, luego se corresponde con un elemento $y_H \in R_{K'}(H)$. Por otra parte, $r \in R'_{K'}(P)$ se corresponde con $y_P = [K'[P]]$.

Como el homomorfismo e' para H es un isomorfismo, podemos expresar

$$y_H = [V \otimes_{D'} K'] - [W \otimes_{D'} K'],$$

donde V y W son $D[H]$-módulos proyectivos finitamente generados. Entonces

$$y = [(V \otimes_{D'} D'[P]) \otimes_{D'} K'] - [(W \otimes_{D'} D'[P]) \otimes_{D'} K'],$$

porque ambos miembros dan lugar al mismo carácter virtual $\chi = fr$. Además, como $D'[G] = D'[H] \otimes_{D'} D'[P]$, es inmediato que los $D'[G]$-módulos $V \otimes_{D'} D'[P]$ y $W \otimes_{D'} D'[P]$ son proyectivos, luego y está en la imagen de e'.

Ahora supongamos que χ toma valores en K y vamos a probar que y está en la imagen de e. Tenemos el diagrama conmutativo

$$\begin{array}{ccc} P_{k'}(G) & \xrightarrow{e'} & R_{K'}(G) \\ \uparrow & & \uparrow \\ P_k(G) & \xrightarrow[e]{} & R_K(G) \end{array}$$

en el que todas las flechas son monomorfismos. En la práctica los identificaremos con inclusiones. Sabemos que $y \in P_{k'}(G)$ y queremos probar que $y \in P_k(G)$.

Consideremos la restricción de coeficientes $\pi : R_{K'}(G) \longrightarrow R_K(G)$ determinada por $\pi([V]) = [V_K]$, donde, para cada $K'[G]$-módulo V, llamamos V_K al mismo V considerado como $K[G]$-módulo.

Observemos que $\pi[P_{k'}(G)] \subset P_k(G)$, pues si V es un $D'[G]$-módulo proyectivo y V_D es V considerado como $D[G]$-módulo, es evidente que también es un $D[G]$-módulo proyectivo, y $(V \otimes_{D'} K')_K \cong V_D \otimes_D K$. En efecto, basta observar que si (v_i) es una D'-base de V y (d'_j) es una D-base de D', entonces $v_i d'_j \otimes 1$ es una K-base de ambos miembros y G actúa igual sobre ella en ambos miembros. Así pues, $\pi([V \otimes_{D'} K]) = [V_D \otimes_D K] \in P_k(G)$.

Si $r = |K' : K|$, el hecho de que el carácter virtual de y tome valores en K se traduce, en virtud de la observación posterior al teorema 4.33, en que $ry = \pi(y) \in P_k(G)$. Ahora basta tener en cuenta el teorema 4.32, según el cual $P_{k'}(G) = P_k(G) \oplus C$, para cierto subgrupo C. Así, si la componente de y en C fuera no nula, la de ry también lo sería, luego concluimos que $y \in P_k(G)$. ∎

Con esto podemos demostrar un resultado técnico que vamos a necesitar:

Teorema 4.42 *Sea K'/K una extensión de cuerpos locales, sean D' y D sus anillos de enteros respectivos, sea G un grupo finito y $x \in R_{K'}(G)$ un elemento que cumpla las dos condiciones siguientes:*

a) El carácter virtual asociado a x toma valores en K.

b) Existe un número natural $n \geq 1$ tal que $nx = [V' \otimes_{D'} K']$, donde V' es un $D'[G]$-módulo proyectivo.

Entonces existe un $D[G]$-módulo proyectivo V, único salvo isomorfismo, tal que $x = [V \otimes_D K] \in R_K(G)$.

Demostración: Por b) tenemos que $nx = e(V' \otimes_{D'} k')$, luego 4.40 nos da que el carácter de nx se anula en los elementos p-singulares de G. Por consiguiente, lo mismo vale para el carácter virtual de x. El teorema 4.41 implica entonces que $x = e(y)$, para cierto $y \in P_k(G)$.

Falta probar que $y = [V \otimes_D k]$, para cierto $D[G]$-módulo proyectivo V, lo cual equivale a que las coordenadas de y en la base $I_k(G)$ sean positivas.

Ahora bien, si $\pi : R_{K'}(G) \longrightarrow R_K(G)$ es la restricción de coeficientes y $r = |K' : K|$, la observación posterior al teorema 4.33 nos da que $\pi(nx) = rnx$. Más aún, en la prueba del teorema anterior hemos visto que

$$rnx = \pi(nx) = \pi[V' \otimes_{D'} K] = [V'_D \otimes_D K].$$

Si no identificamos $P_k(G)$ con su imagen en $R_K(G)$, esto equivale a que $rny = [V'_D \otimes_D k]$, de modo que las coordenadas de rny en la base $I_k(G)$ son positivas, y lo mismo vale, por lo tanto, para las coordenadas de y.

Esto prueba la existencia de V, y la unicidad nos la da el teorema 4.13 (pues si $V_1 \otimes_D K \cong V_2 \otimes_D K$, entonces $V_1 \otimes_D k \cong V_2 \otimes_D k$, por la inyectividad de e).

∎

4.6 El teorema de Fong-Swan

Los resultados de la sección anterior sobre los homomorfismos d y e no son todo lo satisfactorios que podrían ser. Por ejemplo, hemos probado que, si K es suficientemente grande, entonces el homomorfismo $d : R_K(G) \longrightarrow R_k(G)$ es suprayectivo. Por lo tanto, si V es un $k[G]$-módulo, sabemos que existe un $x \in R_K(G)$ tal que $d(x) = [V]$, pero no tenemos la garantía de que x sea de la forma $x = [W]$, para cierto $k[G]$-módulo finitamente generado W, es decir, no

podemos asegurar que todo $k[G]$-módulo finitamente generado sea la reducción de un $K[G]$-módulo finitamente generado. Si llamamos

$$R_K^+(G) = \{[V] \mid V \text{ es un } K[G]\text{-módulo finitamente generado}\},$$

$$R_k^+(G) = \{[V] \mid V \text{ es un } k[G]\text{-módulo finitamente generado}\},$$

sabemos que $d : R_K^+(G) \longrightarrow R_k^+(G)$, pero no tenemos probado que esta restricción sea suprayectiva. De hecho, sucede que no siempre lo es. El teorema central de esta sección afirma que una condición suficiente para que lo sea es que el grupo G sea resoluble.

Definición 4.43 Si p es un primo, diremos que un grupo finito G es *p-resoluble* si admite una serie cuyos factores tengan orden potencia de p o primo con p.

Todo grupo resoluble admite una serie cuyos factores son cíclicos de orden potencia de primo, luego los grupos resolubles son p-resolubles para todo p.

Teorema 4.44 (Fong-Swan) *Sea K un cuerpo local cuyo cuerpo de restos k tenga característica p y sea G un grupo p-resoluble. Si K es suficientemente grande para G, todo $k[G]$-módulo simple es la reducción de un $K[G]$-módulo (necesariamente simple).*

Demostración: Vamos a llamar *altura* de un grupo p-resoluble G a la menor longitud de una serie en G que cumpla la definición de grupo p-resoluble. Demostraremos el teorema por inducción sobre la altura de G. Si G tiene altura 0, entonces $G = 1$ y el teorema es trivial.

Supongamos que G tiene altura h y que el teorema es cierto para grupos p-resolubles de altura menor que h. Si G no cumple el teorema, podemos suponer que es el grupo p-resoluble de altura h de menor orden posible de entre los que no cumplen el teorema. Equivalentemente, podemos suponer que todo grupo p-resoluble de altura h y orden menor que $|G|$ cumple el teorema. Vamos a probar que G también lo cumple y esta contradicción demostrará el teorema.

Sea, pues, V un $k[G]$-módulo simple y vamos a probar que es la reducción de un cierto $K[G]$-módulo.

Sea $N \trianglelefteq G$ el primer término no trivial de una serie mínima según la definición de grupo p-resoluble. De este modo, G/N es p-resoluble de altura $\leq h-1$.

Si N es un p-grupo, el subespacio V^N de los elementos de V fijados por N es no nulo por 1.14, y el hecho de que N sea normal implica que V^N es un $k[G]$-submódulo de V (véase la prueba del teorema 3.51). Como V es simple, ha de ser $V = V^N$, luego V es un $k[G/N]$-módulo simple. Por hipótesis de inducción, V es la reducción de un $K[G/N]$-módulo W, y es claro que V, como $k[G]$-módulo, es la reducción de W como $K[G]$-módulo.

Así pues, a partir de ahora suponemos que p no divide al orden de N. Ahora V es un $k[N]$-módulo semisimple. Si V tiene dos factores de composición no isomorfos, podemos aplicar el teorema 2.38, según el cual[6] existe un subgrupo $N \leq H < G$ y un $k[H]$-módulo simple W tal que $V = W \otimes_{k[H]} k[G]$.

[6]Está probado cuando $k = \mathbb{C}$, pero se comprueba inmediatamente que la prueba es válida siempre que $\operatorname{car} k \nmid |G|$.

El mismo argumento que prueba que todo subgrupo de un grupo resoluble es resoluble muestra que H tiene altura $\leq h$. Si la longitud es h, el hecho de que $|H| < |G|$ nos permite aplicar igualmente la hipótesis de inducción para concluir que existe un $K[H]$-módulo simple M cuya reducción es W, y el teorema 4.29 implica que la reducción de $M \otimes_{K[H]} K[G]$ es V.

Por lo tanto, podemos suponer que todos los factores de composición de V como $k[N]$-módulo son isomorfos a un mismo $k[N]$-módulo simple V_0. Como $p \nmid |N|$, existe un $K[N]$-módulo irreducible W_0 cuya reducción es V_0. El grado de W_0 divide a $|N|$, luego también es primo con p. Más detalladamente, lo que tenemos es que $W_0 = R_0 \otimes_D K$, donde R_0 es un $D[N]$-módulo (libre sobre D) tal que $R_0 \otimes_D k \cong V_0$. Notemos que, como $k[N]$ es semisimple, V_0 es proyectivo, luego R_0 también es un $D[G]$-módulo proyectivo.

Podemos identificar a V_0 con un $k[N]$-submódulo concreto de V. Entonces, dado $\sigma \in G$, tenemos que $V_0\sigma$ es también un $k[N]$-submódulo de V, pues si $v \in V_0$ y $n \in N$, tenemos que $v\sigma n = v(\sigma n \sigma^{-1})\sigma \in V_0\sigma$. Como todos los factores de composición de V como $k[N]$-módulo son isomorfos a V_0, es necesario que $V_0\sigma$ sea simple e isomorfo a V_0 como $k[N]$-módulo.

Consideremos el isomorfismo (de k-espacios vectoriales) $\phi : V_0 \longrightarrow V_0\sigma$ dado por $\phi(v) = v\sigma$. En principio, no es un isomorfismo de módulos, pero sí que lo es si en V_0 consideramos el producto dado por $v \cdot n = v(\sigma n \sigma^{-1})$. Si llamamos V_0^σ a V_0 con esta estructura de $k[N]$-módulo, acabamos de probar que $V_0 \cong V_0^\sigma$.

Análogamente, llamemos R_0^σ a R_0 con la estructura de $D[G]$-módulo dada por el producto $r \cdot n = r(\sigma n \sigma^{-1})$. Es claro que $R_0^\sigma \otimes_D k \cong V_0^\sigma \cong V_0$, luego $R_0^\sigma \cong R_0$ por el teorema 4.13. Sea, pues, $f : R_0^\sigma \longrightarrow R_0$ un isomorfismo de $D[N]$-módulos. Explícitamente, esto significa que

$$f(v(\sigma n \sigma^{-1})) = f(v)n$$

Si llamamos $\rho : G \longrightarrow \mathrm{Aut}(R_0)$ a la representación lineal asociada a R_0, esto equivale a que

$$f \circ \rho(n) \circ f^{-1} = \rho(\sigma n \sigma^{-1})$$

para todo $n \in N$. Para cada $\sigma \in G$, llamemos U_σ al conjunto de todos los $f \in \mathrm{Aut}(R_0)$ que cumplen la relación anterior. Acabamos de ver que $U_\sigma \neq \varnothing$. Se comprueba fácilmente que si $f \in U_\sigma$ y $f' \in U_{\sigma'}$, entonces $f \circ f' \in U_{\sigma\sigma'}$.

Esto hace que el conjunto G_1 de todos los pares (σ, f) con $f \in U_\sigma$ sea un grupo con el producto de G en la primera componente y la composición en la segunda.

La proyección $G_1 \longrightarrow G$ en la primera componente es un epimorfismo, cuyo núcleo es isomorfo a U_1, que es el grupo de todos los $f \in \mathrm{Aut}(R_0)$ que conmutan con todos los automorfismos $\rho(n)$. Equivalentemente, $U_1 = \mathrm{Aut}_N(R_0)$. Como W_0 es (absolutamente) simple (porque su reducción V_0 es simple), sabemos que $\mathrm{End}_N(W_0) = K$, es decir, que los únicos endomorfismos de W_0 son las homotecias. Como cada elemento de U_1 induce un endomorfismo de K, ha de ser una homotecia y, para que tenga tenga inversa en $\mathrm{End}_N(R_0)$, su razón ha de ser una unidad de D. En definitiva, U_1 es el grupo de las unidades de D.

Como las homotecias conmutan con todos los automorfismos, resulta que $U_1 \leq Z(G_1)$. Notemos que G_1 es un grupo infinito. Vamos a construir un grupo con propiedades similares pero que sea finito.

Para ello observamos en primer lugar que podemos sustituir K por una extensión finita K'. En efecto, si probamos que $V \otimes_k k'$ es la reducción de un $K'[G]$-módulo, éste será necesariamente de la forma $W \otimes_K K'$, donde W es un $K[G]$-módulo, porque K es un cuerpo de escisión para G, y la reducción de W será isomorfa a V, porque la extensión de coeficientes es un isomorfismo $R_k(G) \longrightarrow R_{k'}(G)$.

Con la extensión de coeficientes, es claro que V_0 se sustituye por $V_0 \otimes_k k'$ y R_0 por $R_0 \otimes_D D'$, donde D' es el anillo de enteros de K'. Además, cada $f \in U_\sigma$ se extiende a un automorfismo $f' \in U'_\sigma$ con el mismo determinante.

Llamemos $d = \operatorname{rang} R_0$ que, según hemos visto, es primo con p. Para cada $\sigma \in G$, escojamos un $f \in U_\sigma$ y elijamos una raíz $\epsilon_\sigma = \sqrt[d]{\det f}$ en una clausura algebraica de K. Tomamos como K' la adjunción a K de todos los elementos ϵ_σ, para $\sigma \in G$, con lo que tenemos ciertamente una extensión finita de K. Sustituyendo K por K', podemos afirmar que, para cada $\sigma \in G$, existe un $f \in U_\sigma$ tal que $\det f = \epsilon^d$, para cierto $\epsilon \in U_1$. Entonces, $f' = \epsilon^{-1} f \in U_\sigma$ cumple que $\det(f') = 1$. En definitiva, cada conjunto U_σ contiene un automorfismo de determinante 1.

Sea C la imagen del homomorfismo $N \longrightarrow U_1$ dado por $\sigma \mapsto \det \rho(n)$ y sea G_2 el subgrupo de G_1 formado por los pares (σ, f) tales que $\det f \in C$. Como siempre existe un par (σ, f) tal que $\det f = 1 \in C$, resulta que la proyección $G_2 \longrightarrow G$ sigue siendo suprayectiva, y su núcleo N' está formado por las unidades $\epsilon \in U_1$ tales que $\epsilon^d \in C$. Como p no divide al orden de N, tampoco divide al orden de C, luego todo $\epsilon \in N'$ es una raíz de la unidad de orden primo con p. Concluimos que N' es un grupo cíclico de orden primo con p. Más aún, tenemos que $N' \leq Z(G_2)$.

En particular, G_2 es un grupo finito. La proyección en la segunda componente $\rho_2 : G_2 \longrightarrow \operatorname{Aut}(R_0)$ es una representación lineal de G_2 sobre D. Tenemos un monomorfismo de grupos $N \longrightarrow G_2$ dado por $n \mapsto (n, \rho(n))$, a través del cual podemos considerar que $N \trianglelefteq G_2$. Además $N \cap N' = 1$ y la restricción de ρ_2 a N coincide con ρ.

Sea $F = \operatorname{Hom}_N(V_0, V)$ y sea $u : V_0 \otimes_k F \longrightarrow V$ la aplicación lineal dada por $u(v \otimes g) = g(v)$. Vamos a ver que es un isomorfismo.

En efecto, $\dim_k F = \langle [V_0], [V] \rangle$ es la multiplicidad de V_0 como factor de composición de V, luego $\dim_k V_0 \otimes_k F = \dim_k V$. Por lo tanto, basta ver que u es suprayectiva. Ahora bien, dado $v \in V$, el $k[N]$-submódulo de V generado por v es simple, luego isomorfo a V_0, luego existe un $k[N]$-monomorfismo $g : V_0 \longrightarrow V$ y un $v_0 \in V_0$ tal que $v = g(v_0) = u(v_0 \otimes g)$.

La estructura de $D[G_2]$-módulo de R_0 se reduce a una estructura de $k[G_2]$-módulo de V_0. Concretamente, $v(\sigma, f) = \bar{f}(v)$, donde $\bar{f}$ es el automorfismo de V_0 inducido por f.

A su vez, podemos dotar a F de estructura de $k[G_2]$-módulo con el producto dado por

$$(g(\sigma, f))(v) = g(\bar{f}^{-1}(v))\sigma.$$

(Hay que comprobar que $g(\sigma, f)$ así definido es un $D[N]$-homomorfismo y que la aplicación $G_2 \longrightarrow \mathrm{Aut}(F)$ es un homomorfismo. Todo ello se ve sin dificultad.)

Por último, el $k[G]$-módulo V puede verse como un $k[G_2]$-módulo a través del epimorfismo $G_2 \longrightarrow G$. Entonces u es un isomorfismo de $k[G_2]$-módulos. En efecto,

$$u((v\otimes g)(\sigma,f)) = u(\bar{f}(v)\otimes(g(\sigma,f))) = (g(\sigma,f))(\bar{f}(v)) = g(v)\sigma = u(v\otimes g)(\sigma,f).$$

Tenemos que $V_0 = R_0 \otimes_D k$ como $k[G_2]$-módulo. Supongamos que encontramos un $D[G_2]$-módulo D-libre F_0 tal que $F \cong F_0 \otimes_D k$. Entonces tendríamos que $V \cong (R_0 \otimes_D F_0) \otimes_D k$. Este isomorfismo es también un isomorfismo de $k[N']$-módulos, pero p no divide al orden de N, luego la reducción $R_K(N') \longrightarrow R_k(N')$ es un isomorfismo. Como V es un $k[N']$-módulo trivial, resulta que $(R_0 \otimes_D F_0) \otimes_D K$ es un $K[N']$-módulo trivial, es decir, que visto como $K[G_2]$-módulo, sucede que N' actúa trivialmente sobre él, luego tiene una estructura natural de $K[G]$-módulo, ya que $G = G_2/N'$. Tenemos, pues, un $K[G]$-módulo cuya reducción es V.

Así pues, sólo falta probar que F es la reducción de un cierto $D[G_2]$-módulo D-libre. Notemos que F es un $k[G_2]$-módulo simple, pues en caso contrario V tampoco sería simple. La definición de la acción de G_2 sobre F muestra que N actúa trivialmente sobre él, luego F es también un $k[H]$-módulo simple, donde $H = G_2/N$.

Como $N \cap N' = 1$, el homomorfismo natural $N' \longrightarrow H$ es inyectivo, y $N' \trianglelefteq H$. Como $N' \leq Z(G_2)$, también $N' \leq Z(H)$. Además,

$$H/N' = (G_2/N)/(NN'/N) \cong G_2/(NN') \cong (G_2/N')/(NN'/N') \cong G/N.$$

Si la altura de G es $h = 1$, entonces $G = N$, luego $H = N'$ tiene orden primo con p, y es evidente que F es la reducción de un $K[H]$-módulo F_0.

Supongamos, pues, que $h \geq 2$, en cuyo caso G/N tiene altura $\leq h-1$, al igual que H/N', luego H/N' tiene un subgrupo normal M/N' (el primer término no nulo de una serie de altura $h-1$) de orden potencia de p o primo con p de modo que H/M tiene altura $\leq h-2$.

Si M/N' es un p-grupo, sea P un p-subgrupo de Sylow de M. Como el orden de N' no es divisible entre p, tenemos que $N' \cap P = 1$, luego $M = N'P$ y, como $N' \leq Z(M)$, de hecho $M = N' \times P$. Como $P \trianglelefteq M$, resulta ser el único p-subgrupo de Sylow de M, y esto implica a su vez que $P \trianglelefteq H$.

El argumento empleado al principio de la prueba muestra que P actúa trivialmente sobre F, luego F es un $k[H/P]$-módulo simple. Ahora bien, como H/M tiene altura $\leq h-2$, resulta que H/P tiene altura $\leq h-1$ y podemos aplicar la hipótesis de inducción.

Supongamos ahora que el orden de M/N' no es divisible entre p, con lo que el de M tampoco lo es. Como la altura de H/M es $\leq h-2$, la de H es $\leq h-1$ y de nuevo podemos aplicar la hipótesis de inducción. ∎

Como consecuencia inmediata, si G es p-resoluble y K es un cuerpo de escisión para G con cuerpo de restos k de característica p, tenemos que la aplicación $d : R_K^+(G) \longrightarrow R_k^+(G)$ es suprayectiva.

Como consecuencia podemos demostrar un resultado análogo para el homomorfismo $e : P_k(G) \longrightarrow R_K(G)$. Definimos

$$P_k^+(G) = \{[V] \mid V \text{ es un } k[G]\text{-módulo proyectivo finitamente generado}\}.$$

Teorema 4.45 *Si K es un cuerpo local con cuerpo de restos k de característica p y G es un grupo finito p-resoluble, entonces $e[P_k^+(G)] = e(P_k(G)) \cap R_K^+(G)$.*

Demostración: Se trata de probar que si V es un $K[G]$-módulo finitamente generado tal que $[V]$ está en la imagen del homomorfismo e, entonces, más concretamente, $[V] = e([W])$, para cierto $k[G]$-módulo proyectivo W finitamente generado.

Sea K'/K una extensión finita tal que K' sea suficientemente grande para G. Vamos a ver que si el teorema es cierto para K', también lo es para K. En efecto, si $[V]$ está en la imagen de e, entonces $[V_{K'}]$ está en la imagen de e'. Suponemos, pues, que existe un $k'[G]$-módulo proyectivo W tal que $e([W]) = [V_{K'}]$. Esto significa que $W = R \otimes_D k'$, donde R' es un $D'[G]$-módulo proyectivo, y que $[V_{K'}] = [R' \otimes_D k']$. Ahora basta aplicar el teorema 4.42 con $x = [V_{K'}]$ y $n = 1$, de modo que $[V] = [R \otimes_D K] = e(R \otimes_D k)$, donde R es un $D[G]$-módulo proyectivo.

Suponemos, pues, que K es suficientemente grande para G. Consideremos la base $S_k(G) = \{[V_1], \ldots, [V_n]\}$ de $R_k(G)$ y la base $I_k(G) = \{[P_{V_1}], \ldots, [P_{V_n}]\}$ de $P_k(G)$, donde P_{V_i} es la envoltura proyectiva de V_i. Estamos suponiendo que $[V] = e(z)$, donde

$$z = \sum_{i=1}^{n} n_i [P_{V_i}] \in P_k(G),$$

para ciertos $n_i \in \mathbb{Z}$ y queremos probar que $n_i \geq 0$. Por el teorema de Fong-Swan existe $z_i \in R_K^+(G)$ tal que $d(z_i) = [V_i]$. Entonces,

$$n_i = \langle z, [V_i] \rangle_k = \langle z, d(z_i) \rangle_k = \langle e(z), z_i \rangle_K = \langle [V], z_i \rangle_K \geq 0.$$

■

A su vez, esto nos da una versión más precisa del teorema 4.40:

Teorema 4.46 *Si K es un cuerpo local cuyo cuerpo de restos tenga característica p y G es un grupo finito p-resoluble entonces un $K[G]$-módulo finitamente generado V es de la forma $V \cong R \otimes_D K$, para cierto $D[G]$-módulo proyectivo R si y sólo si el carácter de V se anula en los elementos p-singulares de G.*

4.7 Caracteres modulares

Observemos que, con la teoría desarrollada hasta ahora, no podemos responder a una pregunta tan elemental como cuántas representaciones irreducibles tiene un grupo finito G sobre un cuerpo de escisión k cuando la característica

de k divide al orden de G. En esta sección desarrollaremos una teoría de caracteres mejor adaptada al caso modular que la teoría de caracteres ordinarios. Entre otras cosas, con ella podremos responder a la pregunta que acabamos de formular. Por simplicidad trabajaremos con cuerpos suficientemente grandes para G (aunque los resultados se generalizan fácilmente a cuerpos de escisión arbitrarios).

En principio, sabemos que las representaciones irreducibles de G se corresponden biunívocamente con los caracteres irreducibles de G sobre k, que son funciones de clase linealmente independientes, luego su número es a lo sumo igual al número de clases de conjugación de G. Cuando $\operatorname{car} k \nmid |G|$ (y k es un cuerpo de escisión) se da la igualdad, pero vamos a ver que no sucede lo mismo cuando $\operatorname{car} k$ divide a $|G|$. La razón es el teorema 3.52, según el cual, en la tabla de caracteres (irreducibles) de G sobre k, cada columna correspondiente a una clase de elementos p-singulares (de orden múltiplo de p) es igual a otra columna correspondiente a una clase de elementos p-regulares (de orden primo con p). Sabemos que la tabla tiene filas linealmente independientes sobre k, luego, si eliminamos las columnas correspondientes a las clases p-singulares, la tabla seguirá teniendo filas linealmente independientes.

Definición 4.47 Si G es un grupo finito y k es un cuerpo de característica prima p, llamaremos G_r al conjunto de elementos p-regulares de G y $F_k(G_r)$ al k-espacio vectorial de todas las funciones de clases $f : G_r \longrightarrow k$.

En estos términos, acabamos de probar que si $\chi_1, \ldots, \chi_h$ son los caracteres irreducibles de G sobre k, entonces, las restricciones $\chi_i|_{G_r}$ son linealmente independientes en $F_k(G_r)$, luego el número h es a lo sumo igual al número de clases de conjugación p-regulares. Veremos que, si k es un cuerpo de escisión para G, se da la igualdad.

Para ello retomamos la situación de la sección precedente: en lo sucesivo, G será un grupo finito, K un cuerpo local con anillo de enteros D y cuerpo de restos k de característica p, y ahora supondremos además que K es suficientemente grande para G. Llamaremos m' al mínimo común múltiplo de los órdenes de los elementos de G_r. Por hipótesis, K (y, más concretamente, D) contiene al grupo $U_{m'}(K)$ de las raíces m'-ésimas de la unidad, de tal modo que el polinomio $X^{m'} - 1$ factoriza en $D[X]$ en la forma

$$X^{m'} - 1 = (X - \omega_1) \cdots (X - \omega_{m'}).$$

Tomando clases módulo el ideal maximal $\mathfrak{m}$ de D obtenemos una descomposición análoga en $k[X]$, luego concluimos que las clases $[\omega_i] \in k$ son todas las raíces en k del polinomio $X^{m'} - 1$. Como p no divide a m', estas raíces han de ser distintas dos a dos, luego vemos que k contiene al grupo $U_{m'}(k)$ de las raíces m'-ésimas de la unidad y que la reducción módulo $\mathfrak{m}$ induce una aplicación suprayectiva (luego biyectiva) $U_{m'}(K) \longrightarrow U_{m'}(k)$. Para cada $\lambda \in U_{m'}(k)$, llamaremos $\tilde{\lambda} \in U_{m'}(K)$ a su única antiimagen.

Consideremos ahora un $k[G]$-módulo finitamente generado V y sea $\sigma \in G_r$. Llamemos $H = \langle \sigma \rangle$, de modo que podemos considerar a V como $k[H]$-módulo.

Como $p \nmid |H|$, es semisimple y, como H es abeliano y k es un cuerpo de escisión para H, resulta que todas las representaciones irreducibles de H sobre k tienen grado 1. Por consiguiente, podemos descomponer

$$V = V_1 \oplus \cdots \oplus V_n$$

en suma directa de $k[H]$-submódulos $V_i = \langle v_i \rangle$ de dimensión 1 sobre k. Así pues, $v_i\sigma = \lambda_i v_i$ para ciertos $\lambda_i \in k$. La base $v_1, \ldots, v_n$ de V determina una representación matricial $\rho : G \longrightarrow \mathrm{LG}(n,k)$ tal que $\rho(\sigma)$ es una matriz diagonal. Como $\sigma^{m'} = 1$, también $\rho(\sigma)^{m'} = I_n$, lo que se traduce en que los elementos de la diagonal de $\rho(\sigma)$ (es decir, los escalares λ_i) están en $U_{m'}(k)$.

Es claro que los valores λ_i son los vectores propios de $\rho(\sigma)$, es decir, las raíces del polinomio característico de $\rho(\sigma)$, y cada uno aparece repetido tantas veces como indica su multiplicidad como raíz. Por lo tanto, no dependen de la elección de la base con la que hemos calculado la representación ρ.

Definición 4.48 En las condiciones anteriores, si V es un $k[G]$-módulo finitamente generado, su *carácter modular* o *carácter de Brauer* es la función $\phi_V : G_r \longrightarrow D$ que a cada $\sigma \in G_r$ le asigna el valor

$$\phi_V(\sigma) = \sum_{i=1}^{n} \tilde{\lambda}_i,$$

donde $\lambda_1, \ldots, \lambda_n \in U_{m'}(k)$ son los valores propios del endomorfismo inducido por σ en V (repetidos según su multiplicidad en el polinomio característico).

Si $\chi_V : G \longrightarrow k$ es el carácter ordinario de V, su relación con ϕ_V consiste en que $\chi_V|_{G_r}$ es la composición de ϕ_V con el epimorfismo canónico $D \longrightarrow k$. Más aún, si $\sigma \in G$ se descompone como $\sigma = \pi\sigma'$ como en el teorema 3.52, tenemos que $\chi_V(\sigma) = [\phi_V(\sigma')] \in k$, por lo que el carácter modular ϕ_V determina completamente el carácter ordinario χ_V.

Veamos algunas propiedades elementales:

a) $\phi_V(1) = \dim_k V$.

b) *ϕ_V es una función de clases en G_r, en el sentido de que si $\sigma \in G_r$ y $\tau \in G$, entonces $\phi_V(\sigma^\tau) = \phi_V(\sigma)$.*

   Esto se debe a que σ^τ y σ determinan endomorfismos conjugados en V, y dos endomorfismos conjugados tienen matrices semejantes, luego tienen el mismo polinomio característico.

c) *Si $0 \longrightarrow V' \longrightarrow V \longrightarrow V'' \longrightarrow 0$ es una sucesión exacta de $k[G]$-módulos finitamente generados, entonces $\phi_V = \phi_{V'} + \phi_{V''}$.*

   En efecto, dado $\sigma \in G_r$, no perdemos generalidad suponiendo que $G = \langle \sigma \rangle$, pero entonces $k[G]$ es semisimple, luego $V = V' \oplus V''$. Formando una base de vectores propios para σ en V como unión de bases correspondientes para V' y V'', la conclusión es inmediata.

d) *Dados dos $k[G]$-módulos finitamente generados V y V', se cumple que $\phi_{V\otimes_k V'} = \phi_V\phi_{V'}$.*

Dado $\sigma \in G_r$, basta tener en cuenta que el producto tensorial de una base de vectores propios para σ en V por otra en V' es una base de vectores propios para σ en $V \otimes_k V'$.

e) *Sea W un $K[G]$-módulo finitamente generado de carácter χ, sea $R \subset W$ un retículo estable y $V = R \otimes_D k$. Entonces $\phi_V = \chi|_{G_r}$.*

Dado $\sigma \in G_r$, no perdemos generalidad si suponemos que $G = \langle\sigma\rangle$. Según el teorema 4.15, los factores de composición de V son independientes del retículo R que elijamos en W y, por la propiedad c), el carácter ϕ_V es la suma de los caracteres modulares de dichos factores de composición. Por lo tanto, podemos elegir R sin alterar ϕ_V. Dado $\sigma \in G_r$, tomamos como R el retículo generado por una base de vectores propios para σ, con lo que V tiene una base de vectores propios para σ cuyos valores propios son las reducciones de los valores propios de la base de R. La conclusión es inmediata.

La forma bilineal definida en 4.6 puede expresarse en términos de los caracteres modulares:

Teorema 4.49 *Si P y V son $k[G]$-módulos finitamente generados con P es proyectivo y ϕ_P, ϕ_V son sus caracteres modulares respectivos, entonces*

$$\langle [P], [V]\rangle_k = \frac{1}{|G|}\sum_{\sigma\in G_r} \phi_P(\sigma^{-1})\phi_V(\sigma).$$

Demostración: Por definición, $\langle [P], [V]\rangle_k = \dim_k \mathrm{Hom}_G(P, V)$. Según hemos visto en la sección 1.4, el espacio $H = \mathrm{Hom}_k(P, V)$ tiene una estructura natural de $k[G]$-módulo respecto a la cual $\mathrm{Hom}_G(P, V) = H^G$. Según 1.62, tenemos que $H \cong P^* \otimes_k V$, y los teoremas 1.58 y 1.64 implican que H es un $k[G]$-módulo proyectivo. El teorema 4.20 nos da un $D[G]$-módulo proyectivo H_0 tal que $H \cong H_0 \otimes_D k$. Llamemos $H_1 = H_0 \otimes_D K$ y vamos a probar que

$$\dim_K H_1^G = \mathrm{rang}\, H_0^G = \dim_k H^G.$$

Para probar las dos igualdades simultáneamente probaremos que, si $D \longrightarrow E$ es un homomorfismo de anillos, entonces

$$H_0^G \otimes_D E \cong (H_0 \otimes_D E)^G.$$

Más concretamente, el homomorfismo natural $H_0^G \otimes_D E \longrightarrow (H_0 \otimes_D E)^G$ es un isomorfismo. Sea $H_0 \oplus H' = L$, donde K es un $D[G]$-módulo libre. Claramente, $L^G = H_0^G \oplus H'^G$ y tenemos un diagrama conmutativo

$$\begin{array}{ccc} (H_0^G \otimes_D E) \oplus (H'^G \otimes_D E) & \longrightarrow & L^G \otimes_D E \\ \downarrow & & \downarrow \\ (H_0 \otimes_D E)^G \oplus (H' \otimes_D E)^G & \longrightarrow & (L \otimes_D E)^G \end{array}$$

luego basta probar el resultado para un $D[G]$-módulo libre $L \cong D[G]^n$, pero es claro entonces que basta probarlo para $D[G]$. En suma, hay que probar que el homomorfismo canónico $D[G]^G \otimes_D E \longrightarrow E[G]^G$ es un isomorfismo, pero esto es obvio, pues $D[G]^G$ es el D-submódulo generado por $T = \sum_{\sigma\in G} \sigma$, y análogamente con $E[G]^G$.

Retomando el argumento, ahora tenemos que

$$\langle [P], [V] \rangle_k = \dim_K H_1^G = \langle 1_K, \chi \rangle_K = \frac{1}{|G|} \sum_{\sigma\in G} \chi(\sigma),$$

donde χ es el carácter del $K[G]$-módulo H_1. Por el teorema 4.40 sabemos que χ se anula fuera de G_r y, restringido a G_r es el carácter modular del $k[G]$-módulo H, por la propiedad e) anterior. La propiedad d) nos da que $\chi|_{G_r} = \phi_{P^*}\phi_V$. El teorema 1.65 afirma que los caracteres ordinarios χ_{P^*} y χ_P cumplen la relación $\chi_{P^*}(\sigma) = \chi_P(\sigma^{-1})$, de donde se deduce inmediatamente que ϕ_{P^*} y ϕ_P cumplen lo mismo. En definitiva, $\chi|_{G_r}(\sigma) = \phi_P(\sigma^{-1})\phi_V(\sigma)$, y obtenemos la fórmula del enunciado. ∎

Definición 4.50 Llamamos $F_K(G_r)$ a la K-álgebra de las funciones de clase en G_r con valores en K y $R'_K(G_r)$ al subgrupo abeliano generado por los caracteres modulares de G, que es un subanillo por la propiedad d) precedente.

La propiedad c) nos permite definir un epimorfismo $R_k(G) \longrightarrow R'_K(G_r)$ que asigna un *carácter modular virtual* ϕ_x a cada $x \in R_k(G)$. La propiedad e) nos da el diagrama conmutativo

$$\begin{array}{ccc} R_K(G) & \xrightarrow{d} & R_k(G) \\ {\scriptstyle\chi}\downarrow & & \downarrow{\scriptstyle\phi} \\ R'_K(G) & \longrightarrow & R'_K(G_r) \end{array}$$

donde la flecha horizontal inferior es la restricción de G a G_r.

Teorema 4.51 *El homomorfismo $R_k(G) \longrightarrow R'_K(G_r)$ es un isomorfismo de anillos que se extiende a un isomorfismo de K-álgebras $K\otimes_{\mathbb{Z}} R_k(G) \longrightarrow F_K(G_r)$.*

Demostración: Sea $S_k(G) = \{[V_1], \ldots, [V_h]\}$ y vamos a probar que los caracteres modulares $\phi_1, \ldots, \phi_h$ son distintos dos a dos y linealmente independientes en $F_K(G_r)$. En caso contrario tendríamos una combinación lineal

$$\alpha_1\phi_1 + \cdots + \alpha_h\phi_h = 0,$$

donde $\alpha_i \in K$ no son todos nulos. Multiplicándolos por una potencia adecuada de un primo de D, podemos suponer que todos ellos están en D y que al menos uno es una unidad. Componiendo con el epimorfismo canónico $D \longrightarrow k$ obtenemos que $\bar\alpha_1\chi_1|_{G_r} + \cdots + \bar\alpha_h\chi_h|_{G_r} = 0$, donde χ_i es el carácter ordinario de V_i, y tenemos que algún $\bar\alpha_i \neq 0$. Esto contradice la observación tras la definición 4.47.

En particular, los caracteres modulares son linealmente independientes sobre $\mathbb{Z}$, luego son una base de $R'_K(G_r)$ y tenemos el primer isomorfismo del enunciado. Ahora vamos a probar que los caracteres modulares generan $F_K(G_r)$. Para ello, tomamos una función de clases arbitraria $f \in F_K(G_r)$ y la extendemos con el valor 0 fuera de G_r, lo que la convierte en una función de clases $\bar{f} \in F_K(G)$.

Como K es un cuerpo de escisión de G, los caracteres irreducibles $\psi_1, \dots, \psi_n$ de G sobre K forman una base de $F_K(G)$, luego podemos expresar

$$\bar{f} = \alpha_1\psi_1 + \cdots + \alpha_n\psi_n,$$

con $\alpha_i \in K$. Restringiendo a G_r esta expresión obtenemos que

$$f = \alpha_1\psi_1|_{G_r} + \cdots + \alpha_n\psi_n|_{G_r},$$

donde cada $\psi_i|_{G_r}$ está en $R'_K(G_r)$, luego es combinación lineal de los caracteres modulares ϕ_i, luego f también lo es. Esto prueba que los caracteres modulares ϕ_i son una K-base de $R_K(G_r)$, lo que equivale al segundo isomorfismo del enunciado. ∎

En particular, vemos que el número de representaciones irreducibles de G sobre k es igual al número de clases de conjugación p-regulares de G.

Llamemos h al número de clases de conjugación de G y h_p al número de clases de conjugación p-regulares. El monomorfismo $e : P_k(G) \longrightarrow R_K(G)$ induce un monomorfismo $K \otimes_{\mathbb{Z}} P_k(G) \longrightarrow K \otimes_{\mathbb{Z}} R_K(G) \cong F_K(G)$. Sabemos que $P_k(G)$ tiene rango h_p, luego la imagen de $K \otimes_{\mathbb{Z}} P_k(G)$ tiene dimensión h_p sobre K. Según el teorema 4.40, dicha imagen está contenida en el subespacio de las funciones de $F_K(G)$ que se anulan fuera de G_r, pero dicho subespacio se identifica de forma natural con $F_K(G_r)$, luego tiene dimensión h_p. Por consiguiente, podemos identificar $K \otimes_{\mathbb{Z}} P_k(G)$ con $F_K(G_r)$.

Acabamos de ver que, mediante las identificaciones $K \otimes_{\mathbb{Z}} P_k(G) \cong F_K(G_r)$ y $K \otimes_{\mathbb{Z}} R_K(G) \cong F_K(G)$, el monomorfismo $1 \otimes e$ se corresponde con la inclusión, si convenimos a su vez en identificar $F_K(G_r)$ con las funciones de clases que se anulan fuera de G_r.

Por otra parte, el diagrama conmutativo previo a 4.51 implica que, a través de la identificación $K \otimes_{\mathbb{Z}} R_k(G) \cong F_K(G_r)$ dada por dicho teorema, el epimorfismo $1 \otimes d$ se corresponde con la restricción $F_K(G) \longrightarrow F_K(G_r)$. Así pues, el triángulo formado por los homomorfismos c, d, e se convierte, al multiplicar por $K \otimes_{\mathbb{Z}}$, en el triángulo

$$\begin{array}{ccc} F_K(G_r) & \xrightarrow{1\otimes c} & F_K(G_r) \\ & {\scriptstyle 1\otimes e}\searrow \quad \nearrow{\scriptstyle 1\otimes d} & \\ & F_K(G) & \end{array}$$

donde $1 \otimes c$ resulta ser la identidad (la composición de la inclusión con la restricción). Ahora bien, debemos tener presente que, a través de la identificación $K \otimes_{\mathbb{Z}} R_k(G) \cong F_K(G_r)$, la base canónica $1 \otimes S_k(G)$ se corresponde con la

base de los caracteres modulares $\phi_{V_1}, \ldots, \phi_{V_{h_p}}$ de los $k[G]$-módulos irreducibles $V_1, \ldots, V_{h_p}$, mientras que, a través de la identificación $K \otimes_{\mathbb{Z}} P_k(G) \cong F_K(G_r)$, la base canónica $1 \otimes I_k(G)$ se corresponde con la formada por los caracteres modulares $\Phi_{V_1}, \ldots, \Phi_{V_{h_p}}$ de las envolturas proyectivas de los módulos V_i.

En efecto, podemos expresar $P_{V_i} = P'_{V_i} \otimes_D k$, donde P'_{V_i} es un $D[G]$-módulo proyectivo finitamente generado. Así, $1 \otimes [P_{V_i}]$ se identifica con su imagen por $1 \otimes e$, que es $1 \otimes [P'_{V_i} \otimes_D K]$, la cual se identifica a su vez con el carácter ordinario de $P'_{V_i} \otimes_D K$ (que se anula fuera de G_r por 4.40), el cual coincide con el carácter modular de P_{V_i} por la propiedad e) tras la definición 4.48.

Por consiguiente, la matriz de Cartan C y la matriz de descomposición D están relacionadas con los caracteres del modo siguiente:

$$\Phi_V = \sum_{[V'] \in S_k(G)} c_{VV'} \phi_{V'} \quad \text{para todo } [V] \in S_k(G),$$

$$\chi_W = \sum_{[V] \in S_k(G)} d_{WV} \phi_V \quad \text{para todo } [W] \in S_K(G),$$

$$\Phi_V = \sum_{[W] \in S_K(G)} d_{WV} \chi_W \quad \text{para todo } [V] \in S_k(G).$$

La última relación correspondería a la matriz E, que es la traspuesta de D.

4.8 Ejemplo: los caracteres de Σ_4

Como ilustración de la teoría que hemos desarrollado, calcularemos los caracteres irreducibles (ordinarios y modulares) del grupo de permutaciones Σ_4.

Caracteres ordinarios de Σ_4 La tabla de caracteres de Σ_4 es la siguiente:

	1	(a,b)	$(ab)(cd)$	(abc)	$(abcd)$
	1	6	3	8	6
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

Hemos indicado el cardinal de cada clase de conjugación para facilitar el cálculo de la forma bilineal. La tabla puede calcularse como sigue:

a) El carácter χ_1 es el carácter trivial.

b) El carácter χ_2 es el homomorfismo dado por la signatura, que toma el valor 1 sobre las permutaciones pares y -1 sobre las impares.

c) Consideramos la acción $\rho : G \longrightarrow \mathrm{Aut}(\mathbb{C}^4)$ que permuta los vectores de la base canónica. Claramente, las matrices de ρ en la base canónica están

formadas por ceros y unos, y la diagonal de $\rho(\sigma)$ tiene tantos unos como elementos fije σ. Así pues, su carácter χ cumple que $\chi(\sigma)$ es el número de elementos fijados por σ. Concretamente:

	1	(a,b)	$(ab)(cd)$	(abc)	$(abcd)$
χ	4	2	0	1	0

Obviamente, χ no es irreducible, pues $\langle(1,1,1,1)\rangle$ es un subespacio invariante de $\mathbb{C}^4$, que determina la representación trivial, pero esto implica que $\chi_4 = \chi - 1$ es un carácter, y calculando $\langle\chi_4, \chi_4\rangle = 1$ vemos que es irreducible.

d) El producto $\chi_5 = \chi_2\chi_4$ es también un carácter y, como $\chi_4 = \chi_5\chi_2$, ha de ser irreducible.

e) El carácter χ_3 ha de tener grado 2, y puede deducirse entonces de 2.23 comparando la primera columna con las restantes.

La tabla de caracteres modulares respecto de cualquier primo $p \neq 2, 3$ es la misma tabla de caracteres ordinarios.

Caracteres módulo 2 El grupo Σ_4 tiene dos clases de conjugación 2-regulares, a saber, la clase de 1 y la de los ciclos (abc). Por lo tanto, hay dos caracteres modulares irreducibles. Por el teorema de Fong-Swan, los caracteres irreducibles módulo 2 se han de encontrar entre las reducciones de los caracteres irreducibles ordinarios, que se obtienen restringiéndolos a las clases 2-regulares. Vemos entonces que las restricciones cumplen

$$\chi_2 = \chi_1, \quad \chi_4 = \chi_1 + \chi_3, \quad \chi_5 = \chi_1 + \chi_3,$$

luego los caracteres modulares irreducibles han de ser $\phi_1 = \chi_1$ y $\phi_2 = \chi_3$. La tabla es, pues,

	1	(abc)
ϕ_1	1	1
ϕ_2	2	-1

y las relaciones

$$\chi_1 = \phi_1, \quad \chi_2 = \phi_1, \quad \chi_3 = \phi_2, \quad \chi_4 = \phi_1 + \phi_2, \quad \chi_5 = \phi_1 + \phi_2$$

nos dan la matriz de descomposición

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

La matriz traspuesta nos da los caracteres modulares de los módulos proyectivos:

$$\Phi_1 = \chi_1 + \chi_2 + \chi_4 + \chi_5, \quad \Phi_2 = \chi_3 + \chi_4 + \chi_5.$$

Multiplicando D^tD obtenemos la matriz de Cartan:

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

que nos da las expresiones de Φ_1 y Φ_2 en términos de los caracteres modulares:

$$\Phi_1 = 4\phi_1 + 2\phi_2, \qquad \Phi_2 = 2\phi_1 + 4\phi_2.$$

Así, por ejemplo, la envoltura proyectiva del módulo trivial tiene dimensión 8 y seis factores de composición, cuatro triviales y dos isomorfos al módulo simple de dimensión 2.

Caracteres módulo 3 El grupo Σ_4 tiene cuatro clases de conjugación 3-regulares, luego hay otros tantos caracteres irreducibles módulo 3. Al reducir los caracteres ordinarios obtenemos la relación $\chi_3 = \chi_1 + \chi_2$, luego χ_3 no es irreducible. Como, por el teorema de Fong-Swan, los caracteres irreducibles módulo 3 han de aparecer entre las reducciones de los caracteres ordinarios, han de ser los cuatro restantes. Por consiguiente, la tabla es

	1	(ab)	$(ab)(cd)$	$(abcd)$
ϕ_1	1	1	1	1
ϕ_2	1	−1	1	−1
ϕ_3	3	1	−1	−1
ϕ_4	3	−1	−1	1

Las matrices de descomposición y de Cartan resultan ser

$$D = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \qquad C = \begin{pmatrix} 2 & 1 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Y los caracteres modulares proyectivos son

$$\Phi_1 = \chi_1 + \chi_3 = 2\phi_1 + \phi_2, \quad \Phi_2 = \chi_2 + \chi_3 = \phi_1 + 2\phi_2,$$

$$\Phi_3 = \chi_4 = \phi_3, \quad \Phi_4 = \chi_5 = \phi_4.$$

■

Apéndice A

Las representaciones de Artin y Swan

Aquí vamos a estudiar (indirectamente, a través de sus caracteres) dos representaciones asociadas a grupos de Galois de extensiones de cuerpos métricos discretos completos. La construcción de estos caracteres se apoya en resultados nada triviales de la teoría de la ramificación, que recordaremos en la primera sección. Conviene destacar que la construcción de los caracteres (que llevamos a cabo en la sección segunda) sólo requiere la teoría de representaciones ordinarias desarrollada en el capítulo II. En la sección siguiente usaremos los resultados del capítulo IV para demostrar que la representación de Swan puede obtenerse a partir de un $\mathbb{Z}_l$-módulo proyectivo, lo cual nos permitirá a su vez asociar un invariante a ciertos módulos, a partir del cual se define, por ejemplo, el conductor de una curva elíptica.

A.1 Preliminares sobre cuerpos completos

Necesitamos recordar algunos hechos sobre la aritmética de los cuerpos métricos discretos y completos.[1]

NOTA: *A lo largo de este apéndice, salvo que se indique lo contrario, se sobrentenderá que K es un cuerpo métrico discreto y completo de característica 0 cuyo cuerpo de restos es perfecto de característica p.*

Llamaremos D al anillo de enteros de K y k a su cuerpo de restos. El hecho básico [GA 5.27] es que si K'/K es una extensión finita, el valor absoluto de K

[1]Todos los hechos que no demostraremos aquí están probados en mi libro de *Teoría de cuerpos de clases,* en lo sucesivo [CC], si bien figuran como requisitos previos, y no dependen de la teoría de cuerpos de clases propiamente dicha. Algunos resultados están demostrados allí en el contexto más general de dominios de Dedekind arbitrarios, por lo que, para comodidad del lector, remitiremos en algunas ocasiones a mi libro de *Geometría algebraica* [GA], donde están demostrados en el caso particular que aquí nos ocupa.

se extiende de forma única a un valor absoluto de K', con el cual se convierte también en un cuerpo métrico discreto completo. Que sea discreto se prueba en el teorema [GA 5.28], según el cual, la valoración de K' cumple la relación $v_{K'}|_K = ev_K$, para cierto número natural $e \geq 1$ llamado *índice de ramificación* de K'/K.

Llamemos D' y k' al anillo de enteros y el cuerpo de restos de K', respectivamente. Según [GA 5.30], la extensión k'/k es finita, y su grado f se llama *grado de inercia* de K'/K. La relación fundamental entre n, e y f es que $n = ef$ (por [GA 5.32]).

Si la extensión K'/K es finita de Galois, la unicidad de la extensión implica que cada $\sigma \in G(K'/K)$ conserva el valor absoluto (pues $|\alpha|_\sigma = |\sigma(\alpha)|$ es también un valor absoluto en K' que extiende al de K, luego ha de ser el valor absoluto de K'). Por consiguiente, σ induce un k-automorfismo $\bar{\sigma} \in G(k'/k)$. Como k es perfecto, la extensión k'/k es separable y por [CC 1.39] es de Galois, y además tenemos un epimorfismo de grupos[2]

$$G(K'/K) \longrightarrow G(k'/k).$$

El núcleo de este epimorfismo se llama *grupo de inercia* de la extensión, y es claramente

$$G_0(K'/K) = \{\sigma \in G(K'/K) \mid v(\sigma(\alpha) - \alpha) \geq 1 \text{ para todo } \alpha \in D'\}.$$

En particular, vemos que $|G_0(K'/K)| = e$.

Una extensión finita K'/K se dice *no ramificada* si $e = 1$. Se dice que es *dominadamente ramificada* si e no es divisible entre la característica p del cuerpo de restos. En caso contrario se dice que es *libremente ramificada.* En particular, las extensiones no ramificadas son dominadamente ramificadas.

Ahora hemos de recordar la teoría de la ramificación presentada en el capítulo X de [CC]. Allí está expuesta para el caso de los cuerpos numéricos y el de los cuerpos locales (las extensiones finitas de los cuerpos $\mathbb{Q}_p$ de números p-ádicos) para mostrar más fácilmente la relación entre ambos casos, pero es inmediato comprobar que todo lo dicho en el caso p-ádico es válido igualmente —sin cambio alguno en las demostraciones[3]— en el contexto general que estamos considerando aquí.

Si K'/K es una extensión finita de Galois, definimos sus *grupos de ramificación* como los grupos[4]

$$G_i(K'/K) = \{\sigma \in G(K'/K) \mid v(\sigma(\alpha) - \alpha) \geq i + 1 \text{ para todo } \alpha \in D'\},$$

[2]El grupo de descomposición $G_\mathfrak{P}$ que aparece en [CC 1.39] es todo $G(K'/K)$ en el caso que nos ocupa, porque K' sólo tiene un ideal primo.

[3]El teorema [CC 10.6] no es válido en este contexto general porque se apoya en que el cuerpo de restos es finito, pero no vamos a necesitar este hecho ni se usa en los teorema siguientes de [CC]. Podría parecer que la prueba de [CC 10.5] usa también la finitud del cuerpo de restos, pero no es cierto: sólo requiere el hecho de que todo subgrupo finito del grupo multiplicativo de un cuerpo es cíclico (pues, si el grupo tiene orden n, ha de ser el grupo de las raíces n-simas de la unidad, que es cíclico).

[4]En [CC 10.1] están definidos en un contexto más general. En el caso local, el grupo de descomposición $G_\mathfrak{P}$ es todo el grupo de Galois $G(K'/K)$.

donde D' es el anillo de enteros de K'. Observemos que $G_{-1}(K'/K) = G(K'/K)$ y que $G_0(K'/K)$ es el grupo de inercia que ya habíamos definido. Llamaremos g_i al orden del grupo $G_i(K'/K)$.

El teorema [CC 10.4] afirma que todos los grupos $G_i(K'/K)$ son subgrupos normales de $G(K'/K)$, y que existe un i tal que $G_i(K'/K) = 1$. Así pues, forman una serie

$$1 = G_i \trianglelefteq G_{i-1} \trianglelefteq \cdots \trianglelefteq G_0 \trianglelefteq G(K'/K).$$

Si descomponemos el índice de ramificación $e = p^s e_0$, donde $p \nmid e_0$, sabemos que $g_0 = e$, y el teorema [CC 10.5] nos da que $g_1 = p^s$, de modo que $G_1(K'/K)$ es el p-subgrupo de Sylow del grupo de inercia $G_0(K'/K)$. En particular, la extensión K'/K es dominadamente ramificada si y sólo si $G_1(K'/K) = 1$.

Si $D' = D[\alpha_1, \ldots, \alpha_n]$, es fácil ver que

$$G_i(K'/K) = \{\sigma \in G(K'/K) \mid v(\sigma(\alpha_j) - \alpha_j) \geq i+1 \text{ para } j = 1, \ldots, n\}.$$

El teorema [CC 3.12] nos da que existe un $\alpha \in D'$ tal que $D' = D[\alpha]$ y, por consiguiente,

$$G_i(K'/K) = \{\sigma \in G(K'/K) \mid v_{K'}(\sigma(\alpha) - \alpha) \geq i+1\}.$$

De aquí se sigue que la función $i_{K'/K} : G(K'/K) \longrightarrow \mathbb{N} \cup \{\infty\}$ dada por

$$i_{K'/K}(\sigma) = v_{K'}(\alpha^\sigma - \alpha).$$

es independiente de la elección del generador $\alpha \in D'$, pues es igual al máximo número natural i tal que $\sigma \in G_{i-1}(K'/K)$. En términos de esta función, tenemos que[5]

$$G_i(K'/K) = \{\sigma \in G(K'/K) \mid i_{K'/K}(\sigma) \geq i+1\}.$$

El hecho de que $G_i(K'/K) = 1$ para i suficientemente grande se traduce en que

$$i_{K'/K}(\sigma) = \infty \quad \text{si y sólo si} \quad \sigma = 1.$$

Similarmente, el hecho de que los grupos de ramificación sean normales en $G(K'/K)$ se traduce en que

$$i_{K'/K}(\tau^{-1}\sigma\tau) = i_{K'/K}(\sigma), \qquad \text{para todo } \sigma, \tau \in G(K'/K).$$

Otra propiedad elemental es la siguiente:

$$i_{K'/K}(\sigma\tau) \geq \text{mín}\{i_{K'/K}(\sigma), i_{K'/K}(\tau)\}.$$

En efecto:

$$i_{K'/K}(\sigma\tau) = v(\alpha^{\sigma\tau} - \alpha) = v(\alpha^{\sigma\tau} - \alpha^\sigma + \alpha^\sigma - \alpha)$$
$$\geq \text{mín}\{v(\alpha^{\sigma\tau} - \alpha^\sigma), v(\alpha^\sigma - \alpha)\} = \text{mín}\{i_{K'/K}(\tau), i_{K'/K}(\sigma)\}.$$

■

El teorema [CC 10.16] se traduce en una propiedad más de la función $i_{K'/K}$:

[5] En virtud de [CC 10.3], también podemos calcular la función $i_{K'/K}$ con $\alpha = \pi$, donde π es un primo de K', aunque no genere el anillo de enteros.

Teorema A.1 *Sea $k \subset L \subset K$ una cadena de extensiones de Galois de cuerpos locales. Entonces, para cada $\sigma \in G(L/k)$, se cumple que*

$$i_{L/k}(\sigma|_L) = \frac{1}{e_{K/L}} \sum_{\tau \in G(K/L)} i_{K/k}(\tau\sigma).$$

DEMOSTRACIÓN: Sea α (resp. β) un generador del anillo de enteros de K (resp. de L) sobre el anillo de enteros de k. El teorema [CC 10.16] afirma que

$$v_L(\sigma(\beta) - \beta) = \sum_{\tau \in G(K/L)} v_L((\tau\sigma)(\alpha) - \alpha),$$

y esto equivale a que

$$e_{K/L}\, i_{L/k}(\sigma|_L) = \sum_{\tau \in G(K/L)} i_{K/k}(\tau\sigma).$$

■

A.2 El carácter de Artin

De aquí en adelante L/K será una extensión finita de Galois, llamaremos $G = G(L/K)$ a su grupo de Galois y $G_i = G_i(L/K)$ a sus grupos de ramificación. Representaremos por g y g_i sus órdenes respectivos.

La función $i_{L/K} : G \longrightarrow \mathbb{N} \cup \{\infty\}$ que acabamos de definir es una función de clases en G excepto por el hecho de que no está definida en $\sigma = 1$. Vamos a corregir esto:

Definición A.2 La *función de Artin* $a_{L/K} : G(L/K) \longrightarrow \mathbb{Z}$ es la función dada por

$$a_{L/K}(\sigma) = -f\, i_{L/K}(\sigma) \quad \text{si } \sigma \neq 1, \quad a_{L/K}(1) = f \sum_{\sigma \neq 1} i_{L/K}(\sigma),$$

donde f es el grado de inercia de la extensión L/K.

Es claro que $a_{L/K}$ es una función de clases en $G(L/K)$. Hemos definido $a_{L/K}(1)$ para que se cumpla que

$$\sum_{\sigma \in G} a_{L/K}(\sigma) = 0,$$

es decir, que[6] $(a_{L/K}, 1) = 0$.

El valor $a_{L/K}(1)$ tiene una interpretación aritmética. Para obtenerla observamos que $i_{L/K}$ toma el valor i sobre los elementos de $G_{i-1} \setminus G_i$, luego, si $g_t = 1$, tenemos que

$$\sum_{\sigma \neq 1} i_{L/K}(\sigma) = (g_0 - g_1) + 2(g_1 - g_2) + 3(g_2 - g_3) + \cdots + t(g_{t-1} - 1)$$

$$= g_0 + g_1 + \cdots + g_{t-1} - t = \sum_{i=0}^{\infty} (g_i - 1).$$

[6]De este modo, si una función de clases ϕ coincide con $a_{L/K}$ salvo quizá para $\sigma = 1$ y cumple $(\phi, 1) = 0$, entonces $\phi = a_{L/K}$.

El teorema [CC 10.11] nos da inmediatamente el resultado siguiente:

Teorema A.3 *Si $\mathfrak{D}_{L/K}$ es el diferente de la extensión L/K, entonces*

$$a_{L/K}(1) = f v_L(\mathfrak{D}_{L/K}).$$

De la propia definición de la función de Artin se sigue que, $a_{L/K} = 0$ si y sólo si la extensión L/K es no ramificada. El propósito de esta sección es demostrar el teorema siguiente:

Teorema A.4 *Si L/K es ramificada, la función $a_{L/K}$ es un carácter del grupo de Galois $G(L/K)$.*

Como $a_{L/K}$ es una función de clases, el teorema 2.17 nos da que es combinación lineal de los caracteres irreducibles de G, y el coeficiente de cada carácter χ es $(a_{L/K}, \chi)$. Teniendo en cuenta que $a_{L/K} \neq 0$, basta probar que estos coeficientes son números naturales. Observamos que

$$(a_{L/K}, \chi) = \frac{1}{g}\sum_{\sigma\in G} a_{L/K}(\sigma)\chi(\sigma^{-1}) = \frac{1}{g}\sum_{\sigma\in G} \chi(\sigma)\, a_{L/K}(\sigma^{-1})$$

$$= \frac{1}{g}\sum_{\sigma\in G} \chi(\sigma)\,\overline{a_{L/K}(\sigma)} = (\chi, a_{L/K}),$$

donde hemos usado que $a_{L/K}(\sigma^{-1}) = a_{L/K}(\sigma) = \overline{a_{L/K}(\sigma)}$.

Para cada función de clases ϕ de G, definimos

$$f(\phi) = (\phi, a_{L/K}).$$

El teorema A.4 quedará probado si demostramos que $f(\chi)$ es un número natural para todo carácter χ de G.

Para cada $i \geq 0$, llamamos r_{G_i} al carácter regular del grupo de ramificación i-ésimo G_i. Sabemos que en la descomposición de r_{G_i} en suma de caracteres irreducibles aparece cada carácter irreducible con multiplicidad igual a su grado. Por consiguiente, $u_i = r_{G_i} - 1_{G_i}$ es también un carácter de G_i, salvo que sea $G_i = 1$, en cuyo caso $u_i = 0$. Esto sucede para todo i suficientemente grande.

Teorema A.5 *En las condiciones anteriores, se cumple que*

$$a_{L/K} = \sum_{i=0}^{\infty} \frac{g_i}{g_0}\, u_i^G.$$

Demostración: Tenemos que

$$u_i^G(\sigma) = \frac{1}{g_i}\sum_{\tau\in G} u_i^0(\tau\sigma\tau^{-1}).$$

Teniendo en cuenta que G_i es un subgrupo normal en G y que $u_i(\sigma) = -1$ para todo $\sigma \neq 1$, es claro que

$$u_i^G(\sigma) = \begin{cases} \frac{g(g_i-1)}{g_i} & \text{si } \sigma = 1 \\ -g/g_i & \text{si } \sigma \in G_i \setminus \{1\}, \\ 0 & \text{si } \sigma \in G \setminus G_i. \end{cases}$$

Por lo tanto,

$$\frac{g_i}{g_0} u_i^G(\sigma) = \begin{cases} f(g_i-1) & \text{si } \sigma = 1 \\ -f & \text{si } \sigma \in G_i \setminus \{1\}, \\ 0 & \text{si } \sigma \in G \setminus G_i. \end{cases}$$

Así, si $\sigma \in G_k \setminus G_{k+1}$, la suma para todo i es igual a

$$-f(k+1) = -f i_{L/K}(\sigma) = a_{L/K}(\sigma).$$

Ahora observamos que

$$\sum_{\sigma \in G} u_i^G(\sigma) = 0,$$

y lo mismo vale si sumamos para todo i. Como $a_{L/K}$ cumple también que $(a_{L/K}, 1) = 0$, también se tiene la igualdad para $\sigma = 1$. ∎

De aquí extraemos varias consecuencias. En primer lugar, vemos que $g_0 a_{L/K}$ es un carácter de G. Por consiguiente, si χ es un carácter de G, se cumple que $(\chi, g_0 a_{L/K})$ es un número natural. Equivalentemente:

Teorema A.6 *Si χ es un carácter de G, se cumple que $f(\chi)$ es un número racional ≥ 0.*

Para cada función de clases ϕ en G, definimos

$$\phi(G_i) = \frac{1}{g_i} \sum_{\sigma \in G_i} \phi(\sigma).$$

En estos términos se cumple lo siguiente:

Teorema A.7 *Si ϕ es una función de clases en G, entonces*

$$f(\phi) = \sum_{i=0}^{\infty} \frac{g_i}{g_0} (\phi(1) - \phi(G_i)).$$

Demostración: Basta tener en cuenta que

$$(\phi, u_i^G) = (\phi|_{G_i}, u_i) = \phi(1) - \phi(G_i).$$

∎

Teorema A.8 *Sea $\rho : G \longrightarrow \mathrm{Aut}(V)$ una representación de G sobre $\mathbb{C}$ con carácter χ, y sea V^{G_i} el subespacio formado por los elementos de V fijados por cada elemento de G_i. Entonces*

$$f(\chi) = \sum_{i=0}^{\infty} \frac{g_i}{g_0} \dim(V/V^{G_i}).$$

DEMOSTRACIÓN: Observemos que V^{G_1} es el $\mathbb{C}[G_i]$-submódulo de V asociado al carácter trivial 1_{G_i} en la descomposición dada por el teorema 2.19. Por consiguiente, su dimensión es la multiplicidad de 1_{G_i} en $\chi|_{G_i}$, es decir:

$$\dim V^{G_i} = (\chi|_{G_i}, 1_{G_i}) = \chi(G_i).$$

Por otra parte, $\dim V = \chi(1)$, con lo que $\dim V/V^{G_i} = \chi(1) - \chi(G_i)$ y basta aplicar el teorema anterior. ∎

Seguidamente reformulamos el teorema A.1:

Teorema A.9 *Sea $K \subset K' \subset L$ una cadena de extensiones de Galois. Llamemos $N = G(L/K')$, de modo que $G/N \cong G(K'/K)$. Entonces,*

$$a_{K'/K} = a_{L/K}^{G/N}.$$

DEMOSTRACIÓN: Tomemos un $\sigma \in G$, de modo que $\sigma|_{K'}$ se identifica con $N\sigma \in G/N$. De acuerdo con 2.51, la igualdad $a_{K'/K}(N\sigma) = a_{L/K}^{G/H}(N\sigma)$ equivale a

$$a_{K'/K}(N\sigma) = \frac{1}{n_{L/K'}} \sum_{n\in N} a_{L/K}(n\sigma).$$

Si $\sigma \notin N$, esto equivale a su vez a que

$$-f_{K'/K}\, i_{K'/K}(\sigma|_{K'}) = \frac{1}{e_{L/K'} f_{L/K'}} \sum_{n\in N} (-f_{L/K}) i_{L/K}(n\sigma),$$

lo cual, simplificando, se reduce a

$$i_{K'/K}(\sigma|_{K'}) = \frac{1}{e_{L/K'}} \sum_{n\in N} i_{L/K}(n\sigma),$$

que es precisamente lo que afirma el teorema A.1. Falta probar la igualdad cuando $\sigma|_{K'} = 1$, pero ésta es consecuencia inmediata de que

$$(a_{L/K}^{G/N}, 1_{G/N}) = (a_{L/K}, 1_G) = 0.$$

∎

Ahora relacionamos la función $a_{L/K}$ con $a_{L/K'}$.

Teorema A.10 *Sea $K \subset K' \subset L$ una cadena de extensiones tal que L/K es de Galois y sea $H = G(L/K')$. Entonces*

$$a_{L/K}|_H = v_K(\Delta_{K'/K}) r_H + f_{K'/K}\, a_{L/K'},$$

donde $\Delta_{K'/K}$ es el discriminante de K'/K y r_H es el carácter regular de H.

DEMOSTRACIÓN: Si $\sigma \in G$ cumple $\sigma \neq 1$, entonces

$$a_{L/K}(\sigma) = -f_{L/K}\, i_{L/K}(\sigma), \quad a_{L/K'}(\sigma) = -f_{L/K'}\, i_{L(K')}(\sigma), \quad r_H(\sigma) = 0.$$

Además, un generador del anillo de enteros de L sobre el anillo de enteros de K lo genera también sobre el anillo de enteros de K', luego $i_{L/K}(\sigma) = i_{L/K'}(\sigma)$. Ahora es claro que la igualdad del enunciado se cumple para σ. Falta considerar el caso $\sigma = 1$. Teniendo en cuenta el teorema A.3, la igualdad que hemos de probar es equivalente a

$$f_{L/K}\, v_L(\mathcal{D}_{L/K}) = |L : K'| v_K(\Delta_{K'/K}) + f_{K'/K} f_{L/K'}\, v_L(\mathcal{D}_{L/K'}).$$

Según [CC 3.22], el discriminante de una extensión es la norma del diferente, lo cual implica que

$$v_K(\Delta_{L/K}) = f_{L/K}\, v_L(\mathcal{D}_{L/K}), \qquad v_{K'}(\Delta_{L/K'}) = f_{L/K'}\, v_L(\mathcal{D}_{L/K'}).$$

Así pues, la ecuación que hemos de probar equivale a

$$v_K(\Delta_{L/K}) = |L : K'| v_K(\Delta_{K'/K}) + f_{K'/K}\, v_{K'}(\Delta_{L/K'}).$$

A su vez, esta fórmula equivale al teorema [CC 3.24]. ∎

Como consecuencia:

Teorema A.11 *Sea $K \subset K' \subset L$ una cadena de extensiones tal que L/K es de Galois. Sea $H = G(L/K')$. Entonces, para todo carácter ψ de H,*

$$f(\psi^G) = v_K(\Delta_{K'/K})\psi(1) + f_{K'/K} f(\psi).$$

DEMOSTRACIÓN: Hay que entender que la última f de la fórmula es la función correspondiente a la extensión L/K'.

$$\begin{aligned} f(\psi^G) = (\psi^G, a_{L/K}) = (\psi, a_{L/K}|_H) &= v_K(\Delta_{K'/K})(\psi, r_H) + f_{K'/K}(\psi, a_{L/K'}) \\ &= v_K(\Delta_{K'/K})\psi(1) + f_{K'/K}\, f(\psi). \end{aligned}$$

∎

Ahora consideramos la función $\phi_{L/K}$ definida en [CC 10.18]:

Teorema A.12 *Sea χ un carácter de grado 1 en G y sea $c(\chi)$ el mayor número natural tal que $\chi|_{G_{c(\chi)}} \neq 1$. (Si $\chi = 1_G$, tomamos $c(\chi) = -1$.) Entonces,*

$$f(\chi) = \phi_{L/K}(c(\chi)) + 1.$$

DEMOSTRACIÓN: Si $i \leq c(\chi)$, entonces $\chi(G_i) = (\chi|_{G_i}, 1) = 0$ (porque $\chi|_{G_i}$ tiene grado 1, luego es irreducible). Por lo tanto, $\chi(1) - \chi(G_i) = 1$. Si $i > c(\chi)$, entonces $\chi(G_i) = 1$, luego $\chi(1) - \chi(G_i) = 0$. El teorema A.7 nos da que

$$f(\chi) = \sum_{i=0}^{c(\chi)} \frac{g_i}{g_0} = \phi(c(\chi)) + 1.$$

Teorema A.13 *Sea χ un carácter de grado 1 en G, sea N su núcleo y sea K' su cuerpo fijado. Sea $c'(\chi)$ el mayor número natural tal que $(G/N)_{c'(\chi)} \neq 1$. Entonces $f(\chi) = \phi_{K'/K}(c'(\chi)) + 1$ es un número natural.*

Demostración: El teorema [CC 10.19] afirma que

$$(G/N)_i = G_{\psi_{L/K'}(i)}N/N,$$

donde $\psi_{L/K'}$ es la función de Hasse (la inversa de $\phi_{L/K'}$). Por tanto, $(G/N)_i = 1$ equivale a que $G_{\psi_{L/K'}(i)} \leq N$, es decir, a que $\chi|_{G_{\psi_{L/K'}(i)}} = 1$. Por consiguiente, $c(\chi) = \psi_{L/K'}(c'(\chi))$ o, equivalentemente, $c'(\chi) = \phi_{L/K'}(c(\chi))$. El teorema anterior y [CC 10.20] nos dan que

$$f(\chi) = \phi_{L/K}(c(\chi)) + 1 = \phi_{K'/K}(\phi_{L/K'}(c(\chi))) + 1 = \phi_{K'/K}(c'(\chi)) + 1.$$

Por último, la extensión K'/K es abeliana, luego podemos aplicar el teorema [CC 10.25]: el número natural $c'(\chi)$ cumple que $G(K'/K)_{c'(\chi)} \neq 1$ y $G(K'/K)_{c'(\chi)+1} = 1$, luego es un vértice de la función $\phi_{K'/K}$, luego $\phi_{K'/K}(c'(\chi))$ es un vértice de $\psi_{K'/K}$, luego es un número entero ≥ -1. (La función $\psi_{K'/K}$ es lineal hasta -1, luego su primer vértice es ≥ -1.) ∎

Finalmente estamos en condiciones de demostrar el teorema A.4:

Hemos de probar que $f(\chi)$ es un número natural para todo carácter χ de G. Por el teorema A.6 sabemos que $f(\chi)$ es un número racional ≥ 0, luego sólo necesitamos probar que es entero. Por el teorema de Brauer 2.41, podemos expresar

$$\chi = \sum_i n_i \psi_i^G,$$

donde $n_i \in \mathbb{Z}$ y cada ψ_i es un carácter de grado 1 en un cierto subgrupo H_i de G. Por consiguiente, basta probar que $f(\psi_i^G)$ es entero. Por A.11, basta probar que $f(\psi_i)$ es entero, lo que equivale a suponer que χ tiene grado 1. En tal caso basta aplicar el teorema anterior. ∎

A partir del carácter de Artin podemos definir otro que, de hecho, es el que más nos va a interesar:

Definición A.14 Si L/K es una extensión finita de Galois, definimos la *función de Swan* $s_{L/K} : G(L/K) \longrightarrow \mathbb{Z}$ como la función dada por

$$s_{L/K} = a_{L/K} - u_0^G = \sum_{i=1}^{\infty} \frac{g_i}{g_0}\, u_i^G,$$

donde $u_i = r_{G_i} - 1_{G_i}$. (Véase el teorema A.5.)

Explícitamente:

$$s_{L/K}(\sigma) = \begin{cases} f(1 - i(\sigma)) & \text{si } \sigma \in G_0 \setminus 1, \\ 0 & \text{si } \sigma \in G \setminus G_0, \end{cases}$$

y $s_{L/K}(1)$ está determinado por la relación $(s_{L/K}, 1_G) = 0$, que se cumple porque $(a_{L/K}, 1_G) = 0$ y $(u_0^G, 1_G) = (u_0, 1_{G_0}) = 0$.

Es claro entonces que $s_{L/K} = 0$ si y sólo si $G_1 = 1$, es decir, si la extensión L/K es dominadamente ramificada. En caso contrario es una función de clases no nula. Consideremos un carácter irreducible χ de G, y observemos que

$$(s_{L/K}, \chi) = \sum_{i=1}^{\infty} \frac{g_i}{g_0} (u_i^G, \chi) = \sum_{i=1}^{\infty} \frac{g_i}{g_0} (u_i, \chi_{G_i}) \geq 0.$$

Por otra parte, $(s_{L/K}, \chi) = (a_{L/K}, \chi) - (u_0^G, \chi) \in \mathbb{Z}$, puesto que $a_{L/K}$ y u_0^G son caracteres. Concluimos que $(s_{L/K}, \chi)$ es un número natural para todo χ, luego $s_{L/K}$ es un carácter de G, el *carácter de Swan* de la extensión L/K.

A.3 Realización de los caracteres

Aunque los caracteres de Artin y Swan toman valores en $\mathbb{Z}$, existen ejemplos cuyas representaciones correspondientes no son realizables sobre $\mathbb{Q}$, ni siquiera sobre $\mathbb{R}$. Sin embargo, se cumple lo siguiente (manteniendo la notación de la sección anterior):

Teorema A.15 *Si l es un primo distinto de la característica p del cuerpo de restos k, entonces las representaciones de Artin y Swan son realizables sobre el cuerpo $\mathbb{Q}_l$ de los números l-ádicos.*

Notemos que basta probar el teorema para la representación de Swan, puesto que

$$a_{L/K} = s_{L/K} + r_{G_0}^G - 1_{G_0}^G,$$

y las representaciones r_{G_0} y 1_{G_0} son realizables sobre cualquier cuerpo, luego también las representaciones inducidas en G. Para la representación de Swan podemos demostrar algo más preciso todavía:

Teorema A.16 *Si l es un primo distinto de la característica p del cuerpo de restos k, existe un $\mathbb{Z}_l[G]$-módulo proyectivo finitamente generado $S_{L/K}^l$, único salvo isomorfismo, tal que $S_{L/K}^l \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ determina el carácter de Swan.*

Demostración: Vamos a aplicar el teorema 4.42 tomando $K = \mathbb{Q}_l$ y como K' una extensión finita de K suficientemente grande para G. De este modo, el carácter de Swan es realizable sobre K', y su representación asociada determina un elemento $x \in R_{K'}(G)$. Ciertamente, se cumple la condición a) del teorema, pues el carácter de x (el carácter de Swan) toma valores en $\mathbb{Z}$, luego en $\mathbb{Q}_l$.

Demostramos la condición b) tomando como n el orden g_0 del grupo de inercia G_0. Usamos que

$$g_0 s_{L/K} = \sum_{i=1}^{\infty} g_i u_i^G.$$

Los grupos de ramificación G_i son p-grupos, luego el teorema 4.27 nos da que los homomorfismos c, d, e para G_i y K' son isomorfismos. Más concretamente, tenemos que c puede identificarse con la identidad en $R_{k'}(G_i)$ y d y e son isomorfismos mutuamente inversos. Esto implica que existe un $D'[G_i]$-módulo proyectivo finitamente generado P_i tal que $P_i \otimes_{D'} K'$ determina el carácter u_i.

El $D'[G]$-módulo $Q_i = P_i \otimes_{D'[G_i]} D'[G]$ también es proyectivo y

$$(P_i \otimes_{D'[G_i]} D'[G]) \otimes_{D'} K' \cong P_i \otimes_{D'[G_i]} K'[G] \cong P_i \otimes_{D'[G_i]} K'[G_i] \otimes_{K'[G_i]} K'[G]$$

$$(P_i \otimes_{D'[G_i]} \otimes D'[G_i] \otimes_{D'} K') \otimes_{K'[G_i]} K'[G] \cong (P_i \otimes_{D'} K') \otimes_{K'[G_i]} K'[G],$$

luego $Q_i \otimes_{D'} K'$ determina el carácter u_i^G. Si llamamos V a la suma directa de los $D'[G]$-módulos Q_i repetidos g_i veces cada uno, tenemos que V es un $D'[G]$-módulo proyectivo que cumple $x = [V \otimes_{D'} K']$, tal y como exige el apartado b) del teorema 4.42. ∎

Observemos que si la extensión L/K tiene ramificación dominada, entonces $s_{L/K}$ no es un carácter, sino la función nula y, por consiguiente, $S^l_{L/K} = 0$.

A.4 El invariante de Swan

Como en las secciones precedentes, sea K un cuerpo métrico discreto completo de característica 0 con cuerpo de restos k perfecto y de característica prima p, sea L/K una extensión finita de Galois con grupo de Galois G y sea l un número primo distinto de p. Llamaremos $F = \mathbb{Z}/l\mathbb{Z}$, al que podemos identificar con el cuerpo de restos del cuerpo $\mathbb{Q}_l$ de los números l-ádicos.

Definición A.17 Para cada $F[G]$-módulo finitamente generado M, definimos el *invariante de Swan* de M como el número natural

$$\delta(K, M) = \langle [\overline{S}^l_{L/K}], [M] \rangle_F = \dim_F \mathrm{Hom}_{F[G]}(\overline{S}^l_{L/K}, M)$$

$$= \mathrm{rang}_{\mathbb{Z}_l} \mathrm{Hom}_{\mathbb{Z}_l[G]}(S^l_{L/K}, M),$$

donde $\overline{S}^l_{L/K} = S^l_{L/K} \otimes_{\mathbb{Z}_l} F$ es la reducción de $S^l_{L/K}$-módulo l. La última igualdad se sigue del teorema 1.53, teniendo en cuenta que $M \otimes_{\mathbb{Z}_l} F \cong M/lM = M$ y que $\mathrm{Hom}_{\mathbb{Z}_l[G]}(S^l_{L/K}, M)$ es un $\mathbb{Z}_l$-módulo libre (véase la prueba del teorema 4.26).

La notación $\delta(K, M)$ requiere cierta justificación. En lugar de partir de un $F[G]$-módulo M, podríamos haber considerado un F-espacio vectorial de dimensión finita M junto con un homomorfismo

$$\rho : G(\overline{K}/K) \longrightarrow \mathrm{Aut}(M),$$

(donde $\overline{K}$ es la clausura algebraica de K) cuyo núcleo contenga un subgrupo[7] de la forma $G(\overline{K}/L)$, para cierta extensión finita de Galois L/K. En tal caso,

[7]Esta condición equivale a que ρ sea una aplicación continua, considerando en $G(\overline{K}/K)$ la topología de Krull y en $\mathrm{Aut}(M)$ la topología discreta.

ρ induce una representación lineal $\rho_L : G(L/K) \longrightarrow \mathrm{Aut}(M)$ que, a su vez, induce en M una estructura de $F[G]$-módulo. Es claro que todo $F[G]$-módulo puede obtenerse de esta forma. Sucede entonces que $\delta(K, M)$ depende de ρ, pero no de la elección de L. Si consideramos a M como $F[G]$-módulo (donde $G = G(\overline{K}/K)$ y $F[G]$ se define igual que cuando G es finito), podemos decir que $\delta(K, M)$ depende únicamente de K y de M. (La dependencia de l está implícita la dependencia de M, pues —salvo que M sea nulo— es claro que l es el único primo que cumple $lM = 0$.)

Teorema A.18 *Consideremos un F-espacio vectorial M de dimensión finita y sea $\rho : G(\overline{K}/K) \longrightarrow Aut(M)$ un homomorfismo de grupos cuyo núcleo contenga un subgrupo de la forma $G(\overline{K}/L)$, para cierta extensión finita de Galois L/K. Entonces, el valor de $\delta(K, M)$ correspondiente a la estructura de $F[G]$-módulo de M (donde $G = G(L/K)$), es independiente de la elección de L.*

Demostración: Basta probar que si $K \subset L \subset L'$, donde las extensiones L/K y L'/K son finitas de Galois, con grupos de Galois respectivos $G = G(L/K)$, $G' = G(L'/K)$, $N = G(L'/L)$ (de modo que $G = G'/N$) y M es un $F[G]$-módulo, considerado como $F[G']$-módulo de forma natural, entonces $\delta(K, M)$ es el mismo calculado con G o con G'.

Para ello partimos del teorema A.9, según el cual $a_{L/K} = a^G_{L'/K}$. Por otra parte,

$$s_{L/K} = a_{L/K} - r^G_{G_0} + 1^G_{G_0}, \qquad s_{L'/K} = a_{L'/K} - r^{G'}_{G'_0} + 1^{G'}_{G'_0},$$

Ahora bien, según [CC 10.19], el epimorfismo $G' \longrightarrow G$ se restringe a un epimorfismo $G'_0 \longrightarrow G_0$, y es claro que, para todo carácter χ de G'_0 se cumple que $(\chi^{G'})^G = (\chi^{G_0})^G$. En efecto, si V es un $F[G'_0]$-módulo con carácter χ, se cumple que

$$V \otimes_{F[G'_0]} F[G'] \otimes_{F[G']} F[G] = V \otimes_{F[G'_0]} F[G] = V \otimes_{F[G'_0]} F[G_0] \otimes_{F[G_0]} F[G]$$

Por otra parte, de la fórmula 2.51 se sigue inmediatamente que $r^{G_0}_{G'_0} = r_{G_0}$ y que $1^{G_0}_{G'_0} = 1_{G_0}$, luego

$$s^G_{L'/K} = a^G_{L'/K} - r^G_{G_0} + 1^G_{G_0} = s_{L/K}.$$

De aquí se desprende a su vez que el $\mathbb{Z}_l[G]$-módulo proyectivo

$$S = S_{L'/K} \otimes_{\mathbb{Z}_l[G']} \mathbb{Z}_l[G]$$

cumple que $S \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ genera el carácter $s_{L/K}$, luego, por la unicidad, ha de ser

$$S_{L/K} = S_{L'/K} \otimes_{\mathbb{Z}_l[G']} \mathbb{Z}_l[G].$$

El teorema 1.54 nos da el isomorfismo de $\mathbb{Z}_l$-módulos

$$\mathrm{Hom}_{\mathbb{Z}_l[G']}(S_{L'/K}, M) \cong \mathrm{Hom}_{\mathbb{Z}_l[G]}(S_{L/K}, M),$$

luego ambos miembros tienen el mismo rango. ∎

El hecho de que $\delta(K,M)$ dependa en realidad de la clase de M en $R_F(G)$ hace que $\delta(K,M)$ sea aditivo en M, en el sentido de que si

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

es una sucesión exacta de $F[G]$-módulos finitamente generados, se cumple que

$$\delta(K,M) = \delta(K,M') + \delta(K,M'').$$

Teorema A.19 *En las condiciones anteriores, si G_i es el grupo de ramificación i-ésimo de G, g_i es su orden y M^{G_i} es el submódulo de M fijado por G_i, se cumple que*

$$\delta(K,M) = \sum_{i=1}^{\infty} \frac{g_i}{g_0} \dim_F(M/M^{G_i})$$

DEMOSTRACIÓN: Como G_i es un p-grupo, los homomorfismos c, d, e son isomorfismos para G_i y el cuerpo $\mathbb{Q}_l$. Por consiguiente, podemos tomar un $\mathbb{Z}_l[G_i]$-módulo proyectivo P_i de manera que $P_i \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ determine el carácter $u_i = r_{G_i} - 1_{G_i}$ sobre $\mathbb{Q}_l$ y entonces $P_i \otimes_{\mathbb{Z}_l} F$ determina el mismo carácter sobre el cuerpo F (porque $d([P_i \otimes_{\mathbb{Z}_l} \mathbb{Q}_l]) = [P_i \otimes_{\mathbb{Z}_l} F]$). Sabemos que $(P_i \otimes_{\mathbb{Z}[G_i]} \mathbb{Z}[G]) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ determina el carácter u_i^G, luego

$$g_0 S^l_{L/K} = \bigoplus_{i=1}^{\infty} (P_i \otimes_{\mathbb{Z}_l[G_i]} \mathbb{Z}_l[G])^{g_i},$$

pues ambos miembros son proyectivos y determinan el carácter $gs_{L/K}$. Los teoremas 1.54 y 1.53 nos dan que

$$g_0\delta(K,M) = \sum_{i=1}^{\infty} g_i \mathrm{rang}_{\mathbb{Z}_l} \mathrm{Hom}_{\mathbb{Z}_l[G]}(P_i \otimes_{\mathbb{Z}_l[G_i]} \mathbb{Z}_l[G], M)$$

$$= \sum_{i=1}^{\infty} g_i \mathrm{rang}_{\mathbb{Z}_l} \mathrm{Hom}_{\mathbb{Z}_l[G_i]}(P_i, M) = \sum_{i=1}^{\infty} g_i \dim_F \mathrm{Hom}_{F[G_i]}(P_i \otimes_{\mathbb{Z}_l} F, M).$$

Si χ es el carácter de M como $F[G_i]$-módulo, el teorema 3.57 implica que

$$\dim_F \mathrm{Hom}_{F[G_i]}(P_i \otimes_{\mathbb{Z}_l} F, M) = \langle u_i, \chi\rangle_F = \langle r_{G_i}, \chi\rangle_F - \langle 1_{G_i}, \chi\rangle_F$$

$$= \dim_F M - \dim_F M^{G_i} = \dim_F(M/M^{G_i}).$$

■

Es frecuente encontrar la fórmula anterior como definición de $\delta(K,M)$, pero entonces no es evidente que sea un número natural. Ahora es inmediato que $\delta(K,M) = 0$ si y sólo si G_1 actúa trivialmente sobre M o, equivalentemente, si la extensión L/K se puede tomar dominadamente ramificada.

Apéndice B

Los caracteres de A_5

En este apéndice construimos las tablas de caracteres (ordinarios y modulares, sobre cuerpos de escisión) del grupo alternado A_5, que es el menor grupo simple no abeliano.

B.1 Un criterio de irreducibilidad

Para obtener los caracteres modulares de A_5 no podemos contar con el teorema de Fong-Swan, lo cual se traduce en que, al restringir los caracteres ordinarios a caracteres modulares, no tenemos la garantía ni de que los caracteres obtenidos sean irreducibles, ni de que entre ellos se encuentren todos los caracteres irreducibles. Por ello, en esta primera sección demostramos una condición suficiente de irreducibilidad que nos bastará para nuestro objetivo.

Teorema B.1 *Sea K un cuerpo local suficientemente grande para un grupo finito G, sea V un $K[G]$-módulo simple cuya dimensión sobre K sea divisible entre la mayor potencia de p que divide a $|G|$. Sea $R \subset V$ un retículo estable y sea $P = R \otimes_D k$. Entonces R es un $D[G]$-módulo proyectivo y P es un $k[G]$-módulo proyectivo simple.*

Demostración: Sean $V_1, \ldots, V_h$ representantes de las clases de isomorfía de $K[G]$-módulos simples. El teorema de Wedderburn 3.16 nos da la descomposición

$$K[G] \cong A_1 \oplus \cdots \oplus A_h \cong \mathrm{End}_K(V_1) \oplus \cdots \oplus \mathrm{End}_K(V_h),$$

donde el isomorfismo de anillos $A_i \cong \mathrm{End}_K(V_i)$ es el que a cada $x \in A_i$ le asigna la multiplicación por x en V_i. (Aquí hemos usado que K es un cuerpo de escisión para G, por lo que $\mathrm{End}_{K[G]}(V_i) \cong K$.) Si descomponemos $1 = e_1 + \cdots + e_h$, entonces e_i es la unidad de A_i, y el teorema 3.55 nos da la expresión

$$e_i = \frac{\chi_i(1)}{|G|} \sum_{\sigma \in G} \chi_i(\sigma^{-1})\sigma.$$

Observemos que e_i es el elemento de A_i tal que la multiplicación por e_i en V_i es la identidad. Más en general, dado $\tau \in G$, tenemos que $\tau = e_i\tau + (1-e_i)\tau$, de modo que $e_i\tau$ es el elemento de A_i tal que la multiplicación por $e_i\tau$ en V_i coincide con la multiplicación por τ. Explícitamente:

$$e_i\tau = \frac{\chi_i(1)}{|G|}\sum_{\sigma\in G}\chi_i(\tau\sigma^{-1})\sigma.$$

Y aún más en general: si $\phi \in \mathrm{End}_K(V_i)$, el elemento $u_\phi \in A_i$ tal que ϕ es la multiplicación por u_ϕ en V_i es

$$u_\phi = \frac{\chi_i(1)}{|G|}\sum_{\sigma\in G}\mathrm{Tr}(\phi\circ\rho_i(\sigma^{-1}))\sigma,$$

donde $\rho_i(\sigma^{-1})$ es la multiplicación por σ^{-1} en V_i. En efecto, como la expresión de u_ϕ es K-lineal en ϕ y $\mathrm{End}_K(V_i)$ está generado por los automorfismos $\rho_i(\tau)$, con $\tau \in G$, basta probarlo cuando $\phi = \rho_i(\tau)$, pero $u_{\rho_i(\tau)} = e_i\tau$, y la expresión de u_ϕ coincide con la que ya habíamos calculado para $e_i\tau$.

Pongamos que $V = V_1$. Cada $\phi \in \mathrm{End}_D(R)$ induce por linealidad un K-endomorfismo de V. Su matriz en una base de R tiene coeficientes en D, al igual que la matriz de $\rho_i(\sigma^{-1})$ (en este caso porque R es un retículo estable), luego $\mathrm{Tr}(\phi\circ\rho_i(\sigma^{-1})) \in D$. Como $\chi_1(1) = \dim_K V$, la hipótesis del teorema nos da que $\chi_1(1)/|G| \in D$, luego llegamos a que $u_\phi \in D[G]$.

Esto significa que el isomorfismo $A_1 \cong \mathrm{End}_K(V_1)$ se restringe a un isomorfismo $A_1 \cap D[G] \cong \mathrm{End}_D(R)$. Notemos que, en particular, hemos probado que $e_1 \in D[G]$, luego $A_1 \cap D[G] = e_1D[G]$. Por otra parte,

$$D[G] = e_1D[G] \oplus (1-e_1)D[G].$$

Vemos así que la representación $\rho : D[G] \longrightarrow \mathrm{End}_D(R)$ es suprayectiva y que $\mathrm{End}_D(R) \cong e_1D[G]$ es un $D[G]$-módulo proyectivo. Por otra parte, cada endomorfismo de R está determinado por la imagen de una base, luego, si $\mathrm{rang}\, R = n$, tenemos que $\mathrm{End}_D(R) \cong R^n$, lo que prueba que R es proyectivo como $\mathrm{End}_D(R)$-módulo, luego también como $D[G]$-módulo. El teorema 4.13 implica entonces que P es un $k[G]$-módulo proyectivo. Falta probar que es simple.

Para ello usamos el teorema 1.53, según el cual $\mathrm{End}_k(P) \cong \mathrm{End}_D(R) \otimes_R k$, por lo que la representación $\bar\rho : k[G] \longrightarrow \mathrm{End}_k(P)$ es suprayectiva. Esto significa que, dados u, $v \in P$ no nulos, existe un $x \in k[G]$ tal que $u = vx$, por lo que P no puede tener $k[G]$-submódulos propios. ∎

En particular, la reducción módulo p de un carácter ordinario cuyo grado sea divisible entre la mayor potencia de p que divide al orden del grupo es un carácter modular irreducible (que además corresponde a una representación proyectiva).[1]

[1] El lector puede comprobar este hecho en el caso de los caracteres módulo 3 del grupo Σ_4, calculados en la sección 4.8.

B.2 Las clases de conjugación de A_5

El grupo alternado A_5 tiene índice 2 en el grupo simétrico Σ_5. El orden de éste es $5! = 120$, luego $|A_5| = 60$. Para calcular sus clases de conjugación consideramos en primer lugar las de Σ_5. Hay tantas como tipos de permutaciones (siete) y el cálculo de sus cardinales es un simple ejercicio de combinatoria:

$\mathrm{cl}(x)$	1	(ab)	$(ab)(cd)$	(abc)	$(abc)(de)$	$(abcd)$	$(abcde)$
$\lvert\mathrm{cl}(x)\rvert$	1	10	15	20	20	30	24
$\lvert C_{\Sigma_5}(x)\rvert$	120	12	8	6	6	4	5
$\lvert C_{A_5}(x)\rvert$	60	–	4	3	–	–	5

Por ejemplo, una permutación de tipo $(ab)(cd)$ puede expresarse de $2 \cdot 2 \cdot 2$ formas distintas, y hay $5 \cdot 4 \cdot 3 \cdot 2$ formas de elegir cuatro elementos a, b, c, d en un orden dado, por lo que el número de tales permutaciones es 15.

La tercera fila de la tabla contiene los órdenes de los centralizadores de los elementos de Σ_5, calculados con la fórmula

$$|\mathrm{cl}_G(x)| = |G : C_G(x)|.$$

En nuestro caso: $|C_{\Sigma_5}(x)| = 120/|\mathrm{cl}(x)|$. La cuarta fila contiene, para las permutaciones pares, el orden de su centralizador en A_5. Claramente:

$$C_{A_5}(x) = C_{\Sigma_5}(x) \cap A_5.$$

La fórmula

$$|C_{\Sigma_5}(x)A_5| = \frac{|C_{\Sigma_5}(x)||A_5|}{|C_{\Sigma_5}(x) \cap A_5|} \leq |\Sigma_5| = 2|A_5|$$

implica que

$$|C_{A_5}(x)| \geq \frac{1}{2}\,|C_{\Sigma_5}(x)|,$$

luego sólo hay dos posibilidades:

$$|C_{A_5}(x)| = |C_{\Sigma_5}(x)| \qquad \text{o bien} \qquad |C_{A_5}(x)| = \frac{1}{2}\,|C_{\Sigma_5}(x)|.$$

Como (ab) es una permutación impar que centraliza a 1, a $(ab)(cd)$ y a (cde), concluimos que los centralizadores en A_5 de las permutaciones de estos tipos tienen la mitad de elementos que en Σ_5. En cambio, los cinco elementos que centralizan a una permutación de tipo $(abcde)$ son necesariamente sus potencias, que son todas pares, luego el centralizador en A_5 coincide con el centralizador en Σ_5. Esto justifica la cuarta fila de la tabla.

Si $|C_{A_5}(x)| = \frac{1}{2}|C_{\Sigma_5}(x)|$, entonces

$$|\mathrm{cl}_{A_5}(x)| = |A_5 : C_{A_5}(x)| = |\Sigma_5 : C_{\Sigma_5}(x)| = |\mathrm{cl}_{\Sigma_5}(x)|,$$

luego $\mathrm{cl}_{A_5}(x) = \mathrm{cl}_{\Sigma_5}(x)$. Por el contrario, si $|C_{A_5}(x)| = |C_{\Sigma_5}(x)|$, entonces

$$|\mathrm{cl}_{A_5}(x)| = \frac{1}{2}|\mathrm{cl}_{\Sigma_5}(x)|.$$

Esto sucede únicamente con la clase de los ciclos de longitud 5, y vemos así que se desdobla en dos clases de conjugación en A_5, con 12 elementos cada una. Así, pues, las clases de conjugación de A_5 resultan ser:

	C_1	C_2	C_3	C_4	C_5
$\mathrm{cl}(x)$	1	$(ab)(cd)$	(abc)	$(abcde)$	$(abced)$
$\mathrm{ord}\, x$	1	2	3	5	5
$\lvert\mathrm{cl}(x)\rvert$	1	15	20	12	12

B.3 Caracteres ordinarios

Consideremos la restricción a A_5 de la representación de Σ_5 en $\mathbb{C}^5$ que permuta los vectores de la base canónica. Las matrices de la representación matricial en dicha base están compuestas de ceros y unos, y en la diagonal hay tantos unos como elementos fija la permutación correspondiente. Por lo tanto, su carácter χ es el indicado en la tabla siguiente:

	C_1	C_2	C_3	C_4	C_5
$\mathrm{cl}(x)$	1	$(ab)(cd)$	(abc)	$(abcde)$	$(abced)$
$\lvert\mathrm{cl}(x)\rvert$	1	15	20	12	12
χ	5	1	2	0	0
χ_4	4	0	1	-1	-1

El carácter χ no es irreducible, pues $\langle(1,1,1,1,1)\rangle$ es claramente un subespacio invariante asociado al carácter trivial. Por, consiguiente, $\chi_4 = \chi - 1$ es también un carácter de G, y calculando $\langle\chi_4, \chi_4\rangle = 1$ comprobamos que es irreducible.

Observemos ahora que el número de 5-subgrupos de Sylow de A_5 es igual a 6. En efecto, cada uno de ellos contiene, además de la unidad, cuatro ciclos de longitud 5. Como en total hay 24 ciclos, el número de subgrupos ha de ser 6. Llamémoslos $P_1, \ldots, P_6$.

Sea $V \cong \mathbb{C}^6$ el $\mathbb{C}$-espacio vectorial de base $\{P_1, \ldots, P_6\}$. Cada σ en A_5 determina una permutación de la base $P_i \mapsto P_i^\sigma$, la cual se extiende a un automorfismo de V, con lo que tenemos una representación lineal $A_5 \longrightarrow \mathrm{Aut}(V)$. Como en el caso anterior, el carácter ψ de esta representación asigna a cada permutación el número de subgrupos fijados. Vamos a comprobar que ψ viene dado por la tabla siguiente:

	C_1	C_2	C_3	C_4	C_5
$\mathrm{cl}(x)$	1	$(ab)(cd)$	(abc)	$(abcde)$	$(abced)$
$\lvert\mathrm{cl}(x)\rvert$	1	15	20	12	12
ψ	6	2	0	1	1
χ_5	5	1	-1	0	0

Para ello observamos el estabilizador de un subgrupo de Sylow P es su normalizador $N_{A_5}(P)$. Como dos subgrupos de Sylow cualesquiera son conjugados, la acción de A_5 sobre el conjunto de todos ellos forma una única órbita (de cardinal 6), luego el teorema 1.18 nos da que

$$|N_{A_5}(P)| = \frac{60}{6} = 10.$$

Vemos, pues, que $N_{A_5}(P)$ no contiene ciclos de longitud 3, luego tales ciclos no fijan a ningún subgrupo, y esto nos da el valor de ψ sobre C_3.

Por otra parte, $P \trianglelefteq N_{A_5}(P)$, luego P es el único 5-subgrupo de Sylow de $N_{A_5}(P)$, luego el normalizador no contiene más que cuatro ciclos de longitud 5 (que han de ser los de P). En otras palabras, cada ciclo de longitud 5 sólo fija al subgrupo que genera. Esto nos da el valor de ψ sobre C_4 y C_5. El de C_1 es obvio, luego sólo falta calcular el de C_2. Dejémoslo pendiente de momento y observemos que el subespacio $\langle P_1 + P_2 + P_3 + P_4 + P_5 + P_6\rangle \subset V$ es un submódulo cuyo carácter asociado es trivial. Por lo tanto, $\chi_5 = \psi - 1$ es también un carácter de G, del que sólo nos falta calcular su valor x sobre C_2 (del cual sabemos que es un número entero $-1 \leq x \leq 5$) Ahora bien:

$$\langle \chi_5, \chi_5\rangle = \frac{45 + 15x}{60}.$$

Las únicas posibilidades para que el resultado sea entero son $x = 1$ o $x = 5$, pero la segunda posibilidad significaría que $(ab)(cd)$ fija a todos los subgrupos de Sylow, lo cual es claramente falso. Por ejemplo,

$$(abcde)^{(ab)(cd)} = (badce),$$

y si fuera una potencia de $(abcde)$, como transforma b en a, tendría que ser $(abcde)^{-1} = (edcba)$, pero no lo es, luego $(ab)(cd)$ no fija a $P = \langle(abcde)\rangle$.

Concluimos que $x = 1$, lo que termina el cálculo de la tabla. Además, resulta que $\langle \chi_5, \chi_5\rangle = 1$, por lo que χ_5 es irreducible.

La tabla siguiente contiene lo que hemos obtenido hasta ahora y un poco más:

	C_1	C_2	C_3	C_4	C_5
cl(x)	1	$(ab)(cd)$	(abc)	$(abcde)$	$(abced)$
$\lvert\text{cl}(x)\rvert$	1	15	20	12	12
χ_1	1	1	1	1	1
χ_2	3	-1	0	u	v
χ_3	3	-1	0	w	x
χ_4	4	0	1	-1	-1
χ_5	5	1	-1	0	0

La columna de C_1 se completa viendo que los dos treses son la única forma de conseguir que

$$60 = 1^2 + 3^2 + 3^2 + 4^2 + 5^2.$$

Los dos ceros de la columna C_3 se obtienen aplicándole las relaciones de ortogonalidad duales (teorema 2.23), de modo que

$$1 + |\chi_2(abc)|^2 + |\chi_3(abc)|^2 + 1 + 1 = \frac{60}{20} = 3.$$

La columna de C_2 se completa usando que $\langle \chi_2, \chi_5 \rangle = \langle \chi_3, \chi_5 \rangle = 0$.

Nos falta calcular los valores u, v, w, x. Aplicando las relaciones de ortogonalidad duales a las columnas C_2 y C_4 obtenemos que $w = 1 - u$. Con C_2 y C_5 obtenemos que $x = 1 - v$. De $\langle \chi_1, \chi_2 \rangle = 0$ deducimos que $v = 1 - u$, con lo que la tabla se reduce a

	C_1	C_2	C_3	C_4	C_5
$\mathrm{cl}(x)$	1	$(ab)(cd)$	(abc)	$(abcde)$	$(abced)$
$\lvert\mathrm{cl}(x)\rvert$	1	15	20	12	12
χ_1	1	1	1	1	1
χ_2	3	-1	0	u	$1-u$
χ_3	3	-1	0	$1-u$	u
χ_4	4	0	1	-1	-1
χ_5	5	1	-1	0	0

Ahora observamos que

$$\bar{u} = \overline{\chi_2(12345)} = \chi_2((12345)^{-1}) = \chi_2(54321)$$
$$= \chi_2((12345)^{(15)(24)}) = \chi_2(12345) = u,$$

luego $u \in \mathbb{R}$. Con esto podemos aplicar las relaciones de ortogonalidad duales a las columnas C_4 y C_5, de modo que $1 + 2u(1-u) + 1 = 0$, es decir:

$$u^2 - u - 1 = 0.$$

Las raíces de esta ecuación son

$$\alpha = \frac{1+\sqrt{5}}{2}, \qquad 1 - \alpha = \frac{1-\sqrt{5}}{2}.$$

(Elegir una u otra como u sólo supone elegir a qué carácter llamamos χ_2 y a cuál χ_3.) En definitiva, la tabla de caracteres de A_5 resulta ser:

	C_1	C_2	C_3	C_4	C_5
$\mathrm{cl}(x)$	1	$(ab)(cd)$	(abc)	$(abcde)$	$(abced)$
$\mathrm{ord}\, x$	1	2	3	5	5
$\lvert\mathrm{cl}(x)\rvert$	1	15	20	12	12
χ_1	1	1	1	1	1
χ_2	3	-1	0	α	$1-\alpha$
χ_3	3	-1	0	$1-\alpha$	α
χ_4	4	0	1	-1	-1
χ_5	5	1	-1	0	0

$$\alpha = \frac{1+\sqrt{5}}{2}$$

Por ejemplo, en la tabla podemos ver que A_5 es simple, ya que todos sus caracteres son fieles (teorema 2.26).

Observemos también que los caracteres χ_2 y χ_3 son conjugados sobre $\mathbb{Q}$, en el sentido de la definición 3.63.

B.4 Caracteres módulo 2

Tenemos que A_5 tiene 4 clases de conjugación 2-regulares, luego tiene otros tantos caracteres módulo 2. Uno de ellos es $\phi_1 = 1$, y otro $\phi_4 = \chi_4$, por el teorema B.1. Observamos ahora que

$$\chi_2 + \chi_3 = \chi_1 + \chi_5,$$

luego al menos uno de los caracteres χ_2, χ_3 no es irreducible, sino que contiene a $\chi_1 = \phi_1$. Ahora bien, los caracteres modulares χ_2 y χ_3 son conjugados[2] sobre el cuerpo $\mathbb{Q}_2$. Esto es evidente una vez observamos que $\alpha \notin \mathbb{Q}_2$, pues, si $\alpha \in \mathbb{Q}_2$, el polinomio $u^2 - u - 1$ tendría sus raíces en el cuerpo de restos de $\mathbb{Q}_2$, que es $\mathbb{Z}/2\mathbb{Z}$, y no es el caso. Por lo tanto, si, por ejemplo, $\chi_2 = 1 + \phi_2$, para cierto carácter modular ϕ_2, entonces $\chi_3 = \chi_2^\tau = 1 + \phi_2^\tau$, donde τ es el automorfismo no trivial de $\mathbb{Q}_2(\alpha) = \mathbb{Q}(\sqrt{5})$. Vemos, pues, que, de hecho, el carácter trivial aparece en las descomposiciones de ambos caracteres.

Sea, pues, $\chi_2 = \phi_1 + \phi_2$, $\chi_3 = \phi_1 + \phi_3$, donde ϕ_2 y ϕ_3 son los caracteres modulares que aparecen en la tabla siguiente, que son necesariamente irreducibles, pues, como A_5 es simple no abeliano, su único carácter de grado 1 es el trivial,[3] luego si ϕ_2 o ϕ_3 no fueran irreducibles, tendrían que descomponerse como $2\phi_1$, y no es el caso.

$p = 2$	C_1	C_3	C_4	C_5
$\mathrm{cl}(x)$	1	(abc)	$(abcde)$	$(abced)$
$\mathrm{ord}\, x$	1	3	5	5
$\lvert\mathrm{cl}(x)\rvert$	1	20	12	12
ϕ_1	1	1	1	1
ϕ_2	2	-1	$\alpha - 1$	$-\alpha$
ϕ_3	2	-1	$-\alpha$	$\alpha - 1$
ϕ_4	4	1	-1	-1

$$\alpha = \frac{1+\sqrt{5}}{2}$$

De las relaciones

$$\chi_1 = \phi_1, \quad \chi_2 = \phi_1 + \phi_2, \quad \chi_3 = \phi_1 + \phi_3, \quad \chi_4 = \phi_4, \quad \chi_5 = \phi_1 + \phi_2 + \phi_3,$$

obtenemos la matriz de descomposición y la matriz de Cartan:

$$D = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}, \qquad C = \begin{pmatrix} 4 & 2 & 2 & 0 \\ 2 & 2 & 1 & 0 \\ 2 & 1 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

[2]En general, si $\phi : G \longrightarrow K$ es un carácter modular que toma valores en un cuerpo local K (no necesariamente de escisión para G) tal que la extensión $K/\mathbb{Q}_p$ sea de Galois y $\tau \in G(K/\mathbb{Q}_p)$, la función $\phi^\tau : G \longrightarrow K$ dada por $\phi^\tau(\sigma) = \tau(\phi(\sigma))$ es también un carácter modular de G. En efecto, si $\chi : G \longrightarrow k$ es el carácter ordinario asociado a ϕ, entonces τ induce un automorfismo $\bar{\tau} \in G(k/k_0)$, donde $k_0 = \mathbb{Z}/p\mathbb{Z}$ es el cuerpo de restos de $\mathbb{Q}_p$, y es claro que ϕ^τ es el carácter modular asociado al carácter $\chi^{\bar{\tau}}$ dado por 3.62.

[3]Porque una representación lineal no trivial de grado 1 sería un monomorfismo (porque G es simple) de G en el grupo multiplicativo de un cuerpo, luego G sería abeliano.

Los caracteres modulares proyectivos indescomponibles son

$$\begin{aligned}\Phi_1 &= \chi_1+\chi_2+\chi_3+\chi_5 = 4\phi_1+2\phi_2+2\phi_3,\\ \Phi_2 &= \chi_2+\chi_5 = 2\phi_1+2\phi_2+\phi_3,\\ \Phi_3 &= \chi_3+\chi_5 = 2\phi_1+\phi_2+2\phi_3,\\ \Phi_4 &= \chi_4 = \phi_4.\end{aligned}$$

Observemos la relación entre los grados $\Phi_i(1)$ y $\phi_i(1)$:

$$12\cdot 1+8\cdot 2+8\cdot 2+4\cdot 4 = 60.$$

Este ejemplo muestra que el teorema de Fong-Swan no es cierto sin la hipótesis de resolubilidad, pues hay dos representaciones de A_5 en característica 2 que no son la reducción de ninguna representación en característica 0.

B.5 Caracteres módulo 3

El grupo A_5 tiene también cuatro clases de conjugación 3-regulares, luego hemos de encontrar cuatro caracteres modulares irreducibles, de los cuales conocemos el trivial ϕ_1, así como $\phi_2=\chi_2$, $\phi_3=\chi_3$, que son irreducibles por el teorema B.1. Por otro lado, descartamos $\chi_5=\chi_1+\chi_4$. Basta probar que χ_4 es también irreducible.

Observemos que χ_4 no puede descomponerse en la forma $\chi_4=2\phi_4$, pues entonces ϕ_4 tendría que tomar el valor $-1/2$, que no es un entero algebraico. Por lo tanto, si χ_4 no es irreducible, ha de descomponerse en la forma $\chi_4=\phi_1+\phi_4$ o bien $\chi_4=2\phi_1+\phi_4$, para cierto carácter modular irreducible ϕ_4 distinto de los tres que ya conocemos. A su vez, entonces tendríamos que $\chi_5=2\phi_1+\phi_4$ o bien $\chi_5=3\phi_1+\phi_4$. Esto implica que la primera columna de la matriz de descomposición D (o la primera fila de la matriz E) sería

$$(1,0,0,1,2)\quad\text{o bien}\quad(1,0,0,2,3),$$

luego el carácter modular Φ_1 sería de la forma

$$\Phi_1=\chi_1+\chi_4+2\chi_5+\cdots = 6\phi_1+3\phi_4+\cdots$$

y, si P_1 es la envoltura proyectiva del $k[G]$-módulo trivial (donde k es un cuerpo de característica 2 suficientemente grande para $G=A_5$), tendríamos que $\dim_k P_1>6$. Vamos a probar que esto es falso, lo que justificará la irreducibilidad de χ_4.

Para ello consideramos un subgrupo $H\le A_5$ de orden $|H|=10$. (Antes hemos visto que los normalizadores de los 5-subgrupos de Sylow tienen orden 10.) Como $3\nmid |H|$, el álgebra $k[H]$ es semisimple, luego el $k[H]$-módulo trivial k es proyectivo, luego $P=k\otimes_{k[H]}k[G]$ es un $k[G]$-módulo proyectivo. Además, por el teorema 1.54, se cumple que

$$\langle [P],[k]\rangle = \dim_k \mathrm{Hom}_G(P,k) = \dim_k \mathrm{Hom}_H(k,k) = 1.$$

Así pues, P_1 es un sumando directo de P, y $\dim_k P = |G : H| = 6$, luego $\dim_k P_1 \leq 6$. Con esto tenemos probado que la tabla de caracteres modulares es

$p = 3$	C_1	C_2	C_4	C_5
$\mathrm{cl}(x)$	1	$(ab)(cd)$	$(abcde)$	$(abced)$
$\mathrm{ord}\, x$	1	2	5	5
$\lvert\mathrm{cl}(x)\rvert$	1	15	12	12
ϕ_1	1	1	1	1
ϕ_2	3	-1	α	$1-\alpha$
ϕ_3	3	-1	$1-\alpha$	α
ϕ_4	4	0	-1	-1

$$\alpha = \frac{1+\sqrt{5}}{2}$$

De las relaciones

$$\chi_1 = \phi_1, \quad \chi_2 = \phi_2, \quad \chi_3 = \phi_3, \quad \chi_4 = \phi_4, \quad \chi_5 = \phi_1 + \phi_4$$

deducimos las matrices

$$D = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}, \quad C = \begin{pmatrix} 2 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 2 \end{pmatrix}.$$

Los caracteres modulares proyectivos indescomponibles son

$$\Phi_1 = \chi_1 + \chi_5 = 2\phi_1 + \phi_4, \quad \Phi_2 = \chi_2 = \phi_2,$$

$$\Phi_3 = \chi_3 = \phi_3, \quad \Phi_4 = \chi_4 + \chi_5 = \phi_1 + 2\phi_4.$$

(En particular vemos que $\dim_k P_1 = 6$, por lo que P_1 es precisamente el módulo P que hemos considerado en la prueba de la irreducibilidad de χ_4.) Los grados $\Phi_i(1)$ y $\phi_i(1)$ son:

$$6 \cdot 1 + 3 \cdot 3 + 3 \cdot 3 + 9 \cdot 4 = 60.$$

B.6 Caracteres módulo 5

El número de clases de conjugación 5-regulares de A_5 es 3, luego buscamos dos caracteres modulares irreducibles además de $\phi_1 = \chi_1$. El teorema B.1 nos da que $\phi_3 = \chi_5$ es también irreducible, mientras que $\chi_2 = \chi_3$ y $\chi_4 = \chi_1 + \chi_2$. Vamos a probar que $\phi_2 = \chi_2$ también es irreducible, y con ello tendremos la tabla completa.

Si χ_2 no fuera irreducible, sólo podría descomponerse como $\chi_2 = \phi_1 + \phi_2$, para cierto carácter modular ϕ_2. La primera columna de la matriz de descomposición sería $(1, 1, 1, 2, 0)$, luego el coeficiente $(1, 1)$ de la matriz de Cartan sería igual a 7, luego $\dim_k P_1 \geq 7$, donde k es un cuerpo de característica 5 suficientemente grande para $G = A_5$ y P_1 es la envoltura proyectiva del $k[G]$-módulo

trivial. Ahora tomamos $H = A_4 \leq A_5$, que es un subgrupo de orden 12, con lo que el $k[H]$-módulo trivial k es proyectivo y $P = k \otimes_{k[H]} k[G]$ es un $k[G]$-módulo proyectivo de dimensión 5. Como en el caso $p = 3$ concluimos que P_1 es un sumando directo de P, luego ha de ser $\dim P_1 \leq 5$, y esta contradicción prueba que χ_2 es irreducible.

En definitiva, la tabla de caracteres módulo 5 resulta ser la siguiente:

$p = 5$	C_1	C_2	C_3
$\mathrm{cl}(x)$	1	$(ab)(cd)$	(abc)
$\mathrm{ord}\, x$	1	2	3
$\lvert\mathrm{cl}(x)\rvert$	1	15	20
ϕ_1	1	1	1
ϕ_2	3	-1	0
ϕ_3	5	1	-1

De las relaciones

$$\chi_1 = \phi_1, \quad \chi_2 = \phi_2, \quad \chi_3 = \phi_2, \quad \chi_4 = \phi_1 + \phi_2, \quad \chi_5 = \phi_3$$

deducimos las matrices

$$D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad C = \begin{pmatrix} 2 & 1 & 0 \\ 1 & 3 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Los caracteres proyectivos indescomponibles son

$$\Phi_1 = \chi_1 + \chi_4 = 2\phi_1 + \phi_2, \quad \Phi_2 = \chi_2 + \chi_3 + \chi_4 = \phi_1 + 3\phi_2, \quad \Phi_3 = \chi_5 = \phi_3.$$

Los grados $\Phi_i(1)$ y $\phi_i(1)$ son:

$$5 \cdot 1 + 10 \cdot 3 + 5 \cdot 5 = 60.$$

Bibliografía

[1] Dornhoff, L. *Group Representation Theory,* Marcel Dekker, New York, 1971.

[2] Hungerford, T.W. *Algebra,* Springer, New York, 1974.

[3] Isaacs, I.M. *Character Theory of Finite Groups,* Academic Press, New York, 1976.

[4] Ogg, A.P. *Elliptic Curves and Wild Ramification,* Amer. J. Math. 89 (1967), 1–21.

[5] Serre, J.P. *Local Fields,* Springer, New York, 1979.

[6] Serre, J.P. *Linear Representations of Finite Groups,* Springer, New York, 1977.

Índice de Materias