Universidad de Murcia

Facultad de Matemáticas

Máster en Matemática Avanzada

Trabajo Fin de Máster

Los órdenes de las unidades de torsión de un anillo de grupo: el Problema del Espectro

Realizado por **Lourdes Alonso Nanclares**

Dirigido por **Ángel del Río Mateos**

Codirigido por **Leo Margolis**

Febrero 2018

Declaración de originalidad

Lourdes Alonso Nanclares, autora del TFM titulado *Los órdenes de las unidades de torsión de un anillo de grupo: el Problema del Espectro*, bajo la tutela del profesor Ángel del Río Mateos y de Leo Margolis,

DECLARA

que el trabajo que presenta es original, en el sentido de que ha puesto el mayor empeño en citar debidamente todas las fuentes utilizadas.

En Murcia, a 7 de febrero de 2018.

Fdo.: Lourdes Alonso Nanclares

Nota. En la Secretaría de la Facultad de Matemáticas se ha depositado una copia firmada de esta declaración.

A mis padres, Jesús y Lourdes,
quienes más lo merecen.

A mi hermano, Jesús Alberto,
y a mi abuela Mª Pilar.

Al resto de mi familia,
en especial a mi tía Mª Luisa.

A mis amigos,
especialmente a Ángeles.

Índice general

Introducción **1**

1. Preliminares **5**

1.1. Cuerpos perfectos 6

1.2. Álgebras sobre anillos conmutativos 7

1.3. Anillos de valoración discreta. Los enteros p-ádicos 14

1.4. Teorema de Krull-Schmidt-Azumaya 29

1.5. Extensiones no ramificadas 30

1.6. Anillos de grupo 33

1.7. Anillos graduados, productos cruzados y anillos de grupo torcidos 37

2. Teoría de Representaciones. Teoremas de Green **49**

2.1. Representaciones de grupos 49

2.2. Módulos y representaciones restringidas e inducidas 56

2.3. Módulos proyectivos relativos y retículos 69

2.4. Teorema de Indescomponibilidad de Green 71

2.5. Teorema de Green de los Ceros de Caracteres 76

3. El Problema del Espectro y su resolución para grupos resolubles **81**

3.1. Anillos de grupo enteros 81

3.2. Problema del Espectro 84
3.3. Resultados previos al Teorema de Hertweck 85
3.3.1. Grupos resolubles 85
3.3.2. Acción doble 86
3.3.3. Retículos de permutación y Teorema de Weiss 87
3.3.4. Resultados de Hertweck 88
3.4. Teorema de Hertweck 95

4. Otros problemas en el campo de los anillos de grupo 103

Bibliografía 111

Notación 117

Índice alfabético 121

Introducción

En este trabajo G es siempre un grupo, y casi siempre es un grupo finito. Si R es un anillo, entonces RG denota el **anillo de grupo** de G con coeficientes en R, es decir, RG es un anillo que contiene a R como subanillo y a G como un grupo de unidades que forma una base de RG como R-módulo de manera que los elementos de R y G conmutan.

Los anillos de grupo tienen una presencia fundamental tanto en Teoría de Grupos como en Teoría de Anillos, ya que son una herramienta en el estudio de las representaciones de grupos y una fuente de ejemplos e inspiración en el estudio de los anillos. Un problema relativo a los anillos de grupo es el llamado **Problema del Isomorfismo**, que consiste en decidir si es cierto que si dos anillos de grupo RG y RH son isomorfos, entonces los grupos G y H son isomorfos. Aunque es bien sabido que en casi todos los casos que podamos imaginar existe respuesta negativa al Problema del Isomorfismo ([Her01, Dad71]), lo cierto es que en algunos tiene respuesta positiva, y a menudo la demostración de esto se encontró a partir del estudio de las unidades del anillo de grupo. Por ejemplo, Higman demostró en [Hig40a, Hig40b] que si G es abeliano y finito, entonces las únicas unidades de torsión de $\mathbb{Z}G$ son las triviales, es decir, los elementos de G y sus opuestos, y utilizando esto se deduce de forma obvia que el Problema del Isomorfismo tiene respuesta positiva para anillos de grupo de grupos abelianos finitos con coeficientes enteros.

Este trabajo se centra en el estudio del grupo de unidades $\mathcal{U}(\mathbb{Z}G)$ del anillo de grupo $\mathbb{Z}G$, con G un grupo finito, y, más concretamente, en sus unidades de torsión. En realidad, $\mathcal{U}(\mathbb{Z}G) = \pm V(\mathbb{Z}G)$, donde $V(\mathbb{Z}G)$ es el grupo formado por las unidades de $\mathbb{Z}G$ de aumento 1, lo que nos permite

restringirnos al estudio de los elementos de torsión de $V(\mathbb{Z}G)$. Por el resultado de Higman, si G es un grupo abeliano finito, entonces los elementos de torsión de $V(\mathbb{Z}G)$ son únicamente los de G. Sin embargo, no es esperable que esto ocurra si G no es abeliano, pues, por ejemplo, los conjugados de los elementos de G son también elementos de torsión de $V(\mathbb{Z}G)$.

Hughes y Pearson demostraron en [HP72] que para el grupo $\mathcal{S}_3$ de permutaciones de tres elementos, no todas las unidades de torsión de $V(\mathbb{Z}\mathcal{S}_3)$ son conjugadas de elementos de $\mathcal{S}_3$ en $\mathcal{U}(\mathbb{Z}\mathcal{S}_3)$, pero sí que son conjugadas de elementos de $\mathcal{S}_3$ en las unidades de $\mathbb{Q}\mathcal{S}_3$. En particular, los órdenes de los elementos de torsión de $V(\mathbb{Z}\mathcal{S}_3)$ y $\mathcal{S}_3$ son los mismos. El espectro de un grupo es el conjunto de los órdenes de sus elementos de torsión, luego $V(\mathbb{Z}\mathcal{S}_3)$ y $\mathcal{S}_3$ tienen el mismo espectro. Este ejemplo sugirió en su día las conocidas como **Conjeturas de Zassenhaus**. En el capítulo 4 explicaremos de forma más extensa lo que dicen estas conjeturas, pero aquí solo citamos la primera, que postula que todos los elementos de torsión de $V(\mathbb{Z}G)$ son conjugados en $\mathbb{Q}G$ de elementos de G, siendo G un grupo finito.

La Primera Conjetura de Zassenhaus ha tenido un papel muy relevante en el estudio de las unidades de $\mathbb{Z}G$ desde que fue planteada formalmente por Zassenhaus en 1974 ([Zas74]). Esta conjetura ha sido demostrada para grupos nilpotentes ([Wei91]), para grupos que tienen un p-subgrupo de Sylow dentro de su subgrupo conmutador ([Her06]), para grupos metacíclicos ([Her08a]) y, más generalmente, para grupos cíclicos-por-abelianos ([CMR13]). Además, ha sido probada para algunos grupos no resolubles, como los grupos alternados $\mathcal{A}_5$ ([LP89]) y $\mathcal{A}_6$ ([Her07]). Muy recientemente se ha anunciado un contraejemplo ([EM17]).

Observemos que si la Primera Conjetura de Zassenhaus es cierta para un grupo G, entonces $V(\mathbb{Z}G)$ y G tienen el mismo espectro. Este trabajo se centra precisamente en el siguiente problema:

Problema del Espectro para anillos de grupo

Si G es un grupo finito, ¿tienen G y $V(\mathbb{Z}G)$ el mismo espectro?

Todo el trabajo está orientado a demostrar un teorema de Hertweck, el resultado central de [Her08b], que afirma que el Problema del Espectro para grupos resolubles tiene solución positiva. El contraejemplo anunciado en

[EM17] es metabeliano y, en particular, resoluble. Observemos que el Teorema de Hertweck muestra que no puede ser una respuesta negativa al Problema del Espectro. De hecho, a día de hoy no se conoce ningún grupo para el que el Problema del Espectro tenga respuesta negativa.

Hertweck aplica en la demostración de su teorema un resultado clave: el **Teorema de Green de los Ceros de Caracteres**. A su vez, la prueba de este teorema depende del **Teorema de Indescomponibilidad de Green**, así como de otros muchos resultados, bastantes de ellos procedentes de la **Teoría de Representaciones**. Por tanto, en este trabajo necesitamos profundizar en toda esta teoría para poder comprender los Teoremas de Green y, finalmente, la demostración de Hertweck.

Teniendo en cuentra nuestro objetivo, así como los pasos previos que tenemos que dar, hemos organizado el trabajo como describimos a continuación:

- El primer capítulo será de preliminares, y en él se expondrán conceptos y resultados imprescindibles para comprender el resto del trabajo, pero que no son propios de la Teoría de Representaciones. Todos estos resultados están encaminados a la resolución del Problema del Espectro para grupos resolubles y, fundamentalmente, a comprender el enunciado y la demostración de los Teoremas de Green. Por ejemplo, en este capítulo se presentarán los cuerpos perfectos, las álgebras sobre anillos conmutativos, los anillos de valoración discreta, los enteros p-ádicos y los anillos de grupo.
- El segundo capítulo se centrará en el estudio de la Teoría de Representaciones, con el objetivo de probar el Teorema de Green de los Ceros de Caracteres y, como paso previo, el Teorema de Indescomponibilidad de Green. Con estas demostraciones se cerrará el capítulo.
- El capítulo principal es el tercero, que estará dedicado a la exposición del Problema del Espectro y a la resolución de este problema para grupos resolubles, para lo cual necesitaremos los resultados de los capítulos anteriores.
- A modo de conclusión, en el cuarto capítulo se tratarán otros problemas relativos a los anillos de grupo con coeficientes enteros, como el Problema del Isomorfismo y las citadas Conjeturas de Zassenhaus, así como

las conexiones entre ellos y su relación con el Problema del Espectro.

Capítulo 1

Preliminares

Como hemos comentado en la introducción, en este primer capítulo se tratarán ciertos conceptos y resultados imprescindibles para comprender el resto del trabajo. Por ejemplo, en él se presentarán los cuerpos perfectos, las álgebras sobre anillos conmutativos, los anillos de valoración discreta, los enteros p-ádicos y los anillos de grupo.

Antes de comenzar, cabe decir que tendremos en cuenta las siguientes consideraciones a lo largo del trabajo:

- **Se supondrán** al lector **conocimientos generales sobre grupos, anillos y módulos.**
- **Todos los anillos que se consideren se supondrán unitarios, y todo homomorfismo de anillos $f : R \to S$ cumplirá que $f(1_R) = 1_S$**, siendo 1_R y 1_S los elementos neutros para la multiplicación de R y S, respectivamente.
- **Cuando se hable simplemente de un módulo sobre un anillo,** sin especificar si se trata de un módulo por la izquierda o por la derecha, **se supondrá que lo es por la izquierda si el anillo no es conmutativo, y que tiene la misma estructura de módulo por la izquierda y por la derecha si el anillo es conmutativo** (es decir, si M es un R-módulo, donde R es un anillo conmutativo, se supondrá que $rm = mr$ para todo $r \in R$ y $m \in M$).
- Se entenderá que, **aunque se expongan únicamente resultados**

relativos a módulos por la izquierda, se pueden establecer resultados análogos para módulos por la derecha.

Además, al final de cada capítulo del trabajo se indicará la bibliografía que se ha empleado para elaborar las distintas secciones que lo conforman.

1.1. Cuerpos perfectos

A lo largo del trabajo aparecerá en más de una ocasión la hipótesis de que cierto cuerpo sea perfecto. En esta primera sección empezaremos por dar la definición de cuerpo perfecto y, a continuación, veremos algunos resultados relativos a este tipo de cuerpos.

Definición 1.1.1. *Se dice que un cuerpo es* ***perfecto*** *si su característica es* 0*, o bien su característica es* $p > 0$ *y* K *coincide con su subcuerpo*

$$K^p = \{x^p : x \in K\}.$$

Proposición 1.1.2. *Todo cuerpo finito es perfecto.*

Demostración. En primer lugar, sabemos que la característica de un cuerpo finito no puede ser 0, pues todo cuerpo de característica 0 contiene un subcuerpo isomorfo a los números racionales, que es un cuerpo infinito. Ahora, sea K un cuerpo finito de característica p. Se tiene que la aplicación $\psi : K \to K^p$ definida por $\psi(x) = x^p$ es un homomorfismo suprayectivo. Además, $x^p = 0$ implica que $x = 0$ para todo $x \in K$. Por tanto, ψ es un isomorfismo de anillos, luego K y K^p tienen el mismo número (finito) de elementos. Por último, como $K^p \subseteq K$, se cumple que $K = K^p$, por lo que K es un cuerpo perfecto. ∎

Dado un cuerpo K, recordemos que un polinomio irreducible en $K[X]$ es separable si sus raíces en una clausura algebraica de K son todas distintas, y que un polinomio en $K[X]$ arbitrario es separable si todos sus factores irreducibles son separables. Si K es un cuerpo de característica 0, todo polinomio en $K[X]$ de grado mayor que cero es separable. Para cuerpos de característica distinta de cero tenemos la siguiente caracterización de cuerpo perfecto:

Proposición 1.1.3. *Un cuerpo K de característica $p > 0$ es perfecto si, y solo si, todo polinomio en $K[X]$ de grado mayor que cero es separable.*

Demostración. Ver [ZS75, cap. I, secc. 5, Teorema 6]. ■

Observación 1.1.4. Recordemos que, dada una extensión de cuerpos L/K, un elemento de L algebraico sobre K es separable sobre este cuerpo si el polinomio mínimo sobre K de este elemento es separable sobre K, y que una extensión algebraica L/K es separable si todo elemento de L es separable sobre K. Por tanto, se deduce de lo anterior que toda extensión algebraica sobre un cuerpo perfecto es separable.

1.2. Álgebras sobre anillos conmutativos

En esta sección nos ocuparemos del concepto de álgebra sobre un anillo conmutativo, así como de otras nociones relativas a anillos y módulos, como son los idempotentes ortogonales, el radical de un módulo y los módulos libres de torsión. A lo largo de la sección, R denotará un anillo conmutativo.

Definición 1.2.1. *Un anillo A se dice que es un **álgebra sobre un anillo conmutativo** R, o una **R-álgebra**, si existe un homomorfismo de anillos $\psi : R \to Z(A)$, siendo $Z(A)$ el centro de A.*

Existe, sin embargo, una definición alternativa de R-álgebra, que veremos a continuación que es equivalente a la anterior:

Definición 1.2.2. *Un **álgebra sobre un anillo conmutativo** R, o una **R-álgebra**, es un anillo A que es también un R-módulo tal que la multiplicación en el anillo y la multiplicación en el módulo son compatibles, en el sentido de que*

$$r * (ab) = (r * a) \cdot b = a \cdot (r * b)$$

para cualesquiera $a, b \in A$ y $r \in R$, donde $*$ denota la multiplicación en el módulo.

Proposición 1.2.3. *Las dos definiciones anteriores son equivalentes. Con más precisión, dados un anillo conmutativo R y un anillo A, existe una biyección natural entre las estructuras de R-álgebras sobre A de acuerdo con*

la Definición 1.2.1 y las estructuras de R-álgebras sobre A según la Definición 1.2.2.

Demostración. Si $\psi : R \to Z(A)$ es un homomorfismo de anillos, entonces $r * a = \psi(r)a$ define una estructura de R-módulo sobre A, y es fácil ver que se verifican las condiciones de la Definición 1.2.2 y que $\psi(r) = r * 1_A$. Recíprocamente, si R, A y $*$ son como en la Definición 1.2.2, entonces $\psi(r) = r * 1_A$ define un homomorfismo de anillos $\psi : R \to Z(A)$, y se cumple que $r * a = \psi(r)a$ para todo $r \in R$ y $a \in A$. ■

Observación 1.2.4. Puesto que todo espacio vectorial tiene estructura de módulo, la Definición 1.2.2 pone de manifiesto que el concepto de R-álgebra es una generalización del concepto de álgebra sobre un cuerpo K, o K-álgebra.

Ejemplos 1.2.5. (i) Todo anillo A es una $\mathbb{Z}$-álgebra, en virtud del homomorfismo $\psi : \mathbb{Z} \to Z(A)$ definido por $\psi(n) = 1_A + \cdots + 1_A$, donde el elemento 1_A se repite n veces.

(ii) El anillo $\mathcal{M}_n(R)$ de las matrices cuadradas de orden n sobre R es una R-álgebra.

(iii) Dada cualquier inclusión $R \subseteq S$ de anillos conmutativos, S es una R-álgebra.

(iv) Si G es un grupo, el anillo de grupo RG es una R-álgebra, aunque esto lo veremos en la sección 1.6.

Relacionados con el concepto de R-álgebra aparecen otros, tales como el concepto de R-subálgebra o el de homomorfismo de R-álgebras, que generalizan los conceptos relativos a K-álgebras, y que trataremos a continuación.

Una **R-subálgebra** B de una R-álgebra A es un subanillo B de A que contiene a 1_A y es un R-submódulo de A.

Supongamos que $\psi : R \to Z(A)$ define una estructura de R-álgebra y que M es un A-módulo por la izquierda. Entonces M es un R-módulo con la multiplicación dada por

$$rm = \psi(r)m, \quad r \in R,\ m \in M,$$

y satisface la condición

$$r(am) = (ra)m = a(rm), \quad r \in R,\ a \in A,\ m \in M.$$

Nos referiremos a este R-módulo como el **R-módulo subyacente** de M.

Claramente, los A-submódulos de M son también R-submódulos. En particular, los ideales de A por la izquierda o por la derecha son R-submódulos de A.

Ejemplo 1.2.6. Sea A un anillo arbitrario, y sea M un A-módulo por la izquierda. Sabemos que $\mathrm{Hom}_A(M,M)$, el conjunto de los homomorfismos de A-módulos de M en M, es un anillo con la adición y la composición de homomorfismos. Este anillo se conoce como el anillo de endomorfismos de M, y se suele denotar por $\mathrm{End}_A(M)$. Además, $\mathrm{End}_A(M)$ es también un A-módulo si se define, para cada $a \in A$ y $f \in \mathrm{End}_A(M)$,

$$(af)(m) = af(m), \quad m \in M.$$

Si $A = R$ es un anillo conmutativo, la multiplicación en el módulo es compatible con la multiplicación en el anillo, luego $\mathrm{End}_R(M)$ tiene estructura de R-álgebra. En el caso más general de que A sea una R-álgebra, donde R un anillo conmutativo, por la explicación que precede a este ejemplo se tiene que $\mathrm{End}_A(M)$ también es una R-álgebra, que se suele llamar el **álgebra de endomorfismos de** M.

Si A y A' son dos R-álgebras, un homomorfismo de anillos $f : A \to A'$ se dice que es un **homomorfismo de R-álgebras** si f es también un homomorfismo de R-módulos, es decir, si se verifica que

$$f(ra) = rf(a)$$

para todo $r \in R$ y $a \in A$. Si M y M' son dos A-módulos y A es una R-álgebra, entonces un A-homomorfismo $f : M \to M'$ es automáticamente un homomorfismo de R-módulos, puesto que si $\psi : R \to Z(A)$ define una R-álgebra sobre A, entonces se tiene que

$$f(rm) = f(\psi(r)m) = \psi(r)f(m) = rf(m)$$

para todo $r \in R$ y $m \in M$.

Por otra parte, dado un anillo arbitrario A, sabemos que se puede construir el anillo opuesto de A, que es un anillo con los mismos elementos y la misma estructura aditiva que A, y en el cual la multiplicación, que se

denotará por $\cdot^{op}$, está definida como $a \cdot^{op} b = ba$ para cualesquiera $a, b \in A$. Ahora, en el caso de que el anillo A sea una R-álgebra, el anillo A^{op} tiene también estructura de R-álgebra con la misma estructura de R-módulo que A, y recibe entonces el nombre de **álgebra opuesta** de A.

Observación 1.2.7. A lo largo del trabajo se considerará en más de una ocasión el álgebra opuesta del álgebra de endomorfismos $\mathrm{End}_A(M)$, donde A es una R-álgebra y M un A-módulo por la izquierda. En tal caso, empleando la notación $E = (\mathrm{End}_A(M))^{op}$, es fácil ver que M tiene estructura de (A, E)-bimódulo con la multiplicación por la derecha

$$mf = f(m), \quad m \in M,\ f \in E.$$

Por tanto, el álgebra E puede ser vista como un anillo de operadores por la derecha sobre M.

Pasamos ahora a tratar los conceptos de clausura entera de un anillo conmutativo R en una R-álgebra y de dominio entero íntegramente cerrado. Antes hemos de ver qué quiere decir que un elemento de una R-álgebra sea entero sobre R.

Definición 1.2.8. *Sea A una R-álgebra. Se dice que un elemento α de A es **entero sobre** R si existe un polinomio mónico $f(X)$ sobre R tal que $f(\alpha) = 0$.*

Proposición 1.2.9. *Sea A una R-álgebra, y sea α un elemento de A. Las siguientes condiciones son equivalentes:*

(i) α es entero sobre R.

(ii) $R[\alpha]$ es finitamente generado como R-módulo.

(iii) Existe una R-subálgebra B de A tal que $\alpha \in B$ y B es un R-submódulo finitamente generado de A.

Demostración. Ver [Rei03, Teorema 1.10]. ∎

Corolario 1.2.10. *Sea A una R-álgebra conmutativa. El conjunto de todos los elementos de A que son enteros sobre R forman una R-subálgebra de A.*

Demostración. Ver [Rei03, Corolario 1.11]. ∎

Ejemplo 1.2.11. Se llama **cuerpo de números** a una extensión finita de

$\mathbb{Q}$. Debido al apartado (iii) de Ejemplos 1.2.5, todo cuerpo de números es una $\mathbb{Z}$-álgebra. Los **enteros algebraicos** de un cuerpo de números L son los elementos de L que son enteros sobre $\mathbb{Z}$. Por el Corolario 1.2.10, estos forman una $\mathbb{Z}$-subálgebra de L.

Definición 1.2.12. *Sea A una R-álgebra. La **clausura entera de** R **en** A es el conjunto de elementos de A que son enteros sobre R. El anillo R se llama **íntegramente cerrado en** A si la clausura entera de R en A coincide con la R-subálgebra $R\cdot 1_A$. Un dominio entero R es **íntegramente cerrado** si es íntegramente cerrado en su cuerpo de cocientes.*

Observación 1.2.13. El cuerpo de cocientes de un dominio entero R es una R-álgebra debido al apartado (iii) de Ejemplos 1.2.5.

Proposición 1.2.14. *Los dominios de factorización única (DFU) son íntegramente cerrados; en particular, lo son los dominios de ideales principales (DIP).*

Demostración. Sea R un DFU, y sean x e y elementos de R con $y \neq 0$ tales que el elemento x/y del cuerpo de cocientes de R es entero sobre R. Como R es un DFU, podemos suponer que x e y no tienen factores comunes que no sean unidades de R. Entonces se tiene que

$$(x/y)^n + c_{n-1}(x/y)^{n-1} + \cdots + c_1(x/y) + c_0 = 0$$

para algunos $c_0, c_1, \ldots, c_{n-1} \in R$. Multiplicando esta ecuación por y^n, se obtiene que

$$x^n + c_{n-1}yx^{n-1} + \cdots + c_1y^{n-1}x + c_0y^n = 0,$$

de donde se concluye que y divide a x^n. Ahora bien, si y no fuera una unidad de R, entonces algún elemento irreducible de R dividiría a y y a x^n y, por tanto, a x. Esto entraría en contradicción con el hecho de que x e y no tienen factores comunes que no sean unidades de R. Por consiguiente, y es una unidad de R, luego $x/y = xy^{-1} \in R$. ∎

Ejemplo 1.2.15. Sea R un dominio entero con cuerpo de cocientes K. La clausura entera de R en K es un dominio entero íntegramente cerrado con cuerpo de cocientes K.

Introduciremos a continuación los conjuntos de idempotentes ortogonales de un anillo, y enunciaremos un resultado relacionado con estos conjuntos

que se aplicará en la demostración del Teorema de Indescomponibilidad de Green. De ahora en adelante, A denotará un anillo arbitrario.

Sea

$$A = L_1 \oplus \cdots \oplus L_n \tag{1.1}$$

una descomposición de A en ideales por la izquierda $\{L_i\}$, y sea

$$1 = e_1 + \cdots + e_n, \quad e_i \in L_i.$$

Entonces, para cada $x \in A$, se tiene que

$$x = xe_1 + \cdots + xe_n \quad \text{y} \quad xe_i \in L_i.$$

Esto demuestra que si $x \in L_i$, entonces $x = xe_i$, y $xe_j = 0$ para $j \neq i$. Por tanto, tenemos que

$$L_i = Ae_i,\ e_i^2 = e_i,\ \text{y}\ e_ie_j = 0 \text{ para } j \neq i,\ \text{donde } 1 \leq i \leq n.$$

Diremos entonces que $\{e_1, \ldots, e_n\}$ es un conjunto de **idempotentes ortogonales** de A. Estos elementos están completamente determinados por la descomposición (1.1), pero puede haber muchas descomposiciones de A de este tipo, y cada una de ellas dará lugar a un conjunto de idempotentes ortogonales. Recíprocamente, es fácil ver que cada conjunto de idempotentes ortogonales $\{e_1, \ldots, e_n\}$ que verifican $\sum e_i = 1$ da lugar a una descomposición $A = \bigoplus Ae_i$ en ideales por la izquierda.

Para la siguiente proposición tendremos en cuenta la Observación 1.2.7:

Proposición 1.2.16. *Sea M un A-módulo por la izquierda. Consideremos M como (A, E)-bimódulo, donde $E = (\mathrm{End}_A(M))^{op}$. Entonces existe una correspondencia uno a uno entre descomposiciones*

$$M = \bigoplus_{i=1}^{n} M_i,$$

donde los M_i son A-submódulos no nulos de M, y descomposiciones

$$E = \bigoplus_{i=1}^{n} E_i,$$

donde los E_i son ideales por la izquierda no nulos de E, dada como sigue: Comenzando por la descomposición de M, sea $\pi_i : M \to M_i$ la i-ésima aplicación proyección. Entonces π_i es un idempotente de E, y

$$M_i = M\pi_i,\ E_i = E\pi_i,\ M_i = ME_i. \tag{1.2}$$

Recíprocamente, dada una descomposición de E, sea $\{\pi_i\}$ el correspondiente conjunto de idempotentes ortogonales de E. Entonces los $\{M_i\}$ vienen dados por (1.2).

Demostración. Ver [CR81, Proposición 6.3]. ■

Nos ocuparemos ahora de los conceptos de radical de un módulo y de radical de Jacobson de un anillo.

El **radical** de un A-módulo M, denotado por $\operatorname{rad} M$, se define como la intersección de todos los submódulos maximales de M. (Si M no tiene submódulos maximales, entones $\operatorname{rad} M = M$.)

El **radical de Jacobson** de A, denotado por $\operatorname{rad} A$, es el radical del módulo regular por la izquierda ${}_AA$. Por tanto,

$$\operatorname{rad} A = \bigcap L,$$

donde L recorre todos los ideales maximales por la izquierda de A.

Se puede dar otra descripción de $\operatorname{rad} A$. Para cada A-módulo M, definimos su **anulador** como

$$\operatorname{ann} M = \{a \in A : aM = 0\},$$

que es un ideal bilátero de A.

Proposición 1.2.17. *Se cumple que*

$$\operatorname{rad} A = \bigcap_M \operatorname{ann} M,$$

donde M recorre todos los A-módulos por la izquierda simples. Por tanto, $\operatorname{rad} A$ *es un ideal bilátero de A.*

Demostración. Ver [CR81, Proposición 5.5]. ■

Para terminar la sección, hablaremos de los módulos libres de torsión.

Supongamos que R es un dominio entero y que M es un R-módulo. Sea m un elemento de M. Se dice que m es un elemento **de torsión** si existe algún elemento r no nulo de R tal que $rm = 0$. En caso contrario, se dice que m es **libre de torsión**. Un R-módulo M se dice que es **de torsión** si todos sus elementos son de torsión, mientras que se llama **libre de torsión**

si todos sus elementos no nulos son libres de torsión. El conjunto de todos los elementos de torsión de un R-módulo M, es decir,

$$t(M) = \{m \in M : rm = 0 \text{ para algún } r \in R, r \neq 0\},$$

es un submódulo de torsión de M.

Se puede ver que, como R es un dominio entero, todo R-módulo finitamente generado que sea proyectivo es también libre de torsión. El recíproco no es cierto en general: los R-módulos finitamente generados libres de torsión no son necesariamente proyectivos. Sin embargo, para ciertos tipos de anillos R, un R-módulo finitamente generado M es proyectivo si, y solo si, M es libre de torsión. Esto sucede, por ejemplo, cuando R es un DIP, puesto que en este caso todo R-módulo finitamente generado libre de torsión es un R-módulo libre (y, por tanto, proyectivo) con una base finita (ver [CR62, Corolario 16.11]). De hecho, también es cierto el recíproco en la situación más general de que R sea un dominio de Dedekind, concepto que introduciremos más adelante, en la sección que comienza a continuación.

1.3. Anillos de valoración discreta. Los enteros p-ádicos

En el Teorema de Green de los Ceros de Caracteres aparece un anillo de valoración discreta completo R con cuerpo de clases de residuos $\overline{R}$ perfecto de característica p. Como hemos comentado anteriormente, este teorema se aplica en la resolución del Problema del Espectro para grupos resolubles, y el papel del anillo R mencionado lo representa $\mathbb{Z}_p$, el anillo de los enteros p-ádicos. Dedicaremos esta sección a introducir los anillos de valoración discreta y los enteros p-ádicos. Para ello, empezaremos tratando el concepto de valoración sobre un cuerpo.

Sea $\mathbb{R}_+$ el conjunto de los números reales no negativos. Una **valoración** sobre un cuerpo K es una aplicación $\varphi : K \to \mathbb{R}_+$ tal que, para cualesquiera

$a, b \in K$, verifica las siguientes propiedades:

$$\begin{cases} \varphi(a) = 0 \text{ si, y solo si, } a = 0, \\ \varphi(ab) = \varphi(a)\varphi(b), \\ \varphi(a+b) \leq \varphi(a) + \varphi(b). \end{cases}$$

La siguiente observación nos será de utilidad:

Observación 1.3.1. Por la segunda de las propiedades anteriores de una valoración φ sobre un cuerpo K, se cumple que $\varphi(1) = 1$. Aplicando de nuevo la misma propiedad, se tiene que $\varphi(a^{-1}) = 1/\varphi(a)$ para todo $a \in K \setminus \{0\}$.

Existen diferentes tipos de valoraciones. Una valoración **no arquimediana** es una valoración que satisface la condición más fuerte

$$\varphi(a+b) \leq \text{máx}\{\varphi(a), \varphi(b)\}.$$

Se llama **arquimediana** a una valoración que no cumpla dicha condición.

Dada una valoración φ sobre un cuerpo K, el conjunto

$$\{\varphi(a) : a \in K, a \neq 0\},$$

que es un subgrupo del grupo multiplicativo de $\mathbb{R}_+$, se conoce como **grupo valor**. Se dice que una valoración es **discreta** si el grupo valor correspondiente a dicha valoración es un grupo cíclico infinito. Esta denominación procede del hecho de que el grupo valor es en este caso isomorfo a $\mathbb{Z}$. Además, toda valoración discreta ha de ser no arquimediana. Para evitar casos triviales, excluiremos siempre la llamada valoración **trivial**, definida como $\varphi(0) = 0$ y $\varphi(a) = 1$ para $a \in K \setminus \{0\}$.

Cada valoración φ da lugar a una métrica en el espacio K, llamada **métrica φ-ádica**, dada por la función $d : K \times K \to \mathbb{R}_+$ definida por

$$d(x, y) = \varphi(x - y).$$

Esta métrica define una topología sobre K, en la que una base de entornos de un elemento a de K viene dada por las esferas abiertas

$$\{x \in K : \varphi(x - a) < \varepsilon\},$$

donde ε recorre todos los números reales positivos. Dos valoraciones se dicen **equivalentes** si dan lugar a la misma topología sobre K.

Pasamos ahora a tratar los conceptos de anillo de valoración, anillo de valoración discreta y cuerpo de clases de residuos.

Dada una valoración no arquimediana φ sobre un cuerpo K, definimos

$$R = \{a \in K : \varphi(a) \leq 1\} \quad \text{y} \quad P = \{a \in K : \varphi(a) < 1\}. \tag{1.3}$$

Se tiene que R es un anillo local, que recibe el nombre de **anillo de valoración** de φ y su único ideal maximal es P. (Podemos encontrar una demostración de estos resultados en [Jan73, cap. II, Proposición 1.2].) Por la Observación 1.3.1, el ideal P de R está formado por los elementos no invertibles de R. Además, se cumple que $x \in K \setminus R$ si, y solo si, $x^{-1} \in R$, luego el cuerpo de cocientes de R es K. El cuerpo R/P se llama **cuerpo de clases de residuos** (o **cuerpo de residuos**) de R, y se suele denotar por $\overline{R}$. Los anillos de valoración asociados a dos valoraciones equivalentes coinciden.

Si φ es discreta, se dice que el anillo R es un **anillo de valoración discreta**, que abreviaremos como **AVD**. Aunque ya hemos comentado que se verifica en general para un anillo de valoración cualquiera, en la proposición que se enuncia a continuación se prueba, entre otras cosas, que el ideal P definido en (1.3) es el único ideal maximal de un anillo de valoración discreta R.

Proposición 1.3.2. *Sean R un AVD y $\varphi : K \to \mathbb{R}_+$ la valoración asociada a R, siendo K el cuerpo de cocientes de R. Sea $P = \{a \in K : \varphi(a) < 1\}$. Se verifican las siguientes afirmaciones:*

(i) Existe un elemento π de P tal que $\varphi(K \setminus \{0\}) = \langle \varphi(\pi) \rangle$.

(ii) Todo ideal no nulo de R es de la forma $\pi^k R$ para algún $k \geq 0$, por lo que R es un DIP y, en consecuencia, es un anillo noetheriano e íntegramente cerrado. En particular, se verifica que $P = \pi R$, y este es el único ideal maximal de R.

Demostración. (i) Como R es un AVD, se tiene que φ es una valoración discreta, por lo que existe un elemento π no nulo de K tal que

$$\varphi(K \setminus \{0\}) = \langle \varphi(\pi) \rangle .$$

Como se supone que φ no es la valoración trivial, se tiene que $\varphi(\pi) \neq 1$. En el caso de que $\pi \notin P$, se tendría que $\varphi(\pi) > 1$ y, por tanto, $\varphi(\pi^{-1}) = 1/\varphi(\pi) < 1$. En consecuencia, se llegaría a que $\varphi(K \setminus \{0\}) = \langle \varphi(\pi^{-1}) \rangle$, con $\pi^{-1} \in P$. Por tanto, cambiando π por π^{-1} podemos suponer que $\pi \in P$.

(ii) Sean I un ideal no nulo de R y x un elemento no nulo de I con $\varphi(x)$ máximo. Si $y \in I$, entonces $\varphi(y) \leq \varphi(x)$ y, por tanto, $\varphi(yx^{-1}) = \varphi(y)/\varphi(x) \leq 1$. Por consiguiente, $yx^{-1} \in R$, por lo que $y \in Rx$. Esto prueba que $I = Rx$. Por el apartado anterior, $\varphi(K \setminus \{0\}) = \langle \varphi(\pi) \rangle$ para algún elemento π de P, luego $\varphi(x) = \varphi(\pi)^k = \varphi(\pi^k)$ para algún $k \geq 0$, puesto que $x \in R$, y se sigue de lo que acabamos de probar que $I = xR = \pi^k R$.

En particular, el ideal P de R verifica que $P = \pi^k R$ para algún $k \geq 0$. Ahora bien, por ser $\varphi(1) = 1$, P está estrictamente contenido en R, luego se verifica que $k \geq 1$. Además, del hecho de que $\pi \in P$ se deduce que $(\pi^{k-1})^{-1} \in R$ y, por tanto, $\pi^{k-1} \notin P$. Como consecuencia, se cumple que $k = 1$ y, por consiguiente, $P = \pi R$. Por último, el resto de ideales propios de R están contenidos en P, lo que implica que P es el único ideal maximal de R.

El hecho de que R sea íntegramente cerrado es consecuencia de la Proposición 1.2.14. ■

Dado un anillo de valoración discreta R, cualquier elemento π de P tal que $P = \pi R$ recibe el nombre de **elemento primo** o **uniformizador** de R.

Observación 1.3.3. Para introducir el concepto de anillo de valoración discreta, nos hemos basado en [CR81]. No obstante, el enfoque que ofrecen otros textos al tratar este tema es diferente. Por ejemplo, en el caso de [Jan73], se comienza definiendo un **anillo de valoración discreta** como un DIP que tiene un único ideal maximal. Sin embargo, en este libro se definen más adelante los conceptos de valoración, valoración discreta y anillo de valoración, y se comprueba que un anillo de valoración es un anillo de valoración discreta, tal como se había definido al principio, si, y solo si, la valoración correspondiente es discreta. Por consiguiente, las dos definiciones de AVD proporcionadas son equivalentes.

Introduciremos ahora el concepto de valoración exponencial.

Se denomina **valoración exponencial** sobre un cuerpo K a una apli-

cación $v : K \to \mathbb{Z} \cup \{+\infty\}$ tal que, para cualesquiera $a, b \in K$, verifica las siguientes propiedades:

$$\begin{cases} v(0) = +\infty, \\ v(ab) = v(a) + v(b), \\ v(a+b) \geq \text{mín}\{v(a), v(b)\}, \end{cases}$$

con las convenciones obvias con respecto a $v(0) = +\infty$.

A partir de una valoración exponencial sobre un cuerpo K, se puede obtener una valoración no arquimediana sobre K. Para ello, basta elegir un número real $\kappa > 1$, y definir

$$\varphi(a) = \kappa^{-v(a)}, \ a \in K,$$

con $\varphi(0) = 0$. Además, si se modifica el valor de κ, se obtiene una valoración equivalente a la original.

Observación 1.3.4. La definición de valoración la hemos tomado de [CR81]. Dicho término se define de la misma manera en [Jan73], y es de este libro de donde hemos tomado la definición de valoración exponencial. No obstante, en otros textos, como [Gou93] o [Ser79], se llama valor absoluto a lo que nosotros hemos llamado valoración, y valoración a lo hemos denominado valoración exponencial.

A continuación veremos un ejemplo de anillo de valoración discreta, pero antes necesitamos introducir el concepto de dominio de Dedekind.

Definición 1.3.5. *Diremos que un anillo R es un **dominio de Dedekind** (o **anillo de Dedekind**) si es un dominio entero y todo ideal propio no nulo de R se puede expresar de forma única como producto de ideales primos no nulos, salvo el orden de aparición de los factores.*

Todo DIP es un dominio de Dedekind, y el concepto de dominio de Dedekind es una generalización natural del de DIP. Además, un dominio de Dedekind no es necesariamente un DFU; este es el caso, por ejemplo, de $\mathbb{Q}(\sqrt{-5})$. (Esto último aparece demostrado en [Neu99, secc. 3, Ejemplo].)

Ejemplo 1.3.6. Sea R un dominio de Dedekind con cuerpo de cocientes K, y sea P un ideal maximal de R que es principal. Para cada elemento

a no nulo de K, sea $v_P(a)$ el exponente de P en la factorización de aR como producto de potencias de ideales primos, y definimos $v_P(0) = +\infty$. Se tiene que $v_P : K \to \mathbb{Z} \cup \{+\infty\}$ es una valoración exponencial sobre K, que se conoce como **valoración exponencial P-ádica** sobre K. Elegimos ahora un número real $\kappa > 1$, y definimos

$$\varphi_P(a) = \kappa^{-v_P(a)}, \ a \in K,$$

con $\varphi_P(0) = 0$. Entonces φ_P es una valoración no arquimediana discreta sobre K, llamada la **valoración P-ádica** sobre K. Como hemos comentado anteriormente, al modificar el valor de κ no se modifica la clase de equivalencia de la valoración. El anillo de valoración de φ_P es

$$R_P = \{x/s : x \in R, s \in R \setminus P\},$$

es decir, coincide con la localización de R en P. Por tanto, R_P es un anillo de valoración discreta, y su único ideal maximal es $P \cdot R_P$. Además, se cumple que

$$R_P/(P \cdot R_P) \cong R/P.$$

Observación 1.3.7. Esto último se deduce del siguiente resultado más general, que podemos encontrar en [Jan73, cap. I, Lema 3.11]: Sea P un ideal maximal de un anillo conmutativo R, y sea k un entero positivo. Entonces la inclusión de R en R_P induce un isomorfismo $R/P^k \cong R_P/(P^k \cdot R_P)$.

Otra definición equivalente de dominio de Dedekind, que se encuentra estrechamente relacionada con el ejemplo anterior, es la siguiente:

Definición 1.3.8. *Un **dominio de Dedekind** (o **anillo de Dedekind**) es un dominio entero noetheriano R tal que R_P, la localización de R en P, es un AVD para todo ideal primo no nulo P de R.*

Además, se puede probar que todo ideal primo no nulo de un dominio de Dedekind es maximal. (La demostración se puede consultar en [Jan73, cap. I, Propiedades elementales 3.2].)

Abordaremos ahora el proceso de completación de un espacio métrico, es decir, la forma natural de construir a partir de él un espacio métrico completo.

Sea (X, d) un espacio métrico, y sea $\mathfrak{C}$ el conjunto de todas las sucesiones de Cauchy de elementos de X. Definimos ahora la relación de equivalencia $\sim$

en $\mathfrak{C}$ como

$$\{x_n\} \sim \{y_n\} \text{ si, y solo si, } \lim_{n\to\infty} d(x_n, y_n) = 0,$$

y consideramos el conjunto cociente

$$\widehat{X} = \mathfrak{C}/\sim .$$

A partir de la métrica d sobre X se puede definir una métrica $\widehat{d}$ sobre $\widehat{X}$, dada por

$$\widehat{d}([a_n],[b_n]) = \lim_{n\to\infty} d(a_n, b_n),$$

donde $[x_n]$ denota la clase de equivalencia de la sucesión de Cauchy $\{x_n\}$ de elementos de X. Así, $\widehat{X}$ tiene estructura de espacio métrico. Este espacio métrico es completo, y se llama la **completación** de X respecto de la métrica d.

En el caso de que X sea un anillo, el cual denotaremos por R, $\mathfrak{C}$ será también un anillo, con las operaciones

$$\{x_n\} + \{y_n\} = \{x_n + y_n\} \quad \text{y} \quad \{x_n\} \cdot \{y_n\} = \{x_n \cdot y_n\}.$$

Como la relación $\sim$ es compatible con estas operaciones, también la completación $\widehat{R}$ de R será un anillo. Además, R estará embebido en $\widehat{R}$, por medio de la aplicación que a cada elemento x de R le asocia la clase de equivalencia de la sucesión constante $\{x_n\}$ con $x_n = x$. Por último, en el caso de que X coincida con un cuerpo K, $\widehat{K}$ también será un cuerpo.

Consideramos ahora cualquier valoración (no trivial) φ, no necesariamente no arquimediana, sobre un cuerpo K. Puesto que esta valoración da lugar a la métrica $d : K \times K \to \mathbb{R}_+$ definida por $d(x, y) = \varphi(x - y)$, K se puede convertir en un espacio métrico. Podemos entonces construir la completación $\widehat{K}$ de este espacio tal como hemos explicado. Se puede probar que la valoración φ se puede extender de forma única a una valoración $\widehat{\varphi}$ sobre el cuerpo $\widehat{K}$, dada por

$$\widehat{\varphi}([x_n]) = \lim_{n\to\infty} \varphi(x_n).$$

Notemos que este límite existe, ya que $\{\varphi(x_n)\}$ es una sucesión de Cauchy en $\mathbb{R}$. Además, la métrica $\widehat{d}$ sobre $\widehat{K}$, tal como la hemos definido anteriormente, es la métrica asociada a la valoración $\widehat{\varphi}$. En este caso, $\widehat{K}$, que es completo con respecto a la métrica $\widehat{\varphi}$-ádica, se conoce como la **completación φ-ádica** de

K. (Podemos consultar más detalles del proceso de completación en [Jan73, cap. II, secc. 2].)

Si φ es una valoración arquimediana, entonces también lo es $\widehat{\varphi}$, y $\widehat{K}$ es o bien $\mathbb{R}$ o bien $\mathbb{C}$, siendo $\widehat{\varphi}$ equivalente al valor absoluto usual. (Podemos encontrar una demostración en [Jan73, cap. II, Teorema 4.1 (Ostroski)].) Por otro lado, si φ es no arquimediana, también lo es $\widehat{\varphi}$, y tiene el mismo grupo valor que φ; en particular, si φ es una valoración discreta, también lo es $\widehat{\varphi}$.

Sea ahora φ una valoración discreta sobre K, y $\widehat{\varphi}$ su extensión a la completación φ-ádica $\widehat{K}$. Definimos los conjuntos

$$\widehat{R} = \{a \in \widehat{K} : \widehat{\varphi}(a) \leq 1\} \quad \text{y} \quad \widehat{P} = \{a \in \widehat{K} : \widehat{\varphi}(a) < 1\}.$$

Se tiene que $\widehat{R}$ es el anillo de valoración discreta asociado a $\widehat{\varphi}$, y $\widehat{P}$ es su único ideal maximal. Se puede ver que el elemento primo de $\widehat{R}$ es el mismo que el de R.

Además, se tiene un isomorfismo de cuerpos

$$\widehat{R}/\widehat{P} \cong R/P,$$

donde R es el anillo de valoración de φ y P es el ideal maximal de R. De hecho, en general, existe un isomorfismo de anillos

$$\widehat{R}/\widehat{P}^k \cong R/P^k \text{ para cada } k \geq 1.$$

También podemos observar que se verifican las relaciones

$$\widehat{P} = P \cdot \widehat{R} \quad \text{y} \quad P = \widehat{P} \cap R.$$

Otra manera equivalente de definir $\widehat{R}$ es como la completación de R, que es un espacio métrico con la métrica φ-ádica. (La completación se realiza de la manera usual, tal como se ha explicado anteriormente.) Entonces, como sabemos que $\widehat{K}$ es el cuerpo de cocientes de $\widehat{R}$, en lugar de obtener $\widehat{K}$ como la completación de K, y posteriormente $\widehat{R}$ como el anillo de valoración de $\widehat{\varphi}$, se puede obtener primero $\widehat{R}$ como la completación de R, y después $\widehat{K}$ como el cuerpo de cocientes de $\widehat{R}$.

Antes de definir el anillo de los enteros p-ádicos para un entero primo p, veamos cómo podemos dotar a un anillo arbitrario de cierta topología asociada a uno de sus ideales.

Dado un ideal bilátero N de un anillo A, se puede dotar a A de la **topología N-ádica**. En esta topología, una base de los entornos abiertos de un elemento a de A viene dada por

$$\left\{a + N^k : k = 0, 1, 2, \dots\right\}.$$

Se dice que A es **completo en la topología N-ádica** si toda sucesión de Cauchy de elementos de A converge (con relación a la topología N-ádica) a un único elemento de A. Cuando se dice que un anillo local es **completo**, en realidad se quiere decir que es completo en la topología P-ádica, donde P es el único ideal maximal del anillo considerado.

En relación con la topología que acabamos de definir, tenemos el siguiente resultado, que utilizaremos en la demostración del Teorema de Indescomponibilidad de Green:

Teorema 1.3.9. *Sea A un anillo arbitrario, y sea $\overline{A} = A/N$, donde N es un ideal bilátero de A contenido en* $\operatorname{rad} A$. *Supongamos que se cumple alguna de las siguientes dos condiciones:*

(i) A es artiniano por la izquierda.

(ii) A es una R-álgebra, finitamente generada como R-módulo, donde R es un anillo local noetheriano conmutativo completo.

Entonces A es completo en la topología N-ádica, y cada descomposición

$$A = Ae_1 \oplus \cdots \oplus Ae_n$$

en ideales por la izquierda indescomponibles $\{Ae_i\}$ de A da lugar a una descomposición

$$\overline{A} = \overline{A}\overline{e}_1 \oplus \cdots \oplus \overline{A}\overline{e}_n$$

en ideales por la izquierda indescomponibles $\{\overline{A}\overline{e}_i\}$ de $\overline{A}$.

Además, para $1 \le i, j \le n$, se tiene que

$$Ae_i \cong Ae_j \text{ si, y solo si, } \overline{A}\overline{e}_i \cong \overline{A}\overline{e}_j.$$

Demostración. Ver [CR81, Teorema 6.8]. ∎

Estamos ya en condiciones de definir el anillo $\mathbb{Z}_p$ de los enteros p-ádicos, dado un entero primo p, y de comprobar que este anillo es un anillo de

valoración discreta que satisface las hipótesis del Teorema de Green de los Ceros de Caracteres. Esto es lo que haremos a continuación.

Sabemos que $\mathbb{Z}$ es un DIP y, por tanto, es un dominio de Dedekind con cuerpo de cocientes $\mathbb{Q}$. Sea P un ideal maximal de $\mathbb{Z}$, que será de la forma $P = p\mathbb{Z}$, con p un entero primo. Consideramos la valoración exponencial P-ádica sobre $\mathbb{Q}$, definida en el Ejemplo 1.3.6, a la que llamaremos **valoración exponencial p-ádica** y denotaremos por v_p. La aplicación $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{+\infty\}$ asigna a cada entero no nulo el exponente de p en su descomposición en factores primos, mientras que si $x/y \in \mathbb{Q} \setminus \{0\}$, $v_p(x/y) = v_p(x) - v_p(y)$. Además, $v_p(0) = +\infty$.

A partir de la valoración exponencial p-ádica, podemos obtener la valoración P-ádica sobre $\mathbb{Q}$, definida en el Ejemplo 1.3.6, que sabemos que es una valoración discreta. Nos referiremos a esta valoración como **valoración p-ádica** sobre $\mathbb{Q}$, y la representaremos por $|\ |_p$. Con la notación empleada en el Ejemplo 1.3.6, tomaremos $\kappa = p$, por lo que $|\ |_p : \mathbb{Q} \to \mathbb{R}_+$ viene dada por

$$|a|_p = p^{-v_p(a)}, \quad a \in \mathbb{Q},$$

con $|0|_p = 0$. El anillo de valoración discreta asociado a $|\ |_p$ es la localización de $\mathbb{Z}$ en $p\mathbb{Z}$, es decir,

$$\mathbb{Z}_{(p)} = \{x/y : x, y \in \mathbb{Z}, p \nmid y\}.$$

Además, el único ideal maximal de $\mathbb{Z}_{(p)}$ es $p\mathbb{Z}_{(p)}$, y el cuerpo de clases de residuos de $\mathbb{Z}_{(p)}$ es

$$\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \cong \mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p,$$

el cuerpo cíclico de p elementos.

Sea ahora $\mathbb{Q}_p$ la completación $|\ |_p$-ádica (o, simplemente, **completación p-ádica**) de $\mathbb{Q}$. Hemos visto que la valoración p-ádica sobre $\mathbb{Q}$ se puede extender a una valoración sobre $\mathbb{Q}_p$, y lo mismo se puede hacer con la valoración exponencial p-ádica. Sabemos que existe un embebimiento de $\mathbb{Q}$ a $\mathbb{Q}_p$, por lo que $\mathbb{Q}$ puede ser visto como un subcuerpo de $\mathbb{Q}_p$. Así, podemos mantener las notaciones $|\ |_p$ y v_p para las extensiones a $\mathbb{Q}_p$ de la valoración p-ádica y la valoración exponencial p-ádica sobre $\mathbb{Q}$, respectivamente. Además, la inclusión $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ tiene imagen densa. Se llama a $\mathbb{Q}_p$ el **cuerpo de los números**

p-ádicos, que es un espacio métrico completo con respecto a la métrica procedente de la valoración $|\ |_p$. El **anillo de los enteros p-ádicos**, que se denota por $\mathbb{Z}_p$, es el anillo de valoración de $|\ |_p$, es decir,

$$\mathbb{Z}_p = \{a \in \mathbb{Q}_p : |a|_p \leq 1\}.$$

En consecuencia, $\mathbb{Z}_p$ es un anillo de valoración discreta, cuyo único ideal maximal es

$$\widehat{P} = \{a \in \mathbb{Q}_p : |a|_p < 1\} = p\mathbb{Z}_p,$$

debido a que el elemento primo de $\mathbb{Z}_p$ es el mismo que el de $\mathbb{Z}_{(p)}$, es decir, p. Además, por lo que hemos comentado anteriormente, $\mathbb{Z}_p$ es la completación de $\mathbb{Z}_{(p)}$ con respecto a la métrica procedente de la valoración p-ádica, y la topología en $\mathbb{Z}_p$ coincide con la topología $\widehat{P}$-ádica, tal como se ha definido anteriormente. (Para obtener más detalles de esto último, se puede consultar [Jan73, cap. II, secc. 5].) Por tanto, $\mathbb{Z}_p$ es un anillo de valoración discreta completo, con cuerpo de cocientes $\mathbb{Q}_p$.

Por otra parte, sabemos que el cuerpo de clases de residuos de $\mathbb{Z}_p$ es

$$\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \cong \mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p,$$

el cuerpo de p elementos, que tiene característica p. Además, como $\mathbb{F}_p$ es un cuerpo finito, el cuerpo de clases de residuos de $\mathbb{Z}_p$ es perfecto, por la Proposición 1.1.2.

Así, queda probado que $\mathbb{Z}_p$ es un anillo de valoración discreta que cumple las hipótesis que aparecen en el Teorema de Green de los Ceros de Caracteres, como queríamos demostrar. No obstante, por la forma en que hemos construido el anillo $\mathbb{Z}_p$ de los enteros p-ádicos, es difícil hacerse una idea de cómo son sus elementos. Por ello daremos a continuación dos descripciones de los elementos de $\mathbb{Z}_p$, una como sucesiones coherentes y otra como expansiones p-ádicas.

Proposición 1.3.10. *Se verifican las siguientes afirmaciones:*

(i) $\mathbb{Q} \cap \mathbb{Z}_p = \mathbb{Z}_{(p)} = \left\{\frac{a}{b} \in \mathbb{Q} : p \nmid b\right\}$.

(ii) La inclusión $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ tiene imagen densa. En particular, si $x \in \mathbb{Z}_p$ y $n \geq 1$, existe un entero α tal que $0 \leq \alpha \leq p^n - 1$ y $|x - \alpha|_p \leq p^{-n}$. El entero α con estas propiedades es único.

(iii) Para cualquier elemento x de $\mathbb{Z}_p$, existe una sucesión de Cauchy $\{\alpha_n\}$ que converge a x y que verifica las siguientes condiciones:

- *Para todo n, $\alpha_n \in \mathbb{Z}$ y $0 \leq \alpha_n \leq p^n - 1$.*
- *Para cada n se tiene que $\alpha_{n+1} \equiv \alpha_n \pmod{p^n}$.*

La sucesión $\{\alpha_n\}$ con estas propiedades es única.

Demostración. Ver [Gou93, Proposición 3.3.4]. (Observemos que (iii) se deduce de aplicar (ii) a una sucesión de enteros $n = 1, 2, \dots$) ∎

Las sucesiones de números enteros que cumplen las condiciones del apartado (iii) de la proposición anterior reciben el nombre de **sucesiones coherentes**. Si $\{\alpha_n\}$ es una sucesión coherente, es también de Cauchy, puesto que $|\alpha_{n+1} - \alpha_n|_p \leq p^{-n}$ para todo n. Por ser $\mathbb{Q}_p$ completo, esta sucesión debe converger a algún elemento de $\mathbb{Q}_p$, y se puede ver que el límite pertenece a $\mathbb{Z}_p$, debido a que todos los α_n son enteros. Este razonamiento, junto con el apartado (iii) de la proposición anterior, nos permite identificar los elementos de $\mathbb{Z}_p$ con este tipo de sucesiones.

De la Proposición 1.3.10 se deduce que $\mathbb{Z}_p$ es la completación de $\mathbb{Z}$ con respecto a la valoración p-ádica. Otra consecuencia es la siguiente:

Corolario 1.3.11. *Se cumple que $\mathbb{Q}_p = \mathbb{Z}_p[1/p]$, es decir, para cada elemento x de $\mathbb{Q}_p$, existe un entero $n \geq 0$ tal que $p^n x \in \mathbb{Z}_p$.*

Demostración. Si $x \in \mathbb{Q}_p$, podemos calcular su valoración exponencial. Si $v_p(x) \geq 0$, entonces $|x|_p = p^{-v_p(x)} \leq 1$, luego x es ya un elemento de $\mathbb{Z}_p$. En otro caso, $v_p(x)$ es negativa, y tenemos que

$$v_p\left(p^{-v_p(x)}x\right) = -v_p(x) + v_p(x) = 0,$$

lo que significa que $p^{-v_p(x)}x \in \mathbb{Z}_p$, como queríamos demostrar. ∎

Este corolario nos dice que si $x \in \mathbb{Q}_p$, entonces $x \in p^n\mathbb{Z}_p$ para algún entero n. Se puede ver que $v_p(x)$ es el mayor de los enteros que verifican tal condición.

Como hemos comentado anteriormente, podemos identificar los elementos de $\mathbb{Z}_p$ con sucesiones coherentes. Vamos a profundizar más en esto. Conside-

ramos la proyección sobre el cociente

$$\varphi_n : \mathbb{Z}_p \longrightarrow \mathbb{Z}/p^n\mathbb{Z},$$

definida por $\varphi_n(x) = \alpha_n$ para cada $x \in \mathbb{Z}_p$, donde $\{\alpha_n\}$ es la sucesión coherente convergente a x. (Recordemos que para todo n se verifica que $0 \leq \alpha_n \leq p^n - 1$.)

Para cada n, definimos

$$A_n = \mathbb{Z}/p^n\mathbb{Z},$$

y dotamos a este conjunto de la topología discreta, es decir, de aquella en la que todos los conjuntos son abiertos. Existen homomorfismos obvios $\psi_n : A_n \to A_{n-1}$ que envían a mod p^n a a mod p^{n-1}. Consideramos ahora el producto de todos estos anillos, es decir, el anillo de sucesiones $\{\alpha_n\}$ tales que $\alpha_n \in \mathbb{Z}/p^n\mathbb{Z}$, con las operaciones definidas término a término, y dotamos a este anillo de la topología producto. De todo esto se deduce el siguiente resultado:

Proposición 1.3.12. *Juntando todas las aplicaciones proyección φ_n se obtiene una inclusión*

$$\varphi : \mathbb{Z}_p \hookrightarrow \prod_{n \geq 1} A_n$$

que identifica $\mathbb{Z}_p$ como anillo topológico con el subconjunto cerrado de $\prod A_n$ formado por todas las sucesiones coherentes, es decir, aquellas sucesiones $\{\alpha_n\}$ para las cuales $\psi_n(\alpha_n) = \alpha_{n-1}$ para todo $n > 1$.

Esta descripción de los enteros p-ádicos está vinculada a una propiedad universal que cumple $\mathbb{Z}_p$: es el límite inverso (o proyectivo) de los A_n (ver [Gou93, Problema 103] para obtener más información). Ahora, si bien esta descripción de los enteros p-ádicos como sucesiones coherentes es interesante desde el punto de vista teórico, es más "concreta" la descripción que daremos a continuación de estos elementos en términos de expansiones p-ádicas.

Sea x un entero p-ádico. Como hemos visto, existe una sucesión $\{\alpha_n\}$ que converge a x tal que que para todo n, se verifican las condiciones $\alpha_n \in \mathbb{Z}$, $0 \leq \alpha_n \leq p^n - 1$ y $\alpha_{n+1} \equiv \alpha_n \pmod{p^n}$. Para entender los α_n un poco mejor, los escribiremos en base p. La clave es que para enteros escritos en base p, el proceso de reducción módulo p^n es muy simple: se elimina todo salvo los últimos n dígitos. Por tanto, la condición

$$\alpha_{n+1} \equiv \alpha_n \pmod{p^n}$$

significa simplemente que los últimos n dígitos de ambos números coinciden. Entonces obtenemos

$$\begin{aligned}
\alpha_0 &= b_0 & 0 \le b_0 \le p-1\\
\alpha_1 &= b_0 + b_1 p & 0 \le b_1 \le p-1\\
\alpha_2 &= b_0 + b_1 p + b_2 p^2 & 0 \le b_2 \le p-1\\
\alpha_3 &= b_0 + b_1 p + b_2 p^2 + b_3 p^3 & 0 \le b_3 \le p-1,
\end{aligned}$$

y así sucesivamente. De esto se siguen los siguientes resultados:

Lema 1.3.13. *Dado cualquier elemento x de $\mathbb{Z}_p$, la serie*

$$b_0 + b_1 p + b_2 p^2 + \cdots + b_n p^n + \ldots$$

obtenida como arriba converge a x.

Demostración. Recordemos que una sucesión converge a x si la sucesión de sus sumas parciales converge a x. Como las sumas parciales de esta serie son exactamente los α_n, que ya sabemos que convergen a x, queda probado el resultado. ∎

Corolario 1.3.14. *Todo elemento x de $\mathbb{Z}_p$ se puede escribir de la forma*

$$b_0 + b_1 p + b_2 p^2 + \cdots + b_n p^n + \ldots,$$

con $0 \le b_n \le p-1$, y esta representación es única.

Demostración. Hemos probado todo salvo la unicidad. Ahora bien, sabemos que los α_n son únicos, y esto implica que también lo son los b_n, puesto que son los dígitos en base p. ∎

Ahora nos planteamos obtener la representación de cualquier elemento de $\mathbb{Q}_p$. Por el Corolario 1.3.11, todo número p-ádico se puede escribir de la forma y/p^m, con $y \in \mathbb{Z}_p$. Si expresamos y como serie de potencias de p, al dividir por p^m obtenemos una serie de potencias de p donde alguna de las potencias puede ser negativa. Se obtiene así el siguiente resultado:

Corolario 1.3.15. *Todo elemento x no nulo de $\mathbb{Q}_p$ se puede escribir de la forma*

$$b_{n_0} p^{n_0} + b_{n_0+1} p^{n_0+1} + \cdots + b_0 + b_1 p + b_2 p^2 + \cdots + b_n p^n + \cdots = \sum_{n=n_0}^{\infty} b_n p^n,$$

con $n_0 \in \mathbb{Z}$, $0 \le b_n \le p-1$ para todo $n \ge n_0$ y $b_{n_0} \neq 0$. En tal caso, $v_p(x) = n_0$.

Demostración. Únicamente queda probar la afirmación sobre $v_p(x)$, pero es evidente por el comentario posterior al Corolario 1.3.11. ∎

Esta representación de cada elemento x de $\mathbb{Q}_p$ se llama la **expansión p-ádica** de x.

Vamos a determinar ahora $\mathcal{U}(\mathbb{Z}_p)$, el grupo de unidades de $\mathbb{Z}_p$. Como el hecho de que $x \in \mathbb{Z}_p$ significa que $|x|_p \leq 1$, y $x^{-1} \in \mathbb{Z}_p$ equivale a que $|x^{-1}|_p = |x|_p^{-1} \leq 1$, se tiene que

$$\mathcal{U}(\mathbb{Z}_p) = \{x \in \mathbb{Q}_p : |x|_p = 1\}.$$

Además, es fácil ver que

$$\mathcal{U}(\mathbb{Z}_p) \cap \mathbb{Q} = \left\{\frac{a}{b} \in \mathbb{Q} : p \nmid ab\right\},$$

y de esto se desprende que todo entero coprimo con p es invertible en el anillo de los enteros p-ádicos.

A continuación definiremos el concepto de anillo p-ádico. Dado un entero primo p, por un **anillo p-ádico** entenderemos la clausura entera de $\mathbb{Z}_p$ en una extensión finita de $\mathbb{Q}_p$. Un ejemplo de anillo p-ádico es el anillo de los enteros p-ádicos, $\mathbb{Z}_p$, puesto que es íntegramente cerrado, por ser un AVD (ver la Proposición 1.3.2 (ii)), y su cuerpo de cocientes es $\mathbb{Q}_p$.

Para terminar la sección, veremos un resultado relativo a módulos proyectivos en el que aparecen los anillos de valoración discreta, y del que haremos uso en la sección 3.4. No obstante, antes de enunciarlo necesitamos saber qué entendemos por un orden.

Si R es un dominio de Dedekind, un **R-orden** Λ es un anillo cuyo centro contiene a R, y cuyo R-módulo subyacente es finitamente generado y proyectivo, con relación a la acción de R sobre Λ inducida por la inclusión de R en el centro de Λ.

Teorema 1.3.16. *Sea R un AVD, $\mathfrak{p}$ su único ideal maximal, Λ un R-orden y M un Λ-módulo por la izquierda finitamente generado y proyectivo como R-módulo. Se definen $\overline{R} = R/\mathfrak{p}$, $\overline{\Lambda} = \Lambda/\mathfrak{p}\Lambda$ y $\overline{M} = M/\mathfrak{p}M$. Entonces*

M es Λ-proyectivo si, y solo si, $\overline{M}$ es $\overline{\Lambda}$-proyectivo.

Demostración. Ver [CR81, Teorema 30.11]. ∎

1.4. Teorema de Krull-Schmidt-Azumaya

Entre los muchos resultados que se aplican en la demostración de los Teoremas de Green se encuentra el Teorema de Krull-Schmidt-Azumaya, que abreviaremos como Teorema de K-S-A, y del que nos ocuparemos en esta sección. A denotará un anillo arbitrario. Comenzaremos por dar la definición de módulo indescomponible.

Diremos que un A-módulo por la izquierda M es **indescomponible** si $M \neq 0$ y M no se puede expresar como suma directa de A-módulos no nulos.

Aunque no proporcionaremos una demostración del Teorema de K-S-A, la siguiente proposición es clave para ella:

Proposición 1.4.1. *Sean M un A-módulo por la izquierda no nulo y $E = \mathrm{End}_A(M)$ su álgebra de endomorfismos. Supongamos que se cumple alguna de las siguientes dos condiciones:*

(i) Los A-submódulos de M satisfacen ambas condiciones de cadena.

(ii) M es un A-módulo finitamente generado, donde A es una R-álgebra, finitamente generada como R-módulo, siendo R un anillo local noetheriano conmutativo completo.

Entonces M es un A-módulo indescomponible si, y solo si, E es un anillo local.

Demostración. Ver [CR81, Proposición 6.10]. ∎

Teorema 1.4.2 (Teorema de Krull-Schmidt-Azumaya (K-S-A)). *Sea M un A-módulo por la izquierda finitamente generado, y supongamos que se cumple alguna de las siguientes dos condiciones:*

(i) Los A-submódulos de M satisfacen ambas condiciones de cadena.

(ii) A es una R-álgebra, finitamente generada como R-módulo, donde R es un anillo local noetheriano conmutativo completo.

Entonces M se puede expresar como una suma finita de submódulos indescomponibles. Además, si

$$M = \bigoplus_{i=1}^{r} M_i = \bigoplus_{j=1}^{s} N_j$$

son dos de tales sumas, entonces $r = s$ *y* $M_1 \cong N_{j_1}, \ldots, M_r \cong N_{j_r}$*, donde* $\{j_1, \ldots j_r\}$ *es alguna permutación de* $\{1, \ldots r\}$*. En resumen,* M *se puede expresar de forma única como una suma finita de submódulos indescomponibles, salvo isomorfismo y orden de aparición de los sumandos.*

Demostración. Ver [CR81, Teorema 6.12]. ■

Observemos que si A es una R-álgebra, finitamente generada como R-módulo, donde R es un cuerpo o un anillo de valoración discreta completo, entonces se verifica la condición (ii) del Teorema de K-S-A. Para terminar, algunos corolarios útiles de este teorema son los siguientes:

Corolario 1.4.3. *Sean* L*,* M *y* N *tres* A*-módulos por la izquierda que satisfacen las condiciones del Teorema de K-S-A (Teorema 1.4.2), y supongamos que*

$$L \oplus M \cong L \oplus N.$$

Entonces $M \cong N$*.*

Demostración. Ver [CR81, Corolario 6.15]. ■

Corolario 1.4.4. *Sea* L *un sumando directo de un* A*-módulo* M *como el del Teorema de K-S-A (Teorema 1.4.2). Entonces* L *es isomorfo a una subsuma de* $\bigoplus M_i$*.*

Demostración. Ver [CR81, Corolario 6.16]. ■

1.5. Extensiones no ramificadas y módulos absolutamente indescomponibles

El Teorema de Indescomponibilidad de Green se refiere a módulos absolutamente indescomponibles. Por tanto, hemos de introducir este concepto antes de abordar dicho teorema, así como algunos resultados ligados a él. A esto dedicaremos la presente sección. No obstante, necesitamos conocer previamente qué entendemos por una extensión no ramificada, así que empezaremos tratando este asunto.

Sea K un cuerpo, y sea L una extensión finita de K. Supongamos que A es un dominio noetheriano íntegramente cerrado, cuyo cuerpo de cocientes es

K, y que B es la clausura entera de A en L. Se puede ver que $K \cdot B = L$. En particular, el cuerpo de cocientes de B es L. Supongamos también que B es un A-módulo finitamente generado (hipótesis que se satisface, por ejemplo, si A es un AVD completo). Se cumple el siguiente resultado:

Proposición 1.5.1. *Si A es un dominio de Dedekind, entonces B es también un dominio de Dedekind.*

Demostración. Ver [Ser79, cap. I, Proposición 9]. ∎

Añadimos ahora la hipótesis de que A sea un dominio de Dedekind. Por el resultado anterior, también lo será B. Sea ahora $\mathfrak{B}$ un ideal primo no nulo de B. Si $\mathfrak{p} = \mathfrak{B} \cap A$, diremos que $\mathfrak{B}$ **divide** a $\mathfrak{p}$, y escribiremos $\mathfrak{B} \mid \mathfrak{p}$. Esto es equivalente a decir que $\mathfrak{B}$ contiene el ideal $\mathfrak{p}B$. Denotaremos por $e_{\mathfrak{B}}$ el exponente de $\mathfrak{B}$ en la descomposición de $\mathfrak{p}B$ en ideales primos. Por tanto,

$$\mathfrak{p}B = \prod_{\mathfrak{B}\mid\mathfrak{p}} \mathfrak{B}^{e_{\mathfrak{B}}}.$$

El entero $e_{\mathfrak{B}}$ recibe el nombre de **índice de ramificación** de $\mathfrak{B}$ en la extensión L/K.

Si $\mathfrak{B}$ divide a $\mathfrak{p}$, se tiene que $B/\mathfrak{B}$ y $A/\mathfrak{p}$ son cuerpos, puesto que todo ideal primo no nulo de un dominio de Dedekind es maximal. Además, $B/\mathfrak{B}$ es una extensión del cuerpo $A/\mathfrak{p}$. El grado de esta extensión se llama **grado de residuos** de $\mathfrak{B}$ en la extensión L/K, y se denota por $f_{\mathfrak{B}}$. (Si se quiere especificar K, se escribe $e_{\mathfrak{B}/\mathfrak{p}}$ y $f_{\mathfrak{B}/\mathfrak{p}}$ en lugar de $e_{\mathfrak{B}}$ y $f_{\mathfrak{B}}$.)

Cuando existe un único ideal primo $\mathfrak{B}$ que divide a $\mathfrak{p}$ y $f_{\mathfrak{B}} = 1$, se dice que L/K es **totalmente ramificada** en $\mathfrak{p}$. Cuando $e_{\mathfrak{B}} = 1$ y $B/\mathfrak{B}$ es separable sobre $A/\mathfrak{p}$, se dice que L/K es **no ramificada en** $\mathfrak{B}$. Si L/K es no ramificada en todos los ideales primos no nulos de B, se dice que L/K es **no ramificada**. (Para más detalles acerca de extensiones, se puede consultar [Ser79, cap. I, secc. 4].)

Ahora ya sabemos qué se entiende por una extensión (de cuerpos) no ramificada. A continuación introduciremos otro nuevo concepto, el de extensión de un anillo de valoración discreta.

Sea R el anillo de valoración discreta de una valoración discreta φ sobre un cuerpo K, sea P el único ideal maximal de R, y sea $\overline{R} = R/P$ su cuerpo

de clases de residuos. Supongamos que L una extensión del cuerpo K, y que la valoración φ se puede extender a una valoración discreta ϕ sobre L. Sean S el anillo de valoración de ϕ, P_1 su ideal maximal, y $\overline{S} = S/P_1$ su cuerpo de clases de residuos. En este caso se dice que el AVD S es una **extensión** del AVD R, y se cumplen las relaciones

$$R = K \cap S \quad \text{y} \quad P = R \cap P_1.$$

Además, se verifica que $\overline{S}$ es una extensión del cuerpo $\overline{R}$.

En los resultados que vienen a continuación, aparecerán dos AVD completos, R y S, siendo S una extensión de R. Para cada R-módulo M, la aplicación $M \to S \otimes_R M$, dada por $m \mapsto 1 \otimes m$, es un embebimiento (ver [CR81, Ejercicio 8.2]), e identificaremos siempre M con $1 \otimes M$, por lo que podremos escribir $S \otimes_R M$ como SM. Además, si tenemos una R-álgebra Λ, finitamente generada como R-módulo, y un Λ-módulo por la izquierda M finitamente generado, podremos construir la R-álgebra finitamente generada $S \otimes_R \Lambda$, que también se podrá escribir como $S\Lambda$, después de identificar Λ con su imagen $1 \otimes \Lambda$ en $S \otimes_R \Lambda$.

Estamos ya en condiciones de dar la definición de módulo absolutamente indescomponible:

Definición 1.5.2. *Sea R un AVD completo, y sea Λ una R-álgebra finitamente generada como R-módulo. Un Λ-módulo por la izquierda M finitamente generado indescomponible se dice que es* ***absolutamente indescomponible*** *si SM es un $S\Lambda$-módulo indescomponible para todo AVD S completo que es una extensión de R.*

Finalmente, se expondrán a continuación algunos resultados que se utilizarán en la demostración del Teorema de Indescomponibilidad de Green. Supondremos que R es un AVD completo, y denotaremos por $\overline{R}$ su cuerpo de clases de residuos. Además, dados una R-álgebra Λ finitamente generada como R-módulo y un Λ-módulo M por la izquierda finitamente generado, emplearemos la siguiente notación:

$$E(M) = \mathrm{End}_\Lambda(M), \ \widetilde{E}(M) = E(M)/\mathrm{rad}\, E(M).$$

Teorema 1.5.3. *Supongamos que $\overline{R}$ es un cuerpo perfecto. Sea Λ una R-álgebra finitamente generada como R-módulo, y sea M un Λ-módulo por la iz-*

quierda finitamente generado indescomponible. Entonces M es absolutamente indescomponible si, y solo si, $\widetilde{E}(M) \cong \overline{R}$.

Demostración. Ver [CR81, Teorema 30.29]. ■

Proposición 1.5.4. *Sea K el cuerpo de cocientes de R, y sea K' una clausura algebraica de K. Entonces existe una correspondencia $L \leftrightarrow F$ uno a uno, que conserva la inclusión, entre el conjunto de cuerpos L tales que $K \subseteq L \subseteq K'$ y son extensiones finitas no ramificadas de K, y el conjunto de cuerpos F que son extensiones finitas separables de $\overline{R}$. Si S es el anillo de valoración de L obtenido al extender el anillo de valoración de K a L, entonces S es un AVD completo, y el cuerpo de clases de residuos de S es el cuerpo F correspondiente a L.*

Demostración. Ver [Ser79, cap. III, secc. 5]. ■

Corolario 1.5.5. *Supongamos que $\overline{R}$ es un cuerpo perfecto. Sea Λ una R-álgebra finitamente generada como R-módulo, y sea M cualquier Λ-módulo por la izquierda finitamente generado. Entonces existe un AVD completo S, cuyo cuerpo de cocientes L es una extensión finita no ramificada de K, tal que $SM = \bigoplus_i N_i$, donde cada N_i es un $S\Lambda$-módulo absolutamente indescomponible, y $\widetilde{E}(N_i) \cong \overline{S}$ para todo i.*

Demostración. Ver [CR81, Corolario 30.31]. ■

1.6. Anillos de grupo

Vamos ahora a estudiar los anillos de grupo. Aunque los definiremos sobre anillos arbitrarios, a lo largo del trabajo consideraremos sobre todo anillos de grupo con coeficientes en anillos conmutativos. En este caso, como ya adelantamos en la sección 1.2 (Ejemplo 1.2.5 (iv)), los anillos de grupo son ejemplos de álgebras sobre anillos conmutativos. A lo largo de esta sección, G denotará un grupo multiplicativo y R un anillo arbitrario. El grupo de unidades de un anillo cualquiera A se denotará por $\mathcal{U}(A)$.

El **anillo de grupo de G con coeficientes en** R se denota por RG, y es un R-módulo libre para el cual G es una base. Por tanto, todo elemento

de RG tiene una expresión única $a = \sum_{g\in G} a_g g$, con $a_g \in R$ para todo $g \in G$ y

$$\mathrm{Supp}(a) = \{g \in G : a_g \neq 0\}$$

un conjunto finito, que recibe el nombre de **soporte** del elemento a. Aplicando la propiedad distributiva, el producto en RG queda determinado por la identidad

$$(rg)(sh) = (rs)(gh), \quad r, s \in R,\ g, h \in G.$$

Evidentemente, el anillo de grupo RG se puede definir de forma equivalente como el conjunto de las sumas finitas formales

$$\left\{ \sum_{g\in G} a_g g : a_g \in R \text{ para todo } g \in G \right\},$$

con adición y multiplicación definidas por

$$\sum_{g\in G} a_g g + \sum_{g\in G} b_g g = \sum_{g\in G} (a_g + b_g) g$$

y

$$\left(\sum_{g\in G} a_g g\right)\left(\sum_{h\in G} b_h h\right) = \sum_{g,h\in G} a_g b_h gh = \sum_{k\in G} c_k k,$$

donde

$$c_k = \sum_{k=gh} a_g b_h = \sum_{g\in G} a_g b_{g^{-1}k}.$$

Estas son las operaciones inducidas de forma natural en RG a partir de las operaciones en el grupo G y en el anillo R.

Observemos que RG es un anillo unitario, siendo $1_R 1_G$ el elemento neutro para la multiplicación. Además, este anillo está determinado salvo isomorfismo de anillos por la siguiente propiedad, cuya demostración es elemental:

Proposición 1.6.1 (Propiedad universal de los anillos de grupo). *Sean R un anillo y G un grupo. Entonces:*

(i) La aplicación $f_0 : R \to RG$ definida por $f_0(r) = r1_G$ es un homomorfismo de anillos, la aplicación $\phi_0 : G \to \mathcal{U}(RG)$ definida por $\phi_0(g) = 1_R g$ es un homomorfismo de grupos y se verifica que $f_0(r)\phi_0(g) = \phi_0(g)f_0(r)$ para todo $r \in R$ y $g \in G$.

(ii) Sean S un anillo conmutativo, $f : R \to S$ un homomorfismo de anillos y $\phi : G \to \mathcal{U}(S)$ un homomorfismo de grupos que satisface $f(r)\phi(g) = \phi(g)f(r)$ para todo $r \in R$ y $g \in G$. Entonces existe un único homomorfismo de anillos $F : RG \to S$ que satisface $Ff_0 = f$ y $F\phi_0 = \phi$, y viene dado por $F(\sum_{g\in G} a_g g) = \sum_{g\in G} f(a_g)\phi(g)$.

Hagamos ahora una pequeña apreciación. Cada elemento de RG de la forma $1_R g$, donde $g \in G$, se suele identificar con el elemento g del grupo, de acuerdo con el homomorfismo ϕ_0 de la Proposición 1.6.1 (i). Como consecuencia, G se puede ver como el subconjunto $1_R G$ de RG, luego podemos decir que G es un subgrupo de $\mathcal{U}(RG)$ y que el elemento neutro para la multiplicación de RG es 1_G.

Debido también a la Proposición 1.6.1 (i), la aplicación $f_0 : R \to RG$ definida por $f_0(r) = r1_G$ es un homomorfismo de anillos. Además, si R es conmutativo, entonces $f_0(R) \subseteq Z(RG)$, ya que, en tal caso,

$$f_0(r)\left(\sum_{g\in G} a_g g\right) = r1_G\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G}(ra_g)g$$

y

$$\left(\sum_{g\in G} a_g g\right) f_0(r) = \left(\sum_{g\in G} a_g g\right) r1_G = \sum_{g\in G}(a_g r)g$$

coinciden. Por tanto, si R es un anillo conmutativo, entonces el anillo de grupo RG es una R-álgebra, de acuerdo con la Definición 1.2.1.

Observación 1.6.2. Puesto que un anillo de grupo RG sobre un anillo conmutativo R tiene estructura de R-álgebra, se puede llamar también **álgebra de grupo**. No obstante, se suele reservar este nombre a los anillos de grupo KG sobre un cuerpo K.

Por la propiedad universal de los anillos de grupo (Proposición 1.6.1 (ii)), podemos extender el homomorfismo trivial $G \to \mathcal{U}(R)$, definido por $g \mapsto 1$, a un homomorfismo $\varepsilon_G : RG \to R$, que recibe el nombre de **homomorfismo de aumento**, y viene dado por

$$\varepsilon_G\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g.$$

Para cada elemento $a = \sum_{g\in G} a_g g$ de RG, la imagen $\varepsilon_G(a)$ de a por esta

aplicación se llama **aumento** de a. Observemos que el homomorfismo de aumento es suprayectivo, ya que para cada $r \in R$, se tiene que $\varepsilon_G(r1_G) = r$.

Si N es un subgrupo normal del grupo G, entonces la aplicación natural $G \to G/N \subseteq \mathcal{U}(R(G/N))$ se extiende por linealidad a un homomorfismo de anillos

$$\begin{array}{rccc} \varepsilon_{G,N}: & RG & \longrightarrow & R(G/N) \\ & \sum\limits_{g\in G} a_g g & \longmapsto & \sum\limits_{g\in G} a_g gN. \end{array}$$

El núcleo de ε_G se conoce como el **ideal de aumento** de RG, y lo denotaremos por $\mathrm{Aug}(RG)$. Asimismo, denotaremos por $\mathrm{Aug}_N(RG)$ el núcleo de $\varepsilon_{G,N}$. Se pueden probar las siguientes relaciones:

$$\mathrm{Aug}(RG) = \bigoplus_{g\in G\setminus\{1\}} R(g-1) \text{ como } R\text{-módulos},$$

$$\mathrm{Aug}_N(RG) = RG \cdot \mathrm{Aug}(RN) = \mathrm{Aug}(RN) \cdot RG.$$

En particular, $\varepsilon_{G,G} = \varepsilon_G$ y, por tanto, $\mathrm{Aug}(RG) = \mathrm{Aug}_G(RG)$. Además, $\varepsilon_{G,1}$ es la identidad en RG, luego $\mathrm{Aug}_1(RG) = 0$. Cuando no hay riesgo de confusión, el homomorfismo de aumento se puede denotar simplemente por ε, mientras que para el homomorfismo $\varepsilon_{G,N}$ se puede utilizar la notación ε_N.

Para concluir la sección, enunciaremos un resultado necesario para la demostración del Teorema de Indescomponibilidad de Green.

Teorema 1.6.3. *Sean p un entero primo, G un p-grupo finito y K un cuerpo de característica p. Entonces existe, salvo isomorfismo, exactamente un KG-módulo por la izquierda simple, concretamente el cuerpo K, sobre el que los elementos de G actúan trivialmente. Además, KG es un anillo local, y*

$$\operatorname{rad} KG = \bigoplus_{g\in G\setminus\{1\}} K(g-1)$$

como K-módulos. Por tanto, $\operatorname{rad} KG$ *coincide con el ideal de aumento de KG. También se verifica que todo KG-módulo proyectivo finitamente generado es libre.*

Demostración. Ver [CR81, Teorema 5.24]. ∎

En la sección 3.1 nos ocuparemos específicamente de los anillos de grupo enteros $\mathbb{Z}G$, es decir, aquellos con coeficientes en el anillo de los números enteros.

1.7. Anillos graduados, productos cruzados y anillos de grupo torcidos

En esta sección introduciremos los anillos graduados y, en particular, los productos cruzados. También mencionaremos los anillos de grupo torcidos como un caso especial del producto cruzado. A lo largo de la sección, G denotará un grupo multiplicativo. Comenzaremos tratando el concepto de anillo graduado.

Un **anillo graduado por** G es un anillo A que se puede expresar como

$$A = \bigoplus_{g \in G} A_g,$$

donde A_g es un subgrupo aditivo de A para cada $g \in G$, y $A_g A_h \subseteq A_{gh}$ para cualesquiera $g, h \in G$. Cada subgrupo A_g recibe el nombre de **componente homogénea de grado** g. Claramente, A_1 es un subanillo de A, su **anillo base**, que veremos que es unitario. Además, cada A_g es un A_1-bimódulo con las multiplicaciones por la izquierda y por la derecha. Se dice que A es un **anillo fuertemente graduado por** G si $A_g A_h = A_{gh}$ para cualesquiera $g, h \in G$. Por último, si el anillo graduado A tiene una estructura de R-álgebra $\varphi : R \to Z(A)$ sobre un anillo conmutativo R de forma que $\varphi(R) \subseteq A_1$, entonces se suele decir que A es una **R-álgebra graduada por** G.

Ejemplos 1.7.1. (i) Los anillos de polinomios son ejemplos de anillos graduados. Si R es un anillo y $X_1, \ldots, X_n$ son indeterminadas sobre R, entonces $R[X_1, \ldots, X_n]$ es un anillo graduado por $\mathbb{Z}$. En concreto, se tiene que $R[X_1, \ldots, X_n] = \bigoplus_{m \in \mathbb{Z}} A_m$, definiendo para cada entero $m \geq 0$ la componente homogénea de grado m como el conjunto de los polinomios homogéneos de dicho grado; para cada entero $m < 0$ se define A_m como el grupo trivial. Además, $R[X_1, \ldots, X_n]$ es también un anillo graduado por $\mathbb{Z}^n$, puesto que $R[X_1, \ldots, X_n] = \bigoplus_{m \in \mathbb{Z}^n} A_m$, donde cada componente homogénea A_m, con $m = (m_1, m_2, \ldots, m_n) \in \mathbb{Z}^n$, se define del siguiente modo: si se verifica que $m_1, \ldots, m_n \geq 0$, entonces se toma $A_m = \{a\, x_1^{m_1} x_2^{m_2} \cdots x_n^{m_n} : a \in R\}$; en caso contrario, se toma A_m como el grupo trivial.

(ii) Si $A = \bigoplus_{g \in G} A_g$ es un anillo graduado por G y H es un subgrupo de

G, entonces $B = \bigoplus_{h\in H} A_h$ es un anillo graduado por H. Si además H es normal en G, entonces A está graduado por G/H, definiendo para cada elemento x de G/H la componente homogénea de grado x como $A_x = \bigoplus_{g\in x} A_g$.

Veremos a continuación algunas propiedades elementales de los anillos graduados.

En primer lugar, probaremos que 1, el elemento neutro para la multiplicación de un anillo $A = \bigoplus_{g\in G} A_g$ graduado por un grupo G, pertenece a A_1. Puesto que $1 \in A$, de la descomposición de A en suma directa se desprende que $1 = \sum_{g\in G} x_g$ para ciertos elementos x_g de A_g únicos. Entonces, si $y \in A_h$, se tiene que

$$y = y \cdot 1 = \sum_{g\in G} yx_g.$$

Como $yx_g \in A_{gh}$, se verifica que

$$yx_g = \begin{cases} y & \text{si } g = 1 \\ 0 & \text{si } g \neq 1. \end{cases}$$

Ahora, esto también se cumple si se considera cualquier elemento y de A. En particular, se cumple para $y = 1$, luego $1 = x_1 \in A_1$ y $x_g = 0$ para $g \neq 1$.

También se verifica que si u_g es una unidad de A_g, entonces $u_g^{-1} \in A_{g^{-1}}$. Veámoslo. Como u_g^{-1} se puede expresar de la forma $u_g^{-1} = \sum_{h\in G} x_h$ para ciertos elementos x_h de A_h únicos, entonces

$$1 = u_g u_g^{-1} = \sum_{h\in G} u_g x_h.$$

Puesto que $1 \in A_1$ y $u_g x_h \in A_{gh}$, se tiene que

$$u_g x_h = \begin{cases} 1 & \text{si } h = g^{-1} \\ 0 & \text{si } h \neq g^{-1}. \end{cases}$$

Como u_g es una unidad, se cumple que $x_h = 0$ para todo $h \neq g^{-1}$, luego $u_g^{-1} = x_{g^{-1}} \in A_{g^{-1}}$.

Pasamos ahora a tratar el concepto de producto cruzado.

A partir de ahora, R denotará un anillo arbitrario. Consideramos dos aplicaciones $\sigma : G \to \mathrm{Aut}(R)$ y $\alpha : G \times G \to \mathcal{U}(R)$, y consideramos

$$R_\alpha^\sigma G = \bigoplus_{g \in G} R u_g.$$

Definimos la adición en $R_\alpha^\sigma G$ como cabe esperar. Entonces, el conjunto

$$\{u_g : g \in G\}$$

constituye una R-base de $R_\alpha^\sigma G$ como R-módulo. Definimos también una multiplicación, que estará determinada por las siguientes dos reglas:

$$u_g u_h = \alpha(g,h) u_{gh}, \quad g,h \in G$$

y

$$u_g r = \sigma_g(r) u_g, \quad g \in G,\ r \in R.$$

El lema que se enuncia a continuación establece las condiciones que han de verificar σ y α para que esta multiplicación dote a $R_\alpha^\sigma G$ de estructura de anillo. En realidad, todas las hipótesis de anillo se verifican de forma obvia excepto la asociatividad, y lo que establece el lema es qué hace falta para que la multiplicación sea asociativa.

Lema 1.7.2. *La multiplicación en $R_\alpha^\sigma G$ es asociativa si, y solo si, se verifican las siguientes propiedades para cualesquiera $g,h,k \in G$:*

(i) $\alpha(g,h)\,\alpha(gh,k) = \sigma_g(\alpha(h,k))\,\alpha(g,hk)$.

(ii) $\sigma_g \sigma_h = \eta_{g,h} \sigma_{gh}$, *donde* $\eta_{g,h} : R \to R$ *es la aplicación definida por* $\eta_{g,h}(r) = \alpha(g,h)\, r\, (\alpha(g,h))^{-1},\ r \in R$

Demostración. En primer lugar, por linealidad es fácil ver que la multiplicación en $R_\alpha^\sigma G$ es asociativa si, y solo si,

$$[(ru_g)(su_h)](tu_k) = (ru_g)[(su_h)(tu_k)]$$

para cualesquiera $g,h,k \in G$, $r,s,t \in R$.

Desarrollando la expresión del lado izquierdo, obtenemos

$$\begin{aligned}
[(ru_g)(su_h)](tu_k) &= (r\sigma_g(s)\, u_g u_h)(tu_k) = (r\sigma_g(s)\,\alpha(g,h) u_{gh})(tu_k) \\
&= r\sigma_g(s)\,\alpha(g,h)\,\sigma_{gh}(t)\, u_{gh} u_k \\
&= r\sigma_g(s)\,\alpha(g,h)\,\sigma_{gh}(t)\,\alpha(gh,k) u_{ghk}.
\end{aligned}$$

Hacemos lo mismo con la expresión del lado derecho:

$$\begin{aligned}(ru_g)[(su_h)(tu_k)] &= (ru_g)(s\sigma_h(t)\,u_hu_k) = (ru_g)(s\sigma_h(t)\,\alpha(h,k)u_{hk})\\ &= r\sigma_g(s\sigma_h(t)\,\alpha(h,k))\,u_gu_{hk}\\ &= r\sigma_g(s)\,\sigma_g(\sigma_h(t))\,\sigma_g(\alpha(h,k))\,\alpha(g,hk)\,u_{ghk}.\end{aligned}$$

Supongamos ahora que la multiplicación en $R^\sigma_\alpha G$ es asociativa. En este caso, las expresiones a las que acabamos de llegar coinciden. Entonces, haciendo $r = s = t = 1$, se tiene que

$$\alpha(g,h)\,\alpha(gh,k) = \sigma_g(\alpha(h,k))\,\alpha(g,hk)$$

para cualesquiera $g,h,k \in G$, es decir, se cumple la condición (i). Además, si volvemos a igualar las expresiones a las que hemos llegado anteriormente, haciendo $r = s = 1$ se obtiene que

$$\alpha(g,h)\,\sigma_{gh}(t)\,\alpha(gh,k) = \sigma_g(\sigma_h(t))\,\sigma_g(\alpha(h,k))\,\alpha(g,hk).$$

Ahora, como

$$\alpha(g,h)\,\sigma_{gh}(t) = \alpha(g,h)\,\sigma_{gh}(t)(\alpha(g,h))^{-1}\,\alpha(g,h) = \eta_{g,h}(\sigma_{gh}(t))\,\alpha(g,h),$$

se llega a que

$$\eta_{g,h}(\sigma_{gh}(t))\,\alpha(g,h)\,\alpha(gh,k) = \sigma_g(\sigma_h(t))\,\sigma_g(\alpha(h,k))\,\alpha(g,hk).$$

Teniendo en cuenta que se satisface la condición (i), se tiene que

$$\eta_{g,h}\,\sigma_{gh} = \sigma_g\,\sigma_h$$

para cualesquiera $g,h \in G$, es decir, se verifica la condición (ii).

Recíprocamente, supongamos que se cumplen las condiciones (i) y (ii). Entonces, del desarrollo de las expresiones anteriores se desprende que

$$[(ru_g)(su_h)](tu_k) = (ru_g)[(su_h)(tu_k)]$$

para cualesquiera $g,h,k \in G$, $r,s,t \in R$. Por tanto, la multiplicación en $R^\sigma_\alpha G$ es asociativa, con lo que queda probado el resultado. ■

Dadas dos aplicaciones $\sigma : G \to \mathrm{Aut}(R)$ y $\alpha : G \times G \to \mathcal{U}(R)$ que satisfacen las condiciones del Lema 1.7.2, se dice que la aplicación α es un **conjunto de factores** para la acción σ de G sobre $\mathcal{U}(R)$. Hemos visto que, bajo estas condiciones, $R_\alpha^\sigma G$ es un anillo, que recibe el nombre de **producto cruzado** de G sobre R, relativo a la acción σ y al conjunto de factores α.

El conjunto de factores α definido por $\alpha(g,h) = 1$, $g, h \in G$, se llama conjunto de factores **trivial**. Existen algunos casos particulares de productos cruzados $R_\alpha^\sigma G$ que reciben nombres especiales:

- Cuando el conjunto de factores $\alpha : G \times G \to \mathcal{U}(R)$ es trivial, $R_\alpha^\sigma G$ se llama **anillo de grupo inclinado** (*skew group ring* en la literatura en inglés), y se representa por $R^\sigma G$.
- En el caso de que la acción $\sigma : G \to \mathrm{Aut}(R)$ sea trivial, es decir, que $\sigma(g)$ sea la aplicación identidad en R para todo $g \in G$, $R_\alpha^\sigma G$ se denomina **anillo de grupo torcido** (*twisted group ring* en la literatura en inglés), y se denota por $R_\alpha G$.
- Finalmente, cuando son triviales tanto el conjunto de factores α como la acción σ, $R_\alpha^\sigma G$ es en realidad el anillo de grupo ordinario RG.

Por tanto, los anillos de grupo constituyen un caso particular de los anillos de grupo torcidos, los cuales son, a su vez, un caso particular de los productos cruzados.

Veremos a continuación que los productos cruzados $R_\alpha^\sigma G$ son anillos graduados por G, y también una condición que hace que un anillo graduado sea un producto cruzado.

Proposición 1.7.3. *Un anillo $A = \bigoplus_{g \in G} A_g$ graduado por un grupo G es un producto cruzado $R_\alpha^\sigma G$ con $R = A_1$ si, y solo si, cada componente homogénea A_g tiene un elemento invertible. Además, un anillo A graduado por G que verifica esta condición es un anillo fuertemente graduado por G.*

Demostración. Comenzaremos viendo el recíproco, es decir, que todo producto cruzado $A = R_\alpha^\sigma G$ es un anillo $\bigoplus_{g \in G} A_g$ graduado por un grupo G con $A_1 = R$, tal que cada componente homogénea A_g contiene una unidad. Sea $\{u_g : g \in G\}$ una R-base de A. Como $A = \bigoplus_{g \in G} Ru_g$, es fácil comprobar que

basta definir la componente homogénea de grado g como

$$A_g = Ru_g,$$

que para cualquier elemento g de G se verifica que u_g es una unidad de A, y que como A_1 se puede tomar el anillo R.

Supongamos ahora que disponemos de un anillo $A = \bigoplus_{g\in G} A_g$ graduado por un grupo G, tal que cada componente homogénea A_g contiene una unidad de A, a la que llamaremos a_g. Veamos que A es un producto cruzado.

Sabemos que para cada $g \in G$ se tiene que $A_1 a_g \subseteq A_g$ y $A_g a_g^{-1} \subseteq A_1$, ya que $a_g^{-1} \in A_{g^{-1}}$, por ser a_g una unidad de A. Por consiguiente, $A_1 a_g \subseteq A_g \subseteq A_1 a_g$, luego

$$A_g = A_1 a_g = a_g A_1 \tag{1.4}$$

para todo $g \in G$. Por tanto, se tiene que

$$A = \bigoplus_{g\in G} A_1 a_g = \bigoplus_{g\in G} a_g A_1,$$

por lo que todo elemento a de A se puede expresar de la forma $a = \sum_{g\in G} r_g a_g = \sum_{g\in G} a_g r'_g$ para ciertos elementos r_g, r'_g de A_1 únicos.

También por (1.4), si fijamos un elemento g de G, para cada $r \in A_1$ existe un elemento $\sigma_g(r)$ de A_1 tal que

$$a_g r = \sigma_g(r) a_g.$$

Se comprueba fácilmente que la aplicación $\sigma : G \to \mathrm{Aut}(\mathrm{A}_1)$, dada por $g \mapsto \sigma_g$, está bien definida.

Ahora, para cualesquiera $g, h \in G$ se cumple que $a_{gh} = a_g\, a_h\, r_{g,h}$, siendo $r_{g,h} = a_h^{-1} a_g^{-1} a_{gh}$. Teniendo en cuenta que $r_{g,h} \in A_1$, se tiene que $a_h\, r_{g,h} = \sigma_h(r_{g,h}) a_h$ y $a_g\, \sigma_h(r_{g,h}) = \sigma_g(\sigma_h(r_{g,h})) a_g$, luego

$$a_{gh} = a_g\, a_h\, r_{g,h} = a_g\, \sigma_h(r_{g,h}) a_h = \sigma_g(\sigma_h(r_{g,h})) a_g\, a_h.$$

Además, $\sigma_g(\sigma_h(r_{g,h})) \in \mathcal{U}(A_1)$, ya que a_g, a_h y a_{gh} son unidades. Entonces, si definimos la aplicación $\beta : G \times G \to \mathcal{U}(A_1)$ como $\beta(g,h) = \sigma_g\left(\sigma_h\left(a_h^{-1} a_g^{-1} a_{gh}\right)\right)$, se verifica que

$$a_{gh} = \beta(g,h) a_g\, a_h$$

para cualesquiera $g, h \in G$. Así, si definimos la aplicación $\alpha : G \times G \to \mathcal{U}(A_1)$ como $\alpha(g,h) = (\beta(g,h))^{-1}$, se llega a que

$$a_g\, a_h = \alpha(g,h) a_{gh}$$

para cualesquiera $g, h \in G$.

De todo lo anterior se deduce que $A = \bigoplus_{g \in G} A_1 a_g$ es el producto cruzado de G sobre A_1, relativo a la acción σ y al conjunto de factores α. El conjunto $\{a_g : g \in G\}$ constituye una A_1-base de $A = (A_1)^{\sigma}_{\alpha} G$.

Además, A es un anillo fuertemente graduado por G. Vamos a demostrar esto. Para ello, consideramos dos elementos g y h de G. Sabemos que $A_g A_h \subseteq A_{gh}$, por lo que basta probar la inclusión contraria. Ahora bien, como se verifica que

$$a_{gh} = \beta(g,h) a_g\, a_h \in A_1 a_g\, a_h,$$

por (1.4) se tiene que

$$A_{gh} = A_1 a_{gh} \subseteq A_1 A_1 a_g\, a_h \subseteq (A_1 a_g)(A_1 a_h) = A_g A_h.$$

■

Observación 1.7.4. De acuerdo con la Proposición 1.7.3, y en relación con el apartado (ii) de Ejemplos (1.7.1), se puede ver que si $R^{\sigma}_{\alpha} G$ es un producto cruzado, entonces $R^{\sigma}_{\alpha} H$ es un producto cruzado de H sobre R, y si H es normal en G, entonces podemos ver $R^{\sigma}_{\alpha} G$ como un producto cruzado $(R^{\sigma}_{\alpha} H)^{\beta}_{\tau} (G/H)$ de G/H sobre $R^{\sigma}_{\alpha} H$.

A diferencia de los anillos de grupo, los productos cruzados no tienen, en general, una base natural. Esto es evidente si son vistos como anillos graduados, pues para obtener una base basta tomar un elemento invertible de cada componente homogénea, y este no tiene por qué ser único. De hecho, si $R^{\sigma}_{\alpha} G$ es un producto cruzado y $\lambda : G \to \mathcal{U}(R)$ asigna a cada elemento g de G una unidad λ_g de R, entonces

$$\{v_g : v_g = \lambda_g u_g, g \in G\}$$

es una R-base alternativa de $R^{\sigma}_{\alpha} G$ que conserva la estructura original de producto cruzado. Un cambio de base como este se conoce con el nombre de

cambio de base diagonal. En efecto, como $\lambda_g \in \mathcal{U}(R)$ para todo $g \in G$, se tiene que

$$Rv_g = R\lambda_g u_g = Ru_g$$

para todo $g \in G$, por lo que

$$\bigoplus_{g\in G} Ru_g = \bigoplus_{g\in G} Rv_g.$$

Además, para cada $g \in G$, se cumple que

$$v_g\, r\, v_g^{-1} = \lambda_g u_g\, r\, u_g^{-1}\lambda_g^{-1} = \lambda_g\, \sigma_g(r) u_g\, u_g^{-1}\lambda_g^{-1} = \lambda_g\, \sigma_g(r)\lambda_g^{-1},$$

luego

$$v_g\, r = \lambda_g\, \sigma_g(r)\lambda_g^{-1} v_g.$$

Como consecuencia, la nueva acción $\sigma' : G \to \mathrm{Aut}(R)$ viene dada por $g \mapsto \sigma'_g$, con

$$\sigma'_g = \lambda_g\, \sigma_g \lambda_g^{-1}$$

para todo $g \in G$. Se puede comprobar que esta aplicación está bien definida. (Observemos que si R es conmutativo, el cambio de base diagonal no modifica la acción.) Veamos también cómo afecta el cambio de base al conjunto de factores. Se verifica que

$$\begin{aligned} v_g v_h &= \lambda_g u_g\, \lambda_h u_h = \lambda_g\, \sigma_g(\lambda_h) u_g u_h = \lambda_g\, \sigma_g(\lambda_h)\, \alpha(g,h) u_{gh} \\ &= \lambda_g\, \sigma_g(\lambda_h)\, \alpha(g,h)\lambda_{gh}^{-1} v_{gh} = \alpha(g,h)\left(\lambda_g\, \sigma_g(\lambda_h)\lambda_{gh}^{-1}\right) v_{gh}. \end{aligned}$$

Por tanto, el nuevo conjunto de factores es la aplicación $\beta : G \times G \to \mathcal{U}(R)$ dada por

$$\beta(g,h) = \alpha(g,h)\left(\lambda_g\, \sigma_g(\lambda_h)\lambda_{gh}^{-1}\right), \quad g,h \in G.$$

Puesto que el producto cruzado es asociativo, β y σ' satisfacen las condiciones (i) y (ii) del Lema 1.7.2. Así, es correcto llamar a β conjunto de factores, pues lo es para la nueva acción σ'. También la aplicación $\gamma_\lambda : G\times G \to \mathcal{U}(R)$ definida por

$$\gamma_\lambda(g,h) = \lambda_g\, \sigma_g(\lambda_h)\lambda_{gh}^{-1}, \quad g,h \in G,$$

es un conjunto de factores para la nueva acción.

De ahora en adelante, supondremos que R es un anillo conmutativo. Observemos que, con esta nueva suposición, la condición (ii) del Lema 1.7.2

significa que $\sigma : G \to \mathrm{Aut}(R)$ es un homomorfismo de grupos. Además, en el caso de que σ sea el homomorfismo trivial, $R^{\sigma}_{\alpha}G$ es un anillo de grupo torcido y tiene estructura de R-álgebra.

Para un homomorfismo $\sigma : G \to \mathrm{Aut}(R)$, definimos el siguiente conjunto de aplicaciones:

$$Z^2_\sigma(G,\mathcal{U}(R)) = \{\alpha : G \times G \to R \ : \ \alpha \text{ verifica la condición (i) del Lema 1.7.2}\}.$$

Se puede ver que $Z^2_\sigma(G,\mathcal{U}(R))$ es un grupo abeliano con la multiplicación

$$(\alpha\beta)(g,h) = \alpha(g,h)\,\beta(g,h), \quad g,h \in G.$$

Como ya hemos adelantado, los elementos de este grupo reciben el nombre de **conjuntos de factores** o **2-cociclos** para la acción σ de G sobre $\mathcal{U}(R)$.

Sea ahora

$$B^1_\sigma(G,\mathcal{U}(R)) = \{\lambda : G \longrightarrow \mathcal{U}(R) : \lambda \text{ es aplicación}\}.$$

Se puede ver que $B^1_\sigma(G,\mathcal{U}(R))$ es un grupo con la multiplicación

$$(\lambda\mu)(g) = \lambda(g)\,\mu(g), \quad g \in G.$$

Los elementos de este grupo se llaman **derivaciones** o **1-cobordes** para la acción σ de G sobre $\mathcal{U}(R)$.

No es difícil comprobar que la aplicación

$$\begin{array}{ccc} B^1_\sigma(G,\mathcal{U}(R)) & \longrightarrow & Z^2_\sigma(G,\mathcal{U}(R)) \\ \lambda & \longmapsto & \gamma_\lambda \end{array}$$

es un homomorfismo de grupos. La imagen de este homomorfismo, que es un subgrupo de $Z^2_\sigma(G,\mathcal{U}(R))$, se denotará por $B^2_\sigma(G,\mathcal{U}(R))$. Los elementos de este conjunto reciben el nombre de **conjuntos de factores principales** o **2-cobordes** para la acción σ de G sobre $\mathcal{U}(R)$.

Se dice que dos conjuntos de factores α y β para la acción σ de G sobre $\mathcal{U}(R)$ son **equivalentes** si $\alpha\beta^{-1} \in B^2_\sigma(G,\mathcal{U}(R))$. Por lo que hemos visto, mediante los cambios de base diagonales se obtienen conjuntos de factores equivalentes. Además, los anillos de grupo torcidos relativos a conjuntos de factores equivalentes son isomorfos. De hecho, se puede demostrar que

$$R_\alpha G \cong R_\beta G \text{ si, y solo si, } \alpha \text{ y } \beta \text{ son equivalentes.}$$

(Una prueba de este resultado, aunque en un contexto algo diferente, se puede encontrar en [Rei03, Teorema 29.6].) En particular,

$$R_\alpha G \cong RG \text{ si, y solo si } \alpha \in B^2(G,\mathcal{U}(R)). \tag{1.5}$$

(En el caso de anillos de grupos torcidos no hace falta especificar la acción σ, pues se trata de la acción trivial.)

Es fácil ver que el elemento neutro para la multiplicación en un producto cruzado $R_\alpha^\sigma G = \bigoplus_{g\in G} Ru_g$ es de la forma ru_1, con $r \in \mathcal{U}(R)$. Por tanto, mediante un cambio de base diagonal, podemos suponer que este elemento es u_1. Además, con esta suposición, existe un embebimiento de R en $R_\alpha^\sigma G$, que viene dado por $r \mapsto u_1 r$.

Definimos ahora el grupo cociente

$$H^2_\sigma(G,\mathcal{U}(R)) = Z^2_\sigma(G,\mathcal{U}(R))/B^2_\sigma(G,\mathcal{U}(R)),$$

que se conoce como el **segundo grupo de cohomología** de G con coeficientes en $\mathcal{U}(R)$ relativo a la acción σ.

Observación 1.7.5. Las definiciones que aparecen en [CR81, secc. 8B] de conjunto de factores, conjunto principal de factores, derivación o segundo grupo de cohomología parecen muy diferentes a las que hemos proporcionado en este trabajo. No obstante, únicamente se trata de definiciones más generales a las que hemos dado y, por tanto, podemos aplicar sin problema los resultados que aparecen en [CR81] relativos a todos estos conceptos.

Consideraremos ahora un cuerpo K, y utilizaremos la notación K^* para su grupo de unidades. El siguiente lema nos será de utilidad más adelante, así como la proposición que lo acompaña, que cierra la sección. Para ambos supondremos que G es un grupo finito y que disponemos de un anillo de grupo torcido $K_\alpha G$.

Lema 1.7.6. *El orden de todo elemento de $H^2(G,K^*)$ divide a $|G|$.*

Demostración. Ver [CR81, Lema 8.39]. ∎

Antes de enunciar la proposición, necesitamos saber qué entendemos por un p-elemento, dado un primo p. Se dice que un elemento x de un grupo finito G es un **p-elemento** si el orden de x es una potencia de p. Se dice que x

es un **p'-elemento** (o **elemento p-regular**) si el orden de x es coprimo con p. Un elemento que no es p-regular se dice que es **p-singular**. El elemento neutro es el único elemento de G que es simultáneamente un p-elemento y un p'-elemento.

Proposición 1.7.7. *Si K es un cuerpo perfecto de característica $p > 0$, entonces $H^2(G, K^*)$ no contiene p-elementos no triviales.*

Demostración. Ver [CR81, Lema 11.38] y la observación posterior a este lema. ■

La sección 1.1 ha sido realizada a partir de [ZS75, cap. II, seccs. 4–5].

Para la redacción de la sección 1.2 nos hemos basado fundamentalmente en [CR81, seccs. 1A, 5A, 6A, 23]. También hemos utilizado, aunque en menor medida, [Jan73, cap. I, secc. 2], [FD93, cap. 0], [CR62, secc. 16] y [Rei03, secc. 1].

Los resultados expuestos en la sección 1.3 están basados principalmente en [CR81, seccs. 4C, 6A, 23, 30], [Gou93, seccs. 2.1, 3.3], [Jan73, cap. I, secc. 3 y cap. II, seccs. 1, 2, 4, 5] y [Ser79, cap. II, secc. 4], aunque también se ha empleado [Neu99, secc. 3].

La sección 1.4 ha sido redactada a partir de [CR81, seccs. 6A, 6B], mientras que para la sección 1.5 se ha hecho uso de [CR81, seccs. 8, 19B, 30B] y [Ser79, cap. I, secc. 4 y cap. III, secc. 5].

Finalmente, hemos utilizado [Rio16, seccs. 1, 3] y [CR81, seccs. 1A, 5C] para elaborar la sección 1.6, y [CR81, seccs. 8B, 11C, 11E], [Pas89, cap. 1, seccs. 1–2] y [Rei03, secc. 29] para la sección 1.7.

Capítulo 2

Teoría de Representaciones. Teoremas de Green

Como hemos comentado al inicio, el objetivo principal de este trabajo es resolver el Problema del Espectro para el caso de grupos resolubles. En la resolución de este problema resultará fundamental la aplicación del Teorema de Green de los Ceros de Caracteres. En este capítulo nos adentraremos en el estudio de la Teoría de Representaciones, con el propósito de demostrar este teorema, que requiere de un paso previo importante: el Teorema de Indescomponibilidad de Green. Encaminados, pues, a la demostración de ambos Teoremas de Green, iniciamos este nuevo capítulo.

2.1. Representaciones de grupos

En esta sección se introducirán las representaciones de grupos. Este concepto es importante, pues los módulos sobre anillos de grupo, que aparecerán constantemente a lo largo del trabajo, se interpretarán en ocasiones en términos de representaciones de grupos, debido a la equivalencia que existe entre ambos conceptos, y que expondremos en breve. A lo largo de esta sección, R denotará un anillo conmutativo y G un grupo finito.

Dado un R-módulo M, se denotará por $\mathrm{Aut}_R(M)$ el grupo de los R-automorfismos de M, que es el grupo de unidades de la R-álgebra $\mathrm{End}_R(M)$ de

endomorfismos de M (ver Ejemplo 1.2.6). No es difícil probar que en el caso de que M sea un R-módulo libre de rango finito n, $\mathrm{End}_R(M)$ y $\mathcal{M}_n(R)$, las matrices cuadradas de orden n sobre R, son isomorfas como R-álgebras, por lo que se pueden identificar. Por consiguiente, también se puede identificar $\mathrm{Aut}_R(M)$ con el grupo de unidades de $\mathcal{M}_n(R)$, formado por las matrices invertibles de orden n, que se representará por $GL_n(R)$. Esto se pondrá de manifiesto cuando hablemos de representaciones matriciales de grupos.

Por una **representación de G sobre R** (o **R-representación de G**) entenderemos un par (M, ρ), donde M es un R-módulo y

$$\rho : G \longrightarrow \mathrm{Aut}_R(M)$$

es un homomorfismo de grupos. Por abuso del lenguaje, se suele llamar representación de G sobre R únicamente a la función ρ.

Se dice que dos representaciones (M_1, ρ_1) y (M_2, ρ_2) de G sobre R son **equivalentes** si existe un isomorfismo de R-módulos $f : M_1 \to M_2$ tal que

$$\rho_2(g) = f\rho_1(g)f^{-1}$$

para todo $g \in G$. Escribiremos $\rho_1 \sim \rho_2$ para indicar que ρ_1 es equivalente a ρ_2.

Empezaremos ahora a estudiar la relación entre módulos sobre anillos de grupo y representaciones de grupos. Consideramos un RG-módulo M, y definimos la aplicación $\rho_M : G \to \mathrm{Aut}_R(M)$ como

$$\rho_M(g)(m) = gm, \quad g \in G,\ m \in M.$$

Entonces (M, ρ_M) es una representación de G sobre R a la que nos referiremos como la **representación de G asociada a M**.

La siguiente observación nos será de utilidad para la prueba de la proposición que aparece a continuación:

Observación 2.1.1. Estamos acostumbrados a identificar un A-módulo por la izquierda, donde A es un anillo arbitrario, con un grupo abeliano M sobre el que A actúa de forma lineal. Sin embargo, un A-módulo por la izquierda también se puede ver como un grupo abeliano M junto con un homomorfismo de anillos $f : A \to \mathrm{End}(M)$, donde $\mathrm{End}(M)$ denota el anillo de endomorfismos del grupo aditivo M. En este caso, la multiplicación en el módulo viene dada

por $am = f(a)(m)$, y es fácil ver que $\mathrm{End}_A(M)$ es el centralizador de $f(A)$ en $\mathrm{End}(M)$. En particular, un RG-módulo por la izquierda es un grupo abeliano M junto con un homomorfismo de anillos $RG \to \mathrm{End}(M)$.

La siguiente proposición demuestra que el estudio de representaciones de G sobre R es equivalente al estudio de RG-módulos, como ya hemos comentado anteriormente:

Proposición 2.1.2. *La aplicación $M \to \rho_M$ es una correspondencia biyectiva entre RG-módulos y representaciones de G sobre R. Además, dos RG-módulos M y N son isomorfos si, y solo si, ρ_M y ρ_N son equivalentes, donde ρ_M y ρ_N son las representaciones de G asociadas a M y N, respectivamente.*

Demostración. Empezaremos probando la primera afirmación. Supongamos que $\rho_M : G \to \mathrm{Aut}_R(M)$ es la representación de G asociada a M. Entonces, por la propiedad universal de los anillos de grupo (Proposición 1.6.1 (ii)), ρ_M se extiende de forma única a un homomorfismo de anillos

$$\widehat{\rho}_M : RG \to \mathrm{End}_R(M)$$

dado por

$$\widehat{\rho}_M\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g \rho_M(g),$$

por lo que M es un RG-módulo por la izquierda.

Recíprocamente, sea M un RG-módulo por la izquierda, que se puede identificar con el homomorfismo de anillos $F : RG \to \mathrm{End}(M)$ definido por

$$F\left(\sum_{g\in G} a_g g\right)(m) = \left(\sum_{g\in G} a_g g\right) m. \tag{2.1}$$

Por la propiedad universal de los anillos de grupo (Proposición 1.6.1), este homomorfismo es equivalente a un par formado por un homomorfismo de anillos $f : R \to \mathrm{End}(M)$ y un homomorfismo de grupos $\rho : G \to \mathrm{Aut}(M)$ tales que $\rho(G)$ está contenido en el centralizador de $f(R)$ en $\mathrm{End}(M)$ ($\mathrm{Aut}(M)$ denota el grupo de automorfismos del grupo aditivo M). Como hemos comentado en la Observación 2.1.1, el centralizador de $f(R)$ en $\mathrm{End}(M)$ es $\mathrm{End}_R(M)$, por lo que $\rho(G)$ ha de estar contenido en $\mathrm{End}_R(M)$, es decir, $\rho : G \to \mathrm{Aut}_R(M)$. Además, por (2.1) y por la Proposición 1.6.1, se tiene que

$$\rho(g)(m) = F(g)(m) = gm, \quad g \in G,\ m \in M,$$

luego ρ es la representación de G asociada a M.

Probaremos ahora la segunda afirmación. Supongamos que existe un isomorfismo de RG-módulos $f : M \to N$. Sea n un elemento de N, y sea $m = f^{-1}(n)$. Se cumple que

$$\left(f\rho_M(g)f^{-1}\right)(n) = (f\rho_M(g))(m) = f(gm) = gf(m) = gn = \rho_N(g)(n)$$

para todo $g \in G$, luego ρ_M y ρ_N son equivalentes.

Recíprocamente, supongamos que ρ_M y ρ_N son equivalentes. Entonces existe un isomorfismo de R-módulos $f : M \to N$ tal que $f\rho_M(g)f^{-1} = \rho_N$ para todo $g \in G$. Ahora bien, f es también un isomorfismo de RG-módulos, puesto que para cada $g \in G$ y $m \in M$, se verifica que

$$f(gm) = (f\rho_M(g))(m) = \left(f\rho_M(g)f^{-1}\right)(f(m)) = \rho_N(g)(f(m)) = gf(m).$$

■

Por otra parte, si $\rho : G \to \mathrm{Aut}_R(M)$ es una representación de G sobre R y M es un R-módulo libre de rango finito n, entonces n se dice que es el **grado** de ρ, y se denota por $\deg(\rho)$.

A continuación abordaremos las representaciones matriciales de grupos y otros conceptos relacionados, análogos a los ligados a representaciones, así como las relaciones entre representaciones de grupos y representaciones matriciales.

Se llama **representación matricial de** G **sobre** R a cualquier homomorfismo de grupos

$$\lambda : G \longrightarrow GL_n(R),$$

donde $n \geq 1$. El entero n recibe el nombre de **grado** de la representación λ, y se denota por $\deg(\lambda)$.

Supongamos que M es un R-módulo libre de rango finito n. Entonces cualquier elección de una R-base de M conduce a la identificación de $\mathrm{Aut}_R(M)$ con el grupo $GL_n(R)$ de todas las matrices invertibles de orden n. Por tanto, si $\rho : G \to \mathrm{Aut}_R(M)$ es una representación de G sobre R, utilizando esta identificación podemos obtener una representación matricial

$$\rho^* : G \to GL_n(R)$$

de G sobre R, que diremos que es una **representación matricial de G correspondiente a ρ**. (En este caso, por una **representación matricial de G permitida por M** entenderemos una representación matricial correspondiente a la representación de G asociada a M, y la denotaremos por $\mathbf{M}$.) Recíprocamente, cada una de las representaciones ρ^* determina una representación $\rho : G \to \mathrm{Aut}_R(M)$, donde M es R^n (R-módulo de las matrices de tamaño $n \times 1$ sobre R), o cualquier R-módulo libre de rango n, y $\rho(g)(m) = \rho^*(g)m$.

Dos representaciones matriciales $\lambda_1 : G \to GL_n(R)$ y $\lambda_2 : G \to GL_k(R)$ de G sobre R diremos que son **equivalentes**, y lo denotaremos por $\lambda_1 \sim \lambda_2$, si $n = k$ y existe $M \in GL_n(R)$ tal que

$$\lambda_2(g) = M\lambda_1(g)M^{-1}$$

para todo $g \in G$.

Sea M un R-módulo libre de rango finito. Para cualquier representación $\rho : G \to \mathrm{Aut}_R(M)$, denotaremos por $\{\rho\}$ la clase de equivalencia de ρ, y por $\{\rho^*\}$ la clase de equivalencia de una representación matricial ρ^* correspondiente a ρ.

Proposición 2.1.3. *La aplicación $\{\rho\} \to \{\rho^*\}$ es una correspondencia biyectiva entre las clases de equivalencia de representaciones de G sobre R de la forma $\rho : G \to \mathrm{Aut}_R(M)$, donde M es un R-módulo libre de rango finito, y las clases de equivalencia de representaciones matriciales de G sobre R.*

Demostración. Claramente, basta verificar que $\rho_1 \sim \rho_2$ si, y solo si, $\rho_1^* \sim \rho_2^*$. Ahora bien, esto se deduce fácilmente de las definiciones de representaciones equivalentes. ■

Introduciremos a continuación el concepto de carácter de una representación y veremos algunas de sus propiedades.

Sea M un R-módulo libre de rango finito n, y sea $\rho : G \to \mathrm{Aut}_R(M)$ una representación de G sobre R. Sabemos que cualquier elección de una R-base de M permite identificar cada elemento f de $\mathrm{End}_R(M)$ con una matriz de orden n sobre R. Denotaremos por $\mathrm{tr}(f)$ la **traza** de f, es decir, la suma de los elementos de la diagonal principal de la matriz de orden n asociada a f.

Entonces la aplicación

$$\chi_\rho : G \longrightarrow R$$

definida por

$$\chi_\rho(g) = \mathrm{tr}(\rho(g)), \quad g \in G,$$

se llama **carácter** de ρ.

El **carácter** χ_λ de una representación matricial $\lambda : G \to GL_n(R)$ se define como $\chi_\lambda(g) = \mathrm{tr}(\lambda(g))$, donde $\mathrm{tr}(\lambda(g))$ es la traza de la matriz $\lambda(g)$.

Observemos que, dada cualquier representación matricial $\lambda : G \to GL_n(R)$, se verifica que $\lambda(1) = I_n$, donde I_n denota la matriz identidad de orden n sobre R. Por consiguiente, se tiene que $\chi_\lambda(1) = n$, el grado de la representación.

Proposición 2.1.4. *Se verifican las siguientes afirmaciones:*

(i) Representaciones equivalentes de G de la forma $\rho : G \to \mathrm{Aut}_R(M)$, donde M es un R-módulo libre de rango finito, tienen el mismo carácter.

(ii) $\chi_\rho = \chi_{\rho^*}$, donde ρ^* es cualquier representación matricial de G correspondiente a ρ.

(iii) $\chi_\rho(g^{-1}hg) = \chi_\rho(h)$ para cualesquiera $g, h \in G$, es decir, χ_ρ es una función constante en las clases de conjugación.

Demostración. Consecuencia directa de las definiciones y del hecho de que para cualquier par de matrices cuadradas A y B sobre R de orden n, se verifica que $\mathrm{tr}(AB) = \mathrm{tr}(BA)$, debido a que R es un anillo conmutativo, lo cual implica, a su vez, que $\mathrm{tr}(A) = \mathrm{tr}(B^{-1}AB)$ en el caso de que B sea no singular. ■

Sea M un RG-módulo que es libre de rango finito como R-módulo. Por el **carácter de G permitido por M** entenderemos el carácter de la representación de G asociada a M, que coincide con el carácter de cualquier representación matricial de G permitida por M.

El siguiente corolario es inmediato a partir de la Proposición 2.1.2 y la Proposición 2.1.4 (i):

Corolario 2.1.5. *Sean M y N dos RG-módulos que son libres de rango finito como R-módulos. Si M y N son isomorfos, los caracteres permitidos por ambos RG-módulos coinciden.*

Ejemplos 2.1.6. (i) Toda R-representación (M, ρ) de G tal que

$$\rho(g) = 1_M, \quad g \in G,$$

donde 1_M denota la aplicación identidad en M, se dice que es una **representación trivial**. Si M es un R-módulo libre de rango finito n, entonces una representación matricial $\rho^* : G \to GL_n(R)$ de G correspondiente a ρ viene dada por

$$\rho^*(g) = I_n, \quad g \in G.$$

Por tanto, el carácter de ρ viene dado por

$$\chi_\rho(g) = n, \quad g \in G.$$

(ii) La representación $\rho : G \to \mathrm{Aut}_R(RG)$ de G asociada al módulo regular $M = {}_{RG}RG$, es decir, el RG-módulo por la izquierda RG con la multiplicación en el anillo, se conoce como la **representación regular de G sobre R**. Esta representación está definida por

$$\rho(h)(g) = hg, \quad h, g \in G.$$

Podemos obtener una representación matricial $\rho^* : G \to GL_n(R)$ de G correspondiente a ρ respecto de la base G, siendo $n = |G|$. Como para cada elemento h de G, la aplicación $G \to G$ definida por $g \mapsto hg$ es un isomorfismo de grupos, entonces para cada $h \in G$, la matriz $\rho^*(h)$ contiene un único 1 en cada fila y columna, mientras que el resto de elementos son ceros. En concreto, $\rho^*(1) = I_n$, mientras que si $h \neq 1$, entonces $\rho^*(h)$ contiene en la fila correspondiente al elemento g de G un único 1 situado en la columna correspondiente al elemento $hg \neq g$, y ceros en los demás lugares. Por consiguiente, el carácter de ρ viene dado por

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

Para terminar la sección, veremos cómo calcular el carácter de un grupo permitido por una suma directa de módulos a partir de los caracteres permitidos por cada uno de los sumandos.

Proposición 2.1.7. *Para cada $i = 1, 2, \ldots, n$, sea $\chi_i : G \to R$ el carácter de G permitido por un RG-módulo M_i que es libre de rango finito como R-módulo. Entonces la aplicación $\sum_{i=1}^{n} \chi_i : G \to R$ dada por*

$$\left(\sum_{i=1}^{n} \chi_i\right)(g) = \sum_{i=1}^{n} \chi_i(g), \quad g \in G,$$

es el carácter de G permitido por $\bigoplus_{i=1}^{n} M_i$. Nos referiremos a $\sum_{i=1}^{n} \chi_i$ como la suma de caracteres $\chi_1, \ldots, \chi_n$.

Demostración. Se puede probar por inducción sobre n, para lo cual basta ver el caso $n = 2$. Sea ρ_i la representación matricial de G permitida por M_i relativa a la base B_i, $i = 1, 2$. Entonces, identificando cada elemento m_1 de M_1 con el elemento $(m_1, 0)$ de M, y haciendo lo mismo con los elementos de M_2, tenemos que $B = B_1 \cup B_2$ es una base de M. Es fácil ver que la representación matricial de G permitida por M relativa a la base B, que denotaremos por $\rho_1 \oplus \rho_2$, es

$$(\rho_1 \oplus \rho_2)(g) = \begin{pmatrix} \rho_1(g) & 0 \\ 0 & \rho_2(g) \end{pmatrix}, \quad g \in G.$$

Por tanto, si χ es el carácter de G permitido por M, se cumple que

$$\chi(g) = \mathrm{tr}((\rho_1 \oplus \rho_2)(g)) = \mathrm{tr}(\rho_1(g)) + \mathrm{tr}(\rho_2(g)) = \chi_1(g) + \chi_2(g).$$

■

2.2. Módulos y representaciones restringidas e inducidas

La técnica de representaciones restringidas e inducidas es uno de los métodos más importantes en Teoría de Representaciones. A lo largo de esta sección, R denotará un anillo conmutativo arbitrario, G será un grupo finito y H un subgrupo de G. Comenzaremos considerando el problema de construir RH-módulos a partir de RG-módulos, y viceversa. A continuación, nos ocuparemos de un teorema relativo a representaciones inducidas, el Teorema del Subgrupo de Mackey, que interviene en la demostración del Teorema de Green de los Ceros de Caracteres. Para finalizar la sección, trataremos las

representaciones restringidas e inducidas en el caso de disponer de módulos sobre determinadas álgebras graduadas.

Antes de comenzar, recordaremos brevemente algunas propiedades del producto tensorial de módulos, que utilizaremos en más de una ocasión. Las demostraciones de los resultados que enunciaremos a continuación las podemos encontrar en [CR62, secc. 12].

Sean A y B dos anillos, M un A-módulo por la izquierda y L un (B, A)-bimódulo. Entonces $L \otimes_A M$ tiene estructura de B-módulo por la izquierda con la multiplicación

$$b(l \otimes m) = bl \otimes m, \quad b \in B,\ l \in L,\ m \in M.$$

En particular, el anillo A es un (A, A)-bimódulo con las multiplicaciones en el anillo. Por tanto, para cada A-módulo por la izquierda M, $A \otimes_A M$ tiene estructura de A-módulo. Además, existe un isomorfismo natural de A-módulos

$$A \otimes_A M \cong M, \tag{2.2}$$

dado por la aplicación $a \otimes m \mapsto am$, $a \in A$, $m \in M$. Asimismo, se verifica el resultado análogo para A-módulos por la derecha.

También se cumplen las siguientes relaciones:

$$(L \oplus L') \otimes_A M \cong (L \otimes_A M) \oplus (L' \otimes_A M),$$

$$L \otimes_A (M \oplus M') \cong (L \otimes_A M) \oplus (L \otimes_A M').$$

Más aún, dada una familia de A-módulos por la derecha $\{L_\alpha\}$ y un A-módulo por la izquierda M, existe un isomorfismo natural de grupos aditivos

$$\left(\bigoplus_\alpha L_\alpha\right) \otimes_A M \cong \bigoplus_\alpha (L_\alpha \otimes_A M). \tag{2.3}$$

Se verifica también el resultado análogo para expresiones del tipo $L \otimes \left(\bigoplus_\beta M_\beta\right)$. Por tanto, el producto tensorial es distributivo respecto de la suma directa.

Por último, el siguiente resultado permite hablar de la asociatividad del producto tensorial: Dados dos anillos A y B, un A-módulo por la derecha

L, un (A,B)-bimódulo M y un B-módulo por la izquierda N, existe un isomorfismo natural de grupos aditivos

$$(L \otimes_A M) \otimes_B N \cong L \otimes_A (M \otimes_B N), \tag{2.4}$$

determinado por la aplicación $(l \otimes m) \otimes n \to l \otimes (m \otimes n)$, $l \in L$, $m \in M$ y $n \in N$.

Una vez hecho este repaso del producto tensorial, volvamos a nuestros problemas iniciales de construir RH-módulos a partir de RG-módulos, y viceversa. Estos problemas se pueden entender en un contexto general de Teoría de Anillos, y así los expondremos en principio.

Supongamos que $\varphi : B \to A$ es un homomorfismo de anillos. Entonces podemos obtener B-módulos por la izquierda a partir de A-módulos por la izquierda, y viceversa.

El primer problema es bastante sencillo. Sea M un A-módulo por la izquierda. Entonces podemos obtener un B-módulo por la izquierda, que denotaremos por $\varphi_*(M)$, cuyo grupo abeliano subyacente es M, y la multiplicación viene dada por

$$b \cdot m = \varphi(b)m, \quad b \in B,\ m \in M.$$

La operación $M \mapsto \varphi_*(M)$ se llama **restricción de escalares**, y a los módulos obtenidos mediante esta operación los llamaremos módulos **restringidos**.

Procederemos ahora a la construcción inversa, que es más complicada. En primer lugar, se tiene que A es un (A,B)-bimódulo, con la multiplicación por la izquierda dada por la multiplicación en el anillo, y la multiplicación por la derecha definida por

$$a \cdot b = a\varphi(b), \quad a \in A,\ b \in B.$$

Entonces cada B-módulo por la izquierda L define un A-módulo por la izquierda $\varphi^*(L)$, donde

$$\varphi^*(L) = A \otimes_B L.$$

La operación $M \mapsto \varphi^*(M)$ recibe el nombre de **inducción**, y a los módulos obtenidos mediante esta operación los denominaremos módulos **inducidos**. Además, por el resultado análogo a (2.2) para módulos por la derecha, se tiene que $\varphi^*(B) \cong A$.

Ahora vamos a aplicar estos resultados generales al caso de RG-módulos y RH-módulos, siendo H un subgrupo del grupo finito G. Para ello, consideraremos el homomorfismo inyectivo $\varphi : RH \to RG$ que surge de la aplicación inclusión de H en G. φ será vista como una aplicación inclusión, y podemos escribir $RH \subseteq RG$.

En este caso, la operación restricción de escalares asigna a cada RG-módulo por la izquierda M un RH-módulo por la izquierda, que denotaremos por $\mathrm{res}_H^G(M)$, aunque normalmente lo abreviaremos como $M|_H$ ó M_H. Supongamos ahora que M es un RG-módulo que es libre de rango finito n como R-módulo. Entonces, si $\mathbf{M} : G \to GL_n(R)$ es una representación matricial de G permitida por M, la representación matricial $\mathbf{M}|_H$ de H permitida por el módulo restringido $M|_H$ es la restricción del homomorfismo $\mathbf{M}$ al subgrupo H. Análogamente, si $\chi : G \to R$ es el carácter de $\mathbf{M}$, entonces el carácter $\chi|_H$ de $\mathbf{M}|_H$ es la restricción de la aplicación χ a H.

Por otra parte, la aplicación inducción de RH-módulos a RG-módulos asigna a cada RH-módulo por la izquierda L un RG-módulo por la izquierda, que denotaremos por $\mathrm{ind}_H^G(L)$, dado por

$$\mathrm{ind}_H^G(L) = RG \otimes_{RH} L.$$

Normalmente abreviaremos $\mathrm{ind}_H^G(L)$ como L^G. Se verifica que $\mathrm{ind}_H^G(RH) \cong RG$.

Supongamos que $\mathbf{L} : H \to GL_n(R)$ es una representación matricial de H permitida por un RH-módulo L. Se llama **representación (matricial) inducida**, y se denota por $\mathbf{L}^G$, a la representación matricial de G permitida por el módulo inducido L^G. Si $\chi : H \to R$ es el carácter de $\mathbf{L}$, se denota por χ^G el carácter de $\mathbf{L}^G$. Llamaremos a χ^G **carácter inducido**. A continuación, nos ocuparemos de determinar explícitamente la representación inducida $\mathbf{L}^G$ y el carácter inducido χ^G.

Sea $G = g_1H \cup g_2H \cup \cdots \cup g_nH$ una descomposición de G en clases laterales por la izquierda de H, de manera que $g_1 = 1 \in H$. Así, todo elemento de G se puede expresar de forma única como un producto g_ih, con $1 \leq i \leq n$ y $h \in H$. Por tanto, todo elemento de RG se puede expresar de forma única

como $\sum_{i=1}^{n} g_i b_i$, con $b_i \in RH$, luego

$$RG = \bigoplus_{i=1}^{n} g_i RH. \tag{2.5}$$

Por (2.3), tenemos que

$$L^G = RG \otimes_{RH} L = \bigoplus_{i=1}^{n} g_i RH \otimes L = \bigoplus_{i=1}^{n} g_i \otimes (RH)L = \bigoplus_{i=1}^{n} g_i \otimes L, \tag{2.6}$$

debido a que el producto tensorial se toma con respecto a RH.

Observemos que $g_1 \otimes L = 1 \otimes L$ es un RH-submódulo de $L^G|_{RH}$, y la aplicación

$$l \longmapsto 1 \otimes l, \quad l \in L, \tag{2.7}$$

es un RH-monomorfismo de L en L^G, debido al isomorfismo $RH \otimes_{RH} L \cong L$ (ver (2.2)). Además, todo sumando $g_i \otimes L$ de L^G se puede expresar como $g_i(1 \otimes L)$. Entonces se verifica que $1 \otimes L \cong g_i \otimes L$ como R-módulos, con el isomorfismo dado por la multiplicación por g_i por la izquierda.

Sea ahora g un elemento de G. Para cada $i = 1, \ldots, n$, se cumple que $gg_i \in g_j H$ para una única clase lateral por la izquierda $g_j H$. Por tanto, existen un único representante de clase g_j y un único elemento h de H tales que

$$gg_i = g_j h.$$

Como consecuencia, para cada $i = 1, \ldots, n$ y $l \in L$,

$$g(g_i \otimes l) = g_j h \otimes l = g_j \otimes hl. \tag{2.8}$$

luego $g(g_i \otimes L) = g_j \otimes L$, por lo que g permuta los sumandos $\{g_i \otimes L\}$.

Supongamos ahora que L permite una representación matricial $\mathbf{L}$, con respecto a la R-base finita $\{l_1, \ldots, l_m\}$ de L, de manera que

$$hl_j = \sum_{i=1}^{m} \alpha_{ij}(h) l_i, \quad \alpha_{ij}(h) \in R,$$

y $\mathbf{L}(h) = (\alpha_{ij}(h))$ para $h \in H$. Nuestro objetivo es calcular $\mathbf{L}^G(g)$, dado un elemento g de G. En primer lugar, por lo que hemos visto, los elementos

del conjunto $\{g_i \otimes l_j : i = 1, \ldots, n, j = 1, \ldots, m\}$ forman una R-base de L^G. Además, expresando $gg_i = g_j h$ como antes, tenemos que

$$g(g_i \otimes l_s) = g_j \otimes hl_s = \sum_{i=1}^{m} \alpha_{is}(h)(g_j \otimes l_i)$$

para $s = 1, \ldots, m$. Ahora bien, $gg_i = g_j h$ es equivalente a $g_j^{-1} g g_i = h$. Así, extendiendo las funciones coeficientes $\alpha_{ij} : H \to R$ de la matriz a aplicaciones $\dot{\alpha}_{ij} : G \to R$ definidas como

$$\dot{\alpha}_{ij}(g) = \begin{cases} \alpha_{ij}(g) & \text{si } g \in H, \\ 0 & \text{si } g \notin H, \end{cases}$$

llegamos a que

$$g(g_i \otimes l_s) = \sum_{i=1}^{m} \alpha_{is}(h)(g_j \otimes l_i) = \sum_{j=1}^{n} \sum_{i=1}^{m} \dot{\alpha}_{is}(g_j^{-1} g g_i)(g_j \otimes l_i).$$

También podemos extender $\mathbf{L}$ de H a G, definiendo

$$\dot{\mathbf{L}}(g) = (\dot{\alpha}_{ij}(g)), \quad g \in G.$$

Entonces la representación matricial permitida por L^G relativa a la base

$$\{g_1 \otimes l_1, \ldots, g_1 \otimes l_m, g_2 \otimes l_1, \ldots, g_2 \otimes l_m, \ldots, g_n \otimes l_1, \ldots, g_n \otimes l_m\}$$

viene dada por

$$g \longmapsto \mathbf{L}^G(g) = \begin{bmatrix} \dot{\mathbf{L}}(g_1^{-1} g g_1) & \cdots & \dot{\mathbf{L}}(g_1^{-1} g g_n) \\ \vdots & & \vdots \\ \dot{\mathbf{L}}(g_n^{-1} g g_1) & \cdots & \dot{\mathbf{L}}(g_n^{-1} g g_n) \end{bmatrix}. \tag{2.9}$$

Una vez encontrada la representación inducida, es fácil calcular el carácter inducido.

Sea $\chi : H \to R$ el carácter de H permitido por L, es decir,

$$\chi(h) = \operatorname{tr}(\mathbf{L}(h)), \quad h \in H.$$

Esta función también se puede extender a G de la siguiente manera:

$$\dot{\chi}(g) = \begin{cases} \chi(g) & \text{si } g \in H, \\ 0 & \text{si } g \notin H. \end{cases}$$

Entonces es inmediato a partir de (2.9) que el carácter χ^G de G permitido por L^G viene dado por

$$\chi^G(g) = \sum_{i=1}^{n} \dot{\chi}(g_i^{-1} g g_i), \quad g \in G. \tag{2.10}$$

Sin embargo, cuando $|H|$ es invertible en R, la siguiente fórmula, que no involucra a los representantes de clases $\{g_i\}$, proporciona una manera más cómoda de calcular el carácter inducido:

$$|H|\, \chi^G(g) = \sum_{x \in G} \dot{\chi}(x^{-1} g x) \tag{2.11}$$

para todo $g \in G$.

Procedemos a verificar la relación anterior. En primer lugar, se tiene que

$$\sum_{x \in G} \dot{\chi}(x^{-1} g x) = \sum_{\substack{x \in G: \\ x^{-1} g x \in H}} \chi(x^{-1} g x) = \sum_{i=1}^{n} \sum_{\substack{x \in g_i H: \\ x^{-1} g x \in H}} \chi(x^{-1} g x).$$

Además, el carácter es constante en las clases de conjugación (Proposición 2.1.4 (iii)), y para cualquier $x \in g_i H$, se tiene que

$$x^{-1} g x \in H \text{ si, y solo si, } g_i^{-1} g g_i \in H.$$

Por consiguiente,

$$\begin{aligned} \sum_{x \in G} \dot{\chi}(x^{-1} g x) &= \sum_{i=1}^{n} \sum_{\substack{x \in g_i H: \\ x^{-1} g x \in H}} \chi(g_i^{-1} g g_i) = \sum_{i=1}^{n} |g_i H|\, \dot{\chi}(g_i^{-1} g g_i) \\ &= |H| \sum_{i=1}^{n} \dot{\chi}(g_i^{-1} g g_i) = |H|\, \chi^G(g). \end{aligned}$$

Por tanto, si $|H|$ es invertible en R (es decir, si $|H| \cdot 1_R$ es invertible en R), el carácter inducido se puede calcular a partir de la fórmula

$$\chi^G(g) = \frac{1}{|H|} \sum_{x \in G} \dot{\chi}(x^{-1} g x).$$

Por último, veremos algunas propiedades generales de los módulos inducidos, comenzando por una caracterización de estos:

Proposición 2.2.1. *Sea H un subgrupo de G, y sea M un RG-módulo por la izquierda cuya restricción $M|_H$ contiene un RH-submódulo L tal que M es la suma directa $\bigoplus_{i=1}^{n} g_i L$ de los R-submódulos $\{g_i L\}$, donde $\{g_i : 1 \leq i \leq n\}$ es un conjunto de representantes de las clases laterales por la izquierda de H en G. Entonces $M \cong L^G$ como RG-módulos por la izquierda.*

Demostración. Es fácil comprobar que la aplicación $RG \times L \to M$ dada por $(g, l) \mapsto gl$ es R-bilineal y RH-equilibrada. Por tanto, existe un R-homomorfismo suprayectivo $\varphi : RG \otimes_{RH} L \to M$ tal que $\varphi(g_i \otimes_{RH} L) = g_i L$ para todo $1 \leq i \leq n$. Las hipótesis implican que existe un R-homomorfismo de M en L^G que es el inverso de φ, y que toma el valor $g_i \otimes_{RH} L$ sobre $g_i L$ para cada $1 \leq i \leq n$. Como consecuencia, φ es un R-isomorfismo. Ahora bien, por la forma en que está definido, y teniendo en cuenta el razonamiento de (2.8), φ es un RG-isomorfismo, y queda probado el resultado. ■

Proposición 2.2.2. *(i) (Aditividad de la inducción). Sea H un subgrupo de G, y sean L_1 y L_2 dos RH-módulos por la izquierda. Entonces:*

$$\mathrm{ind}_H^G(L_1 \oplus L_2) \cong \mathrm{ind}_H^G(L_1) \oplus \mathrm{ind}_H^G(L_2).$$

(ii) (Transitividad de la inducción). Sean H_1 y H_2 dos subgrupos de G tales que $H_1 \leq H_2$, y sea L un RH_1-módulo por la izquierda. Entonces:

$$\mathrm{ind}_{H_2}^G(\mathrm{ind}_{H_1}^{H_2}(L)) \cong \mathrm{ind}_{H_1}^G(L).$$

Demostración. (i) Se sigue de la distributividad del producto tensorial respecto de la suma directa (ver (2.3)):

$$\begin{aligned} \mathrm{ind}_H^G(L_1 \oplus L_2) &= RG \otimes_{RH} (L_1 \oplus L_2) \\ &\cong (RG \otimes_{RH} L_1) \oplus (RG \otimes_{RH} L_2) \\ &= \mathrm{ind}_H^G(L_1) \oplus \mathrm{ind}_H^G(L_2). \end{aligned}$$

(ii) Por la asociatividad del producto tensorial (ver (2.4)), junto con el isomorfismo $M \otimes_A A \cong M$ para un A-módulo por la derecha M (ver (2.2)), se tiene que

$$\begin{aligned} \mathrm{ind}_{H_2}^G(\mathrm{ind}_{H_1}^{H_2}(L)) &= RG \otimes_{RH_2} (RH_2 \otimes_{RH_1} L) \\ &\cong (RG \otimes_{RH_2} RH_2) \otimes_{RH_1} L \\ &\cong RG \otimes_{RH_1} L = \mathrm{ind}_{H_1}^G(L) \end{aligned}$$

como R-módulos. Además, todos los isomorfismos conmutan con la acción de G por la izquierda, de donde se sigue el resultado. ■

Observación 2.2.3. No es difícil probar que las mismas propiedades de la Proposición 2.2.2 se cumplen también para la restricción de escalares.

Corolario 2.2.4. *Sean H_1 y H_2 dos subgrupos de G tales que $H_1 \leq H_2$, y sea χ el carácter de H_1 permitido por un RH_1-módulo por la izquierda L que es libre de rango finito como R-módulo. Entonces*

$$\left(\chi^{H_2}\right)^G = \chi^G.$$

Demostración. Inmediata a partir de la Proposición 2.2.2 (ii) y el Corolario 2.1.5. ■

En breve enunciaremos y demostraremos el Teorema del Subgrupo de Mackey. No obstante, antes necesitamos hablar de los módulos conjugados.

Sea H un subgrupo de G. Utilizaremos la siguiente notación para los conjugados de elementos de H:

$${}^a h = aha^{-1}, h^b = b^{-1}hb = {}^{b^{-1}}h, \quad a, b \in G,\ h \in H.$$

Análogamente, los conjugados ${}^aH$ y H^a del subgrupo H se definen como

$${}^aH = aHa^{-1} = H^{a^{-1}}, \quad a \in G.$$

A continuación, se considerarán únicamente módulos por la izquierda y conjugados por el mismo lado, si bien las definiciones y resultados expuestos se pueden generalizar, combinando módulos y conjugados tanto por la izquierda como por la derecha.

Sea L un RH-módulo por la izquierda, y sea a un elemento de G. El **módulo conjugado** ${}^aL$ de L es el $R({}^aH)$-módulo por la izquierda con R-módulo subyacente L y multiplicación $*$ definida por

$${}^a h * l = h \cdot l, \quad h \in H,\ l \in L.$$

Si L es libre de rango finito como R-módulo, y $\mathbf{L}$ es una representación (matricial) de H permitida por L, con carácter χ, se define la **representación conjugada** ${}^a\mathbf{L}$ y el **carácter conjugado** ${}^a\chi$ de ${}^aH$ mediante las

fórmulas

$$^a\mathbf{L}(^ah) = \mathbf{L}(h),\ ^a\chi(^ah) = \chi(h), \quad h \in H.$$

Es fácil comprobar que estas definiciones son consistentes con la definición de módulo conjugado, es decir, que ^aL permite la representación $^a\mathbf{L}$ de ^aH, que tiene carácter $^a\chi$.

El siguiente lema recoge algunas propiedades de los módulos conjugados:

Lema 2.2.5. *Sea H un subgrupo de G, y sea L un RH-módulo por la izquierda. Se verifican las siguientes afirmaciones:*

(i) Si L es un submódulo de $M|_H$ para algún RG-módulo M, entonces aL es un $R(^aH)$-módulo por la izquierda, y $aL \cong {}^aL$.

(ii) $(^aL)^G \cong L^G$ como RG-módulos, para todo $a \in G$.

(iii) $^aL \cong L$ como RH-módulos si $a \in H$.

Demostración. (i) La aplicación $\varphi : L \to aL$ definida por $\varphi(l) = al$ es un R-isomorfismo. Además, $(^ah)(al) = a(hl)$ para todo $h \in H$ y $l \in L$, y se tiene que aL es un $R(^aH)$-módulo. Por último, para todo $h \in H$ y $l \in L$, se cumple que

$$\varphi(^ah * l) = \varphi(hl) = ahl = {}^ah(al) = (^ah)\varphi(l),$$

como queríamos probar.

(ii) Sea $\{g_i : 1 \le i \le n\}$ un conjunto de representantes de las clases laterales por la izquierda de H en G. Por (2.6), se cumple que

$$L^G = \bigoplus_{i=1}^{n} g_i \otimes_{RH} L.$$

Sea ahora a un elemento arbitario de G. Puesto que $G = \bigcup_{i=1}^{n} g_iH$, se tiene que $G = \bigcup_{i=1}^{n} ag_ia^{-1} \cdot {}^aH$, y de esto se sigue que $\{ag_ia^{-1} : 1 \le i \le n\}$ es un conjunto de representantes de las clases laterales por la izquierda de ^aH en G. Además, de acuerdo con (2.8), a permuta los sumandos $\{g_i \otimes L\}$, y se tiene que

$$L^G = \bigoplus_{i=1}^{n} a(g_i \otimes L) = \bigoplus_{i=1}^{n} ag_i(1 \otimes L) = \bigoplus_{i=1}^{n} (ag_ia^{-1})(a(1 \otimes L)).$$

Ahora, por (2.7) se verifica que $1 \otimes L \cong L$ como RH-módulos por la izquierda. Por tanto, debido al apartado (i) de este lema, se llega a que $a(1 \otimes L) \cong$

${}^aL$. Basta aplicar la Proposición 2.2.1 para concluir que $L^G \cong ({}^aL)^G$ como RG-módulos.

(iii) La aplicación ${}^aL \to L$ dada por $l \mapsto al$ proporciona el isomorfismo buscado. ■

Nos encontramos ya en condiciones de abordar el Teorema del Subgrupo de Mackey. Emplearemos la notación $Y \setminus G / X$ para el conjunto de las clases laterales dobles YgX de dos subgrupos Y y X en G.

Teorema 2.2.6 (Teorema del Subgrupo de Mackey). *Sean X e Y dos subgrupos de G, y sea L un RX-módulo por la izquierda. Entonces*

$$L^G|_Y \cong \bigoplus_{D=YaX} \left({}^aL|_{{}^aX\cap Y}\right)^Y,$$

donde la suma se toma sobre $Y \setminus G / X$. Los sumandos son independientes de la elección de los representantes de las clases laterales dobles, en el sentido de que

$$\left({}^aL|_{{}^aX\cap Y}\right)^Y \cong \left({}^bL|_{{}^bX\cap Y}\right)^Y$$

como RY-módulos siempre que $YaX = YbX$.

Nota. En términos de las notaciones *ind* y *res*, el resultado del teorema es el siguiente:

$$\operatorname{res}^G_Y\left(\operatorname{ind}^G_X(L)\right) \cong \bigoplus_{D=YaX} \operatorname{ind}^Y_{{}^aX\cap Y}\left(\operatorname{res}^X_{{}^aX\cap Y}({}^aL)\right).$$

Demostración. Sea

$$G = \bigcup_{i=1}^{n\cdot} g_i X$$

la descomposición de G en clases laterales por la izquierda de X. Por (2.6), podemos escribir

$$L^G = \bigoplus_{i=1}^{n} g_i \otimes L.$$

Para cada clase lateral doble $D \in Y \setminus G / X$, sea

$$W(D) = \bigoplus_{g_iX\subseteq D} g_i \otimes L.$$

Se tiene que $W(D)$ es un RY-submódulo de $L^G|_Y$, y es independiente de la elección de los representantes de clases $\{g_i\}$. Además, se cumple que

$$L^G|_Y = \bigoplus_D W(D).$$

Ahora nos queda averiguar la estructura de los RY-módulos $W(D)$. Sea $D = YaX$, y sea

$$Y = \dot{\bigcup_j} s_j({}^aX \cap Y)$$

la descomposición de Y en clases laterales por la izquierda de ${}^aX \cap Y$. Entonces

$$D = YaX = \bigcup_j s_j({}^aX \cap Y)aX = \bigcup_j s_j(aXa^{-1} \cap Y)aX = \dot{\bigcup_j} s_jaX,$$

y la última unión es disjunta debido a que

$$s_jaX = s_kaX \Leftrightarrow a^{-1}{s_j}^{-1}s_ka \in X \Leftrightarrow s_j^{-1}s_k \in {}^aX \cap Y \Leftrightarrow s_j({}^aX \cap Y) = s_k({}^aX \cap Y).$$

Por tanto, los elementos $\{s_ja\}$ son representantes de las clases laterales por la izquierda de X en D, y se tiene que

$$W(D) = \bigoplus_j s_ja \otimes L = \bigoplus_j s_j(a(1 \otimes L)).$$

Por (2.7), $L \cong 1 \otimes L$ como RX-módulos por la izquierda. Ahora, por el Lema 2.2.5 (i) se tiene que $aL \cong {}^aL$ como $R({}^aX)$-módulos. Por tanto, $a(1 \otimes L) \cong {}^aL$ como $R({}^aX)$-módulos, y también se cumple que $a(1 \otimes L) \cong {}^aL$ como $R({}^aX \cap Y)$-módulos. Entonces, por la Proposición 2.2.1 se tiene que

$$W(D) = \left({}^aL|_{{}^aX \cap Y}\right)^Y,$$

con lo que queda demostrada la primera afirmación del teorema.

Finalmente, el mismo argumento prueba que

$$W(D) = \left({}^bL|_{{}^bX \cap Y}\right)^Y$$

para cualquier otro elemento b de $D = YaX$, con lo que queda demostrada también la segunda parte. ■

Como hemos comentado anteriormente, para concluir la sección trataremos las representaciones restringidas e inducidas en el caso de disponer de módulos sobre determinadas álgebras graduadas.

Supongamos que tenemos un anillo conmutativo R y una R-álgebra $A = \bigoplus_{s \in S} A_s$ graduada por un grupo finito S. Supongamos también que A tiene estructura de producto cruzado de S sobre A_1, es decir, que cada componente

homogénea A_s contiene una unidad a_s. Sabemos que podemos tomar $a_1 = 1$; de ahora en adelante lo haremos siempre en esta situación. También sabemos que A_1 es una R-subálgebra de A. Si bien nos hemos centrado anteriormente en el caso particular de módulos sobre anillos de grupo, las operaciones de restricción de escalares y de inducción se pueden aplicar, en general, a módulos sobre R-álgebras. Por tanto, si M es un A-módulo por la izquierda, podemos construir el A_1-módulo obtenido por restricción de escalares de A a A_1, al que llamaremos módulo **restringido** y que denotaremos por M_{A_1}, o por $\mathrm{res}^A_{A_1}(M)$ cuando exista riesgo de confusión. Análogamente, para un A_1-módulo por la izquierda L, podemos considerar el A-módulo **inducido** $A \otimes_{A_1} L$, que denotaremos por L^A, o por $\mathrm{ind}^A_{A_1}(L)$.

De ahora en adelante, todos los módulos se supondrán finitamente generados como R-módulos, y el símbolo $\otimes$ denotará $\otimes_{A_1}$.

Para cada A_1-módulo L, se tiene que

$$L^A = \bigoplus_{s\in S} a_s A_1 \otimes L = \bigoplus_{s\in S} a_s \otimes L. \tag{2.12}$$

Por (1.4) se cumple que $A_1 a_s = a_s A_1$ para todo elemento s de S. Por tanto, todos los R-submódulos $\{a_s \otimes L\}$ son también A_1-submódulos de L^A, y se llaman **conjugados de L en L^A**. Además, como los elementos $\{a_s\}$ son unidades de A, la multiplicación por a_s por la izquierda define un R-isomorfismo

$$1 \otimes L \cong a_s(1 \otimes L) = a_s \otimes L.$$

Observemos también que $L \cong 1 \otimes L$ como A_1-módulos, y que $a_s \otimes L \cong a'_s \otimes L$ como A_1-módulos para cualesquiera dos unidades a_s y a'_s de A contenidas en A_s. Diremos que un A_1-módulo L es **estable** (o **estable relativo a** A) si L es isomorfo como A_1-módulo a todos sus conjugados.

Finalmente, veremos un resultado que nos será de utilidad más adelante, para el que tendremos en cuenta la Observación 1.2.7:

Proposición 2.2.7. *Supongamos que R es un anillo conmutativo y que $A = \bigoplus_{s\in S} A_s$ es una R-álgebra graduada por un grupo finito S. Consideremos que A tiene estructura de producto cruzado de S sobre A_1, es decir, que cada componente homogénea A_s contiene una unidad a_s. Supongamos también que L es un A_1-módulo por la izquierda y que E denota el álgebra de endomorfismos*

opuesta $(\mathrm{End}_A(L^A))^{op}$*, que será vista como un anillo de operadores por la derecha sobre* L^A*, el* A*-módulo inducido* $A \otimes_{A_1} L$*. Además, para cada* $s \in S$*, sea*

$$E_s = \{f \in E : (1 \otimes L)f \subseteq a_s \otimes L\}.$$

Entonces:

(i) Para cualesquiera $s, t \in S$*, se tiene que*

$$A_s(a_t \otimes L) = a_{st} \otimes L, \ (a_s \otimes L)E_t \subseteq a_{st} \otimes L,$$

$$E_s E_t \subseteq E_{st}, \ 1 \in E_1, \ E = \bigoplus_{s \in S} E_s.$$

(ii) Todo elemento φ *de* $(\mathrm{Hom}_{A_1}(1 \otimes L, a_s \otimes L))$ *se extiende a un único elemento* $\widehat{\varphi}$ *de* E_s*, dado por* $(a \otimes l)\widehat{\varphi} = a((1 \otimes l)\varphi)$ *para* $l \in L$, $a \in L$*. La aplicación* $\varphi \to \widehat{\varphi}$ *define un isomorfismo de* R*-módulos*

$$(\mathrm{Hom}_{A_1}(1 \otimes L, a_s \otimes L)) \cong E_s, \quad s \in S,$$

que para $s = 1$ *da lugar a un isomorfismo de* R*-álgebras* $(\mathrm{End}_{A_1}(L))^{op} \cong E_1$*.*

Demostración. Ver [CR81, Proposición 11.14]. ∎

2.3. Módulos proyectivos relativos y retículos

A continuación abordaremos los conceptos de módulo proyectivo relativo y de retículo, necesarios para comprender el Teorema de Green de los Ceros de Caracteres. A lo largo de esta sección, R denotará un anillo conmutativo, G un grupo finito y H un subgrupo de G. Además, todos los RG-módulos se supondrán finitamente generados como R-módulos, y se utilizará la notación

$$M \mid N$$

para indicar que el RG-módulo M es isomorfo a un sumando directo del RG-módulo N.

Comenzaremos tratando los módulos proyectivos relativos.

Definición 2.3.1. *Un RG-módulo M finitamente generado es* ***proyectivo relativo a*** *H, o* ***(G,H)-proyectivo****, si toda sucesión exacta corta de RG-módulos*

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

para la cual la sucesión exacta corta de restricciones a H

$$0 \to M'_H \to M''_H \to M_H \to 0$$

es RH-escindida, es necesariamente RG-escindida.

Aunque no la utilizaremos posteriormente, existe también la definición análoga de RG-módulo (G,H)-inyectivo:

Definición 2.3.2. *Un RG-módulo M finitamente generado es* ***inyectivo relativo a*** *H, o* ***(G,H)-inyectivo****, si toda sucesión exacta corta de RG-módulos*

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

para la cual la sucesión exacta corta de restricciones a H

$$0 \to M_H \to M'_H \to M''_H \to 0$$

es RH-escindida, es necesariamente RG-escindida.

Tenemos el siguiente resultado:

Teorema 2.3.3. *Sea M un RG-módulo finitamente generado, y sea H un subgrupo de G. Las siguientes afirmaciones son equivalentes:*

(i) *M es (G,H)-proyectivo.*

(ii) *M es (G,H)-inyectivo.*

(iii) *Sea $G = \dot{\bigcup}_{i=1}^{n} g_i H$. Entonces existe un elemento γ de $\mathrm{End}_{RH}(M_H)$ tal que*

$$\sum_{i=1}^{n} g_i \gamma g_i^{-1} = 1_M,$$

donde 1_M es la identidad en M.

(iv) *$M \mid (M_H)^G$.*

(v) *$M \mid L^G$ para algún RH-módulo L.*

Demostración. Ver [CR81, Teorema 19.2]. ∎

Para continuar, necesitamos introducir el concepto de RG-retículo. Un **RG-retículo** es un RG-módulo por la izquierda cuyo R-módulo subyacente es finitamente generado y proyectivo.

Observación 2.3.4. Es conveniente observar que si M es un RG-retículo, entonces M_H es un RH-retículo. Este hecho será usado más adelante en más de una ocasión.

Por último, la siguiente proposición también será de utilidad posteriormente:

Proposición 2.3.5. *Se cumplen las siguientes afirmaciones:*

(i) Los sumandos directos de RG-retículos son RG-retículos.

(ii) Si L es un RH-retículo, entonces L^G es un RG-retículo.

(iii) Sea M un RG-retículo tal que $M = M_1 \oplus M_2$, con M_1 y M_2 dos RG-retículos. Entonces M es (G,H)-proyectivo si, y solo si, M_1 y M_2 son (G,H)-proyectivos.

(iv) Si el índice $|G:H|$ es una unidad en R, entonces cada RG-módulo M es (G,H)-proyectivo, y $M \mid (M_H)^G$.

Demostración. Los tres primeros apartados no son difíciles de demostrar. Probaremos únicamente el último apartado:

(iv) Sea $G = \dot{\bigcup}_{i=1}^{n} g_i H$. Definimos $\gamma(m) = |G:H|^{-1} m$, para $m \in M$, con lo que tenemos que $\gamma \in \mathrm{End}_{RH}(M_H)$. Entonces $\sum_{i=1}^{n} g_i \gamma g_i^{-1} = 1_M$, y se deduce del Teorema 2.3.3 que M es (G,H)-proyectivo y que $M \mid (M_H)^G$. ∎

2.4. Teorema de Indescomponibilidad de Green

Estamos ya cerca de poder demostrar el Teorema de Indescomponibilidad de Green. Lo haremos al final de esta sección, después de ver los últimos resultados previos necesarios para ello.

A lo largo de esta sección, supondremos que G es un grupo finito, que p es un entero primo y que R es un AVD con ideal maximal P, tal que el

cuerpo de clases de residuos $\overline{R} = R/P$ es un cuerpo perfecto de característica p, y R es completo en la topología P-ádica. Se incluye el caso particular de que R sea un cuerpo perfecto de característica p (en este caso, se tiene que $P = 0$, y se puede identificar $\overline{R}$ con R).

Sea S un grupo finito, y sea $A = \bigoplus_{s\in S} A_s$ una R-álgebra graduada por S. Supongamos también que A es un producto cruzado de S sobre A_1, es decir, que cada componente homogénea A_s contiene una unidad a_s. Si L es un A_1-módulo por la izquierda, denotaremos por L^A el A-módulo inducido $A \otimes_{A_1} L$. Por (2.12) se tiene que

$$L^A = \bigoplus_{s\in S} a_s \otimes L.$$

Además, como por (1.4) se tiene que $a_s A_1 = A_1 a_s$ para todo $s \in S$, se cumple que cada $a_s \otimes L$ es un A_1-submódulo de L^A. El álgebra de endomorfismos opuesta $E = (\mathrm{End}_A(L^A))^{op}$ será vista como un anillo de operadores por la derecha sobre L^A, de acuerdo con la Observación 1.2.7.

Expondremos a continuación el último resultado previo al Teorema de Indescomponibilidad de Green y, seguidamente, dicho teorema, acompañado de su demostración.

Teorema 2.4.1. *Sea R un AVD completo con cuerpo de clases de residuos $\overline{R} = R/P$ perfecto de característica $p > 0$, siendo P el único ideal maximal de R. Supongamos que $A = \bigoplus_{s\in S} A_s$ es una R-álgebra graduada por un grupo finito S. Consideremos que A tiene estructura de producto cruzado de S sobre A_1, es decir, que cada componente homogénea A_s contiene una unidad a_s. Supongamos también que L es un A_1-módulo por la izquierda indescomponible, y que E denota el álgebra de endomorfismos opuesta $(\mathrm{End}_A(L^A))^{op}$, donde L^A es el A-módulo inducido $A \otimes_{A_1} L$. Además, para cada $s \in S$, sea*

$$E_s = \{f \in E : (1 \otimes L)f \subseteq a_s \otimes L\},$$

y sea

$$\widetilde{E}_1 = E_1/\mathrm{rad}\, E_1.$$

Supongamos que $\widetilde{E}_1 \cong \overline{R}$. Por último, sea

$$T = \{s \in S : 1 \otimes L \cong a_s \otimes L \text{ como } A_1\text{-módulos}\}.$$

Se verifican las siguientes afirmaciones:

(i) T *es un subgrupo de* S.

(ii) Existe un ideal bilátero J *de* E *tal que*

$$PE \subseteq J \subseteq \operatorname{rad} E,\ J = \bigoplus_{s\in S}(J \cap E_s),\ E_1 \cap J \cong \operatorname{rad} E_1$$

y E/J *es una* $\overline{R}$*-álgebra graduada por* T *que es un producto cruzado, con*

$$E/J = \bigoplus_{t\in T} E_t/(E_t \cap J).$$

Además, cada submódulo $E_t/(E_t \cap J)$ *es un* $\overline{R}$*-subespacio unidimensional de* E/J.

(iii) Sea

$$B = \bigoplus_{t\in T} A_t.$$

Sea $L^B = B \otimes_{A_1} L$, *y sea* $L^B = \bigoplus_{i=1}^{m} U_i$ *la descomposición de* L^B *en* B*-módulos indescomponibles* $\{U_i\}$. *Entonces*

$$L^A = \bigoplus_{i=1}^{m} U_i^A,\ \textit{donde } U_i^A = A \otimes_B U_i,$$

proporciona la descomposición de L^A *en* A*-módulos indescomponibles* $\{U_i^A\}$. *Además,* $U_i \cong U_j$ *como* B*-módulos si, y solo si,* $U_i^A \cong U_j^A$ *como* A*-módulos.*

(iv) Supongamos que L *es un* A_1*-módulo estable relativo a* A, *es decir, que los grupos* S *y* T *coinciden. Entonces cada descomposición* $L^A = \bigoplus W_i$ *en sumandos indescomponibles corresponde a una descomposición de* E/J *en ideales por la izquierda indescomponibles, conservándose los isomorfismos entre sumandos. Además,* E/J *es isomorfo a un anillo de grupo torcido de* S *sobre el cuerpo de clases de residuos* $\overline{R}$.

Demostración. Ver [CR81, Teoremas 19.19, 19.20, 19.21] y la demostración del primero de ellos. ■

Teorema 2.4.2 (Teorema de Indescomponibilidad de Green). *Sea* R *un AVD completo con cuerpo de clases de residuos* $\overline{R}$ *perfecto de característica* $p > 0$. *Sea* L *un* RH*-módulo absolutamente indescomponible, donde* H *es un subgrupo normal de* G *tal que* $|G : H| = p$. *Entonces el módulo inducido* L^G *es absolutamente indescomponible.*

Demostración. Por la Observación 1.7.4 (ver también la Proposición 1.7.3), $A = RG$ es una R-álgebra graduada por $S = G/H$ que tiene estructura de producto cruzado de S sobre $A_1 = RH$, siendo $A = \bigoplus_{s\in S} A_s$. Al ser L un RH-módulo absolutamente indescomponible, es un RH-módulo finitamente generado indescomponible. Por tanto, por el Teorema 1.5.3 tenemos que $\widetilde{E}(L) \cong \overline{R}$, donde $E(L) = (\mathrm{End}_{RH}(L))^{op}$ y $\widetilde{E}(L) = E(L)/\mathrm{rad}\, E(L)$. Ahora bien, por la Proposición 2.2.7 (ii) sabemos que $E_1 \cong (\mathrm{End}_{RH}(L))^{op} = E(L)$ como R-álgebras, puesto que $L \cong 1 \otimes_{RH} L$ como RH-módulos. Por consiguiente, $\widetilde{E}_1 = E_1/\mathrm{rad}\, E_1 \cong \widetilde{E}(L) \cong \overline{R}$, luego se cumplen las hipótesis del Teorema 2.4.1. Entonces, por el apartado (ii) de este teorema, existe un ideal bilátero J de $E = E(L^G) = (\mathrm{End}_{RG}(L^G))^{op}$ tal que

$$PE \subseteq J \subseteq \mathrm{rad}\, E,\ \ J = \bigoplus_{s\in S}(J \cap E_s)$$

y E/J es una $\overline{R}$-álgebra graduada por T que es un producto cruzado, con

$$E/J = \bigoplus_{t\in T} E_t/(E_t \cap J).$$

Ahora, como $|G : H| = p$, que es primo, solamente se pueden dar dos casos:

- Caso (i). El subgrupo $T = \{s \in S : 1 \otimes L \cong a_s \otimes L \text{ como } A_1\text{-módulos}\}$ del Teorema 2.4.1 es trivial.

  Por el Teorema 2.4.1 (ii) se tiene que $E_1 \cap J \cong \mathrm{rad}\, E_1$. Como T es trivial, aplicando este mismo teorema se llega a que

  $$E/J = E_1/(E_1 \cap J) \cong E_1/\mathrm{rad}\, E_1 = \widetilde{E}_1.$$

  Por tanto, se cumple que $E/J \cong \overline{R}$ y, como consecuencia, J es un ideal maximal de E.

  Empleando la notación del Teorema 2.4.1 (iii), se tiene que $B = A_1 = RH$, así como

  $$L^A = A \otimes_{A_1} L = RG \otimes_{RH} L = L^G$$

  y

  $$L^B = B \otimes_{A_1} L = RH \otimes_{RH} L \cong L.$$

  También por el Teorema 2.4.1 (iii), L^G es un RG-módulo indescomponible, al ser L un RH-módulo indescomponible. Entonces, por la

Proposición 1.4.1, E es un anillo local, luego $J = \operatorname{rad} E$. Como $\widetilde{E}(L^G) = E/\operatorname{rad} E$, se tiene que

$$\widetilde{E}(L^G) = E/J \cong \overline{R}.$$

Para concluir, del Teorema 1.5.3 se deduce que L^G es absolutamente indescomponible, y el teorema queda probado en este caso.

- Caso (ii). El subgrupo $T = \{s \in S : 1 \otimes L \cong a_s \otimes L \text{ como } A_1\text{-módulos}\}$ del Teorema 2.4.1 coincide con S y tiene orden p.

  En este caso, aplicamos el Teorema 2.4.1 (iv) para concluir que una descomposición de L^G en sumandos indescomponibles corresponde a una descomposición de E/J en ideales por la izquierda indescomponibles. Además, se sigue de la Proposición 1.2.16 que los sumandos correspondientes de L^G y E/J tienen las mismas álgebras de endomorfismos. (Con más precisión, por la Proposición 1.2.16 se tiene que los sumandos correspondientes de L^G y E tienen las mismas álgebras de endomorfismos, pero para concluir el resultado se ha de aplicar también el Teorema 1.3.9.)

  Aplicando de nuevo el Teorema 2.4.1 (iv), se tiene que E/J es isomorfo al anillo de grupo torcido $\overline{R}_\alpha S$ sobre el cuerpo perfecto $\overline{R}$ para algún conjunto de factores $\alpha : S \times S \to \overline{R}^*$, donde $\overline{R}^*$ es el grupo de unidades de $\overline{R}$. Ahora, por el Lema 1.7.6, el orden de todo elemento de $H^2\left(S, \overline{R}^*\right)$ divide a $|S| = p$, luego todos los elementos de $H^2\left(S, \overline{R}^*\right)$ son p-elementos. Además, puesto que $\overline{R}$ es un cuerpo perfecto de característica p, podemos aplicar la Proposición 1.7.7, según la cual $H^2\left(S, \overline{R}^*\right)$ no contiene p-elementos no triviales. Así, $H^2\left(S, \overline{R}^*\right)$ es el grupo trivial, por lo que $B^2\left(S, \overline{R}^*\right) = Z^2\left(S, \overline{R}^*\right)$. Por consiguiente, α es un conjunto de factores principal, y por (1.5) tenemos que $\overline{R}_\alpha S \cong \overline{R}S$. Como consecuencia, E/J es isomorfo al anillo de grupo $\overline{R}S$.

  Ahora, de acuerdo con el Teorema 1.6.3 se tiene que $\overline{R}S$ es un anillo local, y se cumple que

$$\operatorname{rad} \overline{R}S = \bigoplus_{s \in S \setminus \{1\}} \overline{R}(s-1)$$

como $\overline{R}$-módulos, luego $\operatorname{rad}\overline{R}S$ coincide con $\operatorname{Aug}(\overline{R}S)$, el ideal de aumento de $\overline{R}S$. Ahora bien, como el homomorfismo de aumento es suprayectivo, se verifica que $\overline{R}S/\operatorname{rad}\overline{R}S \cong \overline{R}$, por lo que $\overline{R}S/\operatorname{rad}\overline{R}S$ es indescomponible. Por tanto, por el Teorema 1.3.9 se tiene que $\overline{R}S$ es un ideal por la izquierda indescomponible, luego E/J también lo es y, por consiguiente, L^G es un RG-módulo indescomponible. Como consecuencia, L^G y E/J tienen las mismas álgebras de endomorfismos. Además, de nuevo por la Proposición 1.2.16 se llega a que el álgebra de endomorfismos de $E/J \cong \overline{R}S$ es $\overline{R}S$.

Por todo lo anterior, se verifica que

$$\widetilde{E}\left(L^G\right) \cong \left(\operatorname{End}_{RG}\left(E/J\right)\right)^{op}/\operatorname{rad}\left(\operatorname{End}_{RG}\left(E/J\right)\right)^{op} \cong \overline{R}S/\operatorname{rad}\overline{R}S \cong \overline{R},$$

y se deduce del Teorema 1.5.3 que L^G es absolutamente indescomponible, por lo que el teorema queda probado también en este segundo caso. ■

2.5. Teorema de Green de los Ceros de Caracteres

Iniciaremos esta sección proporcionando las definiciones de p-parte y p'-parte de un elemento de un grupo finito, dado un primo p, y a continuación veremos que, bajo ciertas hipótesis que consideraremos, el Teorema de K-S-A se verifica para los retículos. Estos son los últimos detalles que debemos conocer antes de proceder a la demostración del Teorema de Green de los Ceros de Caracteres, que utiliza gran cantidad de la teoría expuesta hasta este momento. Con la prueba de este teorema concluiremos el segundo capítulo del trabajo, que tenía como objetivo final presentar esta demostración.

Sea x un elemento de un grupo finito G. La descomposición del grupo cíclico $\langle x \rangle$ proporcionada por el Teorema Chino de los Restos muestra que, para cada primo p, existe una factorización

$$x = x'x'',$$

con x' un p-elemento y x'' un p'-elemento, tal que $x'x'' = x''x'$. Los factores x' y x'' se conocen como la **p-parte** de x, y la **p'-parte** (o **parte p-regular**) de x, respectivamente. Los elementos x' y x'' de G están determinados de forma única por estas propiedades.

A partir de ahora, supondremos que se cumplen las mismas hipótesis de la sección anterior, es decir, que G es un grupo finito, que p es un entero primo y que R es un AVD con ideal maximal P, tal que el cuerpo de clases de residuos $\overline{R} = R/P$ es un cuerpo perfecto de característica p, y R es completo en la topología P-ádica. Como ya comentamos en la sección anterior, se incluye el caso particular de que R sea un cuerpo perfecto de característica p (en este caso, se tiene que $P = 0$, y se puede identificar $\overline{R}$ con R).

Denotaremos por $\operatorname{Ind} RG$ el conjunto de todos los RG-retículos indescomponibles. La siguiente observación nos será de utilidad en la demostración del teorema al que se dedica esta sección:

Observación 2.5.1. Debido a las hipótesis que se consideran, el Teorema de K-S-A (Teorema 1.4.2) se verifica para todos los RG-retículos.

Por fin podemos probar este teorema, que nos será de utilidad en el capítulo siguiente:

Teorema 2.5.2 (Teorema de Green de los Ceros de Caracteres). *Sea R un AVD completo con cuerpo de clases de residuos $\overline{R}$ perfecto de característica $p > 0$. Sea M un RG-retículo tal que es (G, D)-proyectivo para algún p-subgrupo D de G. Sea x un elemento de G cuya p-parte u no es conjugada de ningún elemento de D. Entonces el carácter de G permitido por M se anula en x, es decir,*

$$\operatorname{tr}(x, M) = 0.$$

Demostración. En primer lugar, podemos hablar del carácter de G permitido por M porque M es un RG-módulo que es libre de rango finito como R-módulo. Esto se deduce de lo que vimos al final de la sección 1.2. (Con más precisión: Se tiene que M es un RG-retículo y, por consiguiente, como R-módulo es finitamente generado y proyectivo. Además, R es un AVD, luego es un DIP. Como consecuencia, M es un R-módulo finitamente generado libre de torsión, y, por tanto, es libre de rango finito como R-módulo.)

Observemos que basta probar el teorema en el caso de que M sea un RG-retículo indescomponible. En caso contrario, de acuerdo con la Observación 2.5.1 y la Proposición 2.3.5 (i), podríamos descomponer M como una suma directa

$$M = \bigoplus_{i=1}^{m} U_i, \text{ con } U_i \in \operatorname{Ind} RG.$$

Ahora, si suponemos probado el resultado para los RG-retículos indescomponibles, tendríamos que $\operatorname{tr}(x, U_i) = 0$ para todo $i = 1, \ldots, m$, puesto que, gracias a los apartados (i) y (iii) de la Proposición 2.3.5, se mantendrían las hipótesis del teorema para cada uno de los sumandos indescomponibles. Entonces, por la Proposición 2.1.7 se cumpliría que $\operatorname{tr}(x, M) = \sum_{i=1}^{m} \operatorname{tr}(x, U_i) = 0$. Podemos suponer, por tanto, que $M \in \operatorname{Ind} RG$.

Sea u la p-parte de x. Por hipótesis, u no es conjugado de ningún elemento de D y, en particular, $u \notin D$. Definimos $X = \langle x \rangle$ e $Y = \langle x^p \rangle$. Al ser $u \neq 1$, se tiene que $p \mid o(x)$ y, por consiguiente, $o(x^p) = o(x)/p$. En consecuencia, $|X : Y| = p$.

Además, como para cualquier elemento a de G se verifica que $u \notin {}^aD$, se llega a que

$${}^aD \cap X \leq Y \text{ para todo } a \in G,$$

teniendo en cuenta que ${}^aD \cap X$ es un subgrupo cíclico de X.

Ahora bien, como M es (G, D)-proyectivo, por la Proposición 2.3.3 (iv) se cumple que $M \mid (M_D)^G$. Por tanto, se verifica que $M \mid L^G$ para algún RD-retículo L. Además, puesto que M es indescomponible, por el Teorema de K-S-A (Proposición 1.4.2) se puede suponer que L también lo es, debido a la aditividad de la inducción (Proposición 2.2.2 (i)), luego $L \in \operatorname{Ind} RD$.

También se verifica que $M_X \mid (L^G)_X$ y, por el Teorema del Subgrupo de Mackey (Proposición 2.2.6), se tiene que para todo $a \in G$,

$$(L^G)_X \cong \bigoplus_{XaD} ({}^aL_{{}^aD \cap X})^X.$$

Sabemos que ${}^aL_{{}^aD \cap X}$ es un $R({}^aD \cap X)$-retículo y, puesto que ${}^aD \cap X \leq Y \leq X$, se cumple que $({}^aL_{{}^aD \cap X})^X \cong \left(({}^aL_{{}^aD \cap X})^Y\right)^X$ por la transitividad de la inducción (Proposición 2.2.2 (ii)). Por tanto,

$$(L^G)_X \cong \bigoplus_{XaD} \left(({}^aL_{{}^aD \cap X})^Y\right)^X.$$

Ahora, por la Proposición 2.3.5 (ii), se tiene que $({}^{a}L_{{}^{a}D\cap X})^{Y}$ es un RY-retículo y, en virtud de la Observación 2.5.1 y la Proposición 2.3.5 (i), podemos escribir

$$({}^{a}L_{{}^{a}D\cap X})^{Y} = \bigoplus_{j} N_j$$

para ciertos RY-retículos indescomponibles N_j. Es más, podemos suponer, por el Corolario 1.5.5, considerando una extensión adecuada de R (lo cual no afecta a la función traza), que los $\{N_j\}$ son RY-retículos absolutamente indescomponibles. Por otra parte, sabemos que $X = \langle x\rangle$ es un subgrupo cíclico de G y, por consiguiente, $Y = \langle x^p\rangle$ es un subgrupo normal de X con $|X : Y| = p$. Por tanto, podemos aplicar el Teorema de Indescomponibilidad de Green (Teorema 2.4.2) y afirmar que cada RX-módulo N_j^X es un RX-retículo indescomponible.

Ahora bien, hemos visto anteriormente que $M_X \mid (L^G)_X$, por lo que, aplicando la aditividad de la inducción y el Corolario 1.4.4, llegamos a que M_X es isomorfo a la suma directa de algunos de los módulos $\left\{N_j^X\right\}$. Veamos a continuación que $\mathrm{tr}\left(x, N_j^X\right) = 0$ para todo j.

Sea $\chi_j : Y \to R$ el carácter permitido por el RY-módulo N_j. De acuerdo con (2.11), si $\chi_j^X : X \to R$ es el carácter permitido por el RX-módulo N_j^X, se verifica que

$$|Y|\,\chi_j^X(z) = \sum_{y\in X} \dot{\chi}\left(y^{-1}zy\right),$$

donde $\dot{\chi} : X \to R$ es la extensión a X de la función χ, y está definida de la forma

$$\dot{\chi}(z) = \begin{cases} \chi(z) & \text{si } z \in Y \\ 0 & \text{si } z \notin Y. \end{cases}$$

Ahora, como $X = \langle x\rangle$ es abeliano, se tiene que

$$|Y|\,\chi_j^X(z) = \sum_{y\in X} \dot{\chi}(z)$$

para todo $z \in X$. En particular, como $x \notin Y = \langle x^p\rangle$, se verifica que

$$|Y|\,\chi_j^X(x) = \sum_{y\in X} \dot{\chi}(x) = 0.$$

Como consecuencia, se llega a que

$$\mathrm{tr}\left(x, N_j^X\right) = \chi_j^X(x) = 0$$

para todo j.

Para finalizar, únicamente hemos de tener en cuenta la Proposición 2.1.7. Puesto que M_X es isomorfo a la suma directa de algunos de los módulos $\left\{N_j^X\right\}$, se puede escribir $M = \bigoplus_{j\in J} N_j^X$ para algún conjunto de índices J, de donde se concluye que

$$\operatorname{tr}(x, M) = \operatorname{tr}(x, M_X) = \sum_{j\in J} \operatorname{tr}\left(x, N_j^X\right) = 0.$$

■

Para la redacción de la sección 2.1 hemos utilizado principalmente [Kar92, cap. 17, secc. 1] y, en menor medida, [FD93, cap. 0] y [Rio16, secc. 3].

Los resultados expuestos en la sección 2.2 están basados en [CR81, seccs. 10A, 10B, 11C] y [CR62, secc. 12], si bien para el repaso del producto tensorial de módulos hemos empleado [CR81, secc. 2B].

Por último, para elaborar la sección 2.3 se ha utilizado [CR81, seccs. 10D, 19A], mientras que las secciones 2.4 y 2.5 se han realizado a partir de [CR81, seccs. 1B, 19B, 19C].

Capítulo 3

El Problema del Espectro y su resolución para grupos resolubles

Este es el capítulo fundamental del trabajo, pues en él lograremos el objetivo que nos planteamos al inicio: exponer la resolución del Problema del Espectro para grupos resolubles, llevada a cabo por Martin Hertweck en [Her08b]. Es aquí donde aplicaremos el Teorema de Green de los Ceros de Caracteres, con el que concluimos el capítulo anterior. Como el problema planteado hace referencia a anillos de grupo enteros, parece lógico comenzar con el estudio de este tipo de anillos.

3.1. Anillos de grupo enteros

A lo largo de esta sección, G denotará un grupo finito. En la sección 1.6 estudiamos los anillos de grupo en general. Ahora nos restringiremos al caso en que el anillo de coeficientes es $\mathbb{Z}$. Este tipo de anillos de grupo reciben el nombre de **enteros**.

Como veremos en el siguiente capítulo, muchos problemas en el campo de los anillos de grupo enteros surgen al preguntarse hasta qué punto el anillo $\mathbb{Z}G$ refleja las propiedades del grupo G sobre el que se construye. Así, el Problema del Espectro trata de relacionar los órdenes de las unidades de orden finito de $\mathbb{Z}G$ que tienen aumento 1 con los órdenes de los elementos de

G. Empezaremos entonces por estudiar el grupo de unidades de $\mathbb{Z}G$.

El grupo $\mathcal{U}(\mathbb{Z}G)$ tiene algunos subgrupos finitos obvios, como G y el conjunto $\pm G$ formado por los elementos de G y sus opuestos. Los elementos de $\pm G$ se llaman **unidades triviales** de $\mathbb{Z}G$.

Recordemos que un elemento de un grupo se dice que es un **elemento de torsión** si tiene orden finito. El siguiente teorema nos será bastante útil:

Teorema 3.1.1 (Teorema de Berman-Higman). *Si $u = \sum_{g\in G} u_g g$ es una unidad de torsión de $\mathbb{Z}G$, entonces o bien $u = \pm 1$, o bien $u_1 = 0$.*

Demostración. Una observación clave para esta demostración es que toda matriz invertible compleja de orden finito es diagonalizable. Esto es consecuencia del hecho de que una matriz elemental de Jordan

$$J_k(a) = \begin{pmatrix} a & & & & \\ 1 & a & & & \\ & \ddots & \ddots & & \\ & & 1 & a & \\ & & & 1 & a \end{pmatrix} \in \mathcal{M}_k(\mathbb{C})$$

es de orden finito si, y solo si, $k = 1$ y a es una raíz de la unidad.

Consideramos la representación regular de G sobre $\mathbb{C}G$, es decir, el homomorfismo $G \to \mathrm{End}_{\mathbb{C}}(\mathbb{C}G)$ que asocia a cada elemento g de G la aplicación $\rho(g) : x \mapsto gx$. Utilizamos la misma notación para la representación matricial correspondiente a ρ en la base G, que es un homomorfismo de grupos $\rho : G \to GL_n(\mathbb{C})$, donde $n = |G|$. De acuerdo con el apartado (ii) de Ejemplos 2.1.6, la traza de $\rho(1)$ es $|G|$, y si $g \in G \setminus \{1\}$, entonces la traza de $\rho(g)$ es 0. Por la propiedad universal de los anillos de grupo (Proposición 1.6.1), ρ se extiende a un homomorfismo de $\mathbb{C}$-álgebras $\rho : \mathbb{C}G \to \mathcal{M}_n(\mathbb{C})$.

Supongamos que $u = \sum_{g\in G} u_g g$ es una unidad de torsión de $\mathbb{Z}G$, y sea m su orden. Por la observación del principio, se tiene que la matriz $\rho(u)$ es diagonalizable, y es conjugada en $\mathcal{M}_n(\mathbb{C})$ de una matriz diagonal $\mathrm{diag}(\xi_1, \ldots, \xi_n)$, donde cada ξ_i es una raíz m-ésima compleja de la unidad. Como la aplicación traza $\mathrm{tr} : \mathcal{M}_n(\mathbb{C}) \to \mathbb{C}$ es $\mathbb{C}$-lineal, se cumple que

$$nu_1 = \sum_{g\in G} u_g \mathrm{tr}(\rho(g)) = \mathrm{tr}(\rho(u)) = \mathrm{tr}(\mathrm{diag}(\xi_1, \ldots, \xi_n)) = \sum_{i=1}^{n} \xi_i.$$

Tomando valores absolutos y teniendo en cuenta que $|\xi_i| = 1$ para todo i, se tiene que

$$n\,|u_1| \leq \sum_{i=1}^{n} |\xi_i| = n,$$

y se da la igualdad si, y solo si, todos los ξ_i son iguales. Por tanto, si no todos los ξ_i son iguales, u_1 ha de ser un entero con valor absoluto menor que 1, es decir, $u_1 = 0$. En otro caso, $\mathrm{diag}(\xi_1, \ldots, \xi_n) = \xi I_n$, donde I_n denota la matriz identidad de orden n. Como ξI_n es central, se tiene que $\rho(u) = \xi I_n$ y $u_1 = \xi$, una raíz entera de la unidad. Por tanto, $\xi = \pm 1$ y $\rho(u) = \pm I_n = \rho(\pm 1)$. Como ρ es inyectiva en $\mathbb{C}G$, se deduce que $u = \pm 1$. ■

Como consecuencia del Teorema de Berman-Higman, podemos describir todas las unidades centrales de torsión de $\mathbb{Z}G$:

Corolario 3.1.2. *Las unidades centrales de torsión de $\mathbb{Z}G$ son las unidades triviales $\pm g$, con $g \in Z(G)$. En particular, si G es abeliano, toda unidad de torsión es trivial y, por tanto, todo subgrupo finito de $\mathcal{U}(\mathbb{Z}G)$ está contenido en $\pm G$.*

Demostración. Sea $u = \sum_{g \in G} u_g g$ una unidad central de torsión de $\mathbb{Z}G$, y sea g un elemento de $\mathrm{Supp}(u) = \{g \in G : u_g \neq 0\}$. Entonces $v = ug^{-1}$ es una unidad de torsión de $\mathbb{Z}G$, con $1 \in \mathrm{Supp}(v)$. Por el Teorema de Berman-Higman (Teorema 3.1.1) se tiene que $v = \pm 1$ y, por tanto, $u = \pm g$. ■

No obstante, si G no es abeliano, es posible construir unidades de torsión de $\mathbb{Z}G$ que no sean triviales. Por ejemplo, se pueden obtener unidades de este tipo conjugando unidades triviales por otras unidades no triviales (ver el capítulo 4, en particular las Conjeturas de Zassenhaus).

Ahora veremos que nos podemos restringir a estudiar únicamente las unidades de $\mathbb{Z}G$ que tienen aumento 1. Como el homomorfismo de aumento $\varepsilon_G : \mathbb{Z}G \to \mathbb{Z}$ es un homomorfismo de anillos, la imagen de una unidad de $\mathbb{Z}G$ por ε_G es una unidad de $\mathbb{Z}$. Por tanto, si $u \in \mathcal{U}(\mathbb{Z}G)$, entonces $\varepsilon_G(u) \in \{-1, 1\}$. Por consiguiente, $\mathcal{U}(\mathbb{Z}G) = \pm V(\mathbb{Z}G)$, donde

$$V(\mathbb{Z}G) = \{u \in \mathbb{Z}G : \varepsilon_G(u) = 1\}.$$

Entonces, para conocer $\mathcal{U}(\mathbb{Z}G)$ es suficiente con conocer $V(\mathbb{Z}G)$.

Para terminar la sección, veremos el concepto de aumento parcial, que

se puede definir para un anillo de grupo cualquiera RG, siendo R un anillo arbitrario. Si $g \in G$, denotaremos por g^G la clase de conjugación de g en G. Si $a = \sum_{h \in G} a_h h \in RG$, con $a_h \in R$, y $g \in G$, entonces el **aumento parcial** de a en g (o con respecto a la clase de conjugación de g) es

$$\varepsilon_g^G(a) = \sum_{h \in g^G} a_h.$$

Si el grupo G está claro por el contexto, lo denotaremos simplemente por $\varepsilon_g(a)$.

En el caso de que R sea $\mathbb{Z}$, puesto que la clase de conjugación del 1 en G está formada únicamente por el 1, el Teorema de Berman-Higman (Teorema 3.1.1) establece que si a es un elemento de torsión de $V(\mathbb{Z}G)$ de orden diferente de 1, entonces $\varepsilon_1(a) = 0$.

3.2. Problema del Espectro

El **espectro** de un grupo G es el conjunto de los órdenes de los elementos de torsión de G. Dado un grupo finito G, el **Problema del Espectro**, que será el protagonista de esta sección, es el siguiente:

¿Tienen G y $V(\mathbb{Z}G)$ el mismo espectro?

Hechos como que el mínimo común múltiplo de los órdenes de los elementos de torsión de $V(\mathbb{Z}G)$ sea el exponente de G ([CL65] y [Seh93, Teorema 7.3 (Zassenhaus)]) o que el Problema del Espectro tenga solución positiva para grupos metabelianos, es decir, para grupos cuyo subgrupo conmutador es abeliano ([Seh93, Lema 37.4]), dan soporte a este problema. No se conoce a día de hoy nigún grupo para el que el Problema del Espectro tenga respuesta negativa; se trata de un problema abierto.

Si tenemos en cuenta que G es un subgrupo de $V(\mathbb{Z}G)$, el Problema del Espectro es claramente equivalente al Problema de Investigación número 8 expuesto en [Seh93, secc. 49], que dice así:

Si u es una unidad de torsión de $V(\mathbb{Z}G)$,
¿existe un elemento g de G tal que $o(g) = o(u)$?

Además, el Problema 8 añade que, posiblemente, se cumpla $\varepsilon_g(u) \neq 0$. Martin Hertweck demostró en [Her08b] que este problema tiene solución positiva en el caso de que el grupo G sea resoluble, y que se verifica también la condición mencionada del aumento parcial no nulo. Al resultado principal de este artículo lo llamaremos a partir de ahora Teorema de Hertweck:

Teorema 3.2.1 (Teorema de Hertweck). *Sea G un grupo finito resoluble. Entonces cualquier unidad de torsión de $V(\mathbb{Z}G)$ tiene un aumento parcial no nulo con respecto a la clase de conjugación de un elemento del grupo del mismo orden. En particular, los órdenes de las unidades de torsión de $V(\mathbb{Z}G)$ son los órdenes de los elementos de G.*

No obstante, se necesitan bastantes resultados previos para poder demostrar este teorema, por lo que la siguiente sección la dedicaremos a ver estos resultados. Por último, adelantamos que en el capítulo 4 veremos la relación del Problema del Espectro con otros problemas planteados en el campo de los anillos de grupo enteros y, en particular, con las Conjeturas de Zassenhaus.

3.3. Resultados previos al Teorema de Hertweck

En esta sección se recogen definiciones y resultados necesarios para comprender la demostración del Teorema de Hertweck (Teorema 3.2.1). Entre ellos destaca un resultado de Weiss relativo a retículos de permutación, al que llamaremos Teorema de Weiss, y otros procedentes de trabajos previos de Hertweck.

3.3.1. Grupos resolubles

Para comenzar, recordaremos la definición de grupo resoluble.

Una **serie normal de longitud** s de un grupo G es una cadena de subgrupos

$$G = G_1 \geq G_2 \geq \cdots \geq G_s \geq G_{s+1} = 1$$

tal que $G_{i+1} \trianglelefteq G_i$ para todo $1 \leq i \leq s$. Los **cocientes** de la serie normal son

los grupos cociente $\{G_i/G_{i+1} : 1 \leq i \leq s\}$. Se dice que un grupo es **resoluble** si tiene una serie normal tal que todos los cocientes son abelianos.

Sabemos que el subgrupo derivado G', también llamado subgrupo conmutador, de un grupo G es el subgrupo generado por todos los conmutadores $\{(a,b) = aba^{-1}b^{-1} : a, b \in G\}$. Por tanto, G' es el subgrupo normal más pequeño de G tal que el grupo cociente es abeliano. La **serie derivada** de G es la serie

$$G \geq G^{(1)} \geq G^{(2)} \geq \cdots,$$

donde para cada $i \geq 1$, $G^{(i)}$ es el i-ésimo subgrupo derivado de G, es decir, $G^{(1)} = G'$ y $G^{(i)} = \left(G^{(i-1)}\right)'$ para cada $i \geq 2$.

Manteniendo la notación anterior, tenemos la siguiente caracterización de grupo resoluble: un grupo G es resoluble si, y solo si, $G^{(n)} = 1$ para algún n. (Se puede consultar una prueba en [CR62, Teorema 5.10].) El número natural n más pequeño para el cual $G^{(n)}$ es el grupo trivial se llama **longitud derivada de** G.

3.3.2. Acción doble

Este apartado está dedicado a la acción doble.

Sean R un anillo conmutativo, G y H dos grupos finitos y $\Gamma = H \times G$. Si M es un $R\Gamma$-módulo por la izquierda, entonces tiene también estructura de (RH, RG)-bimódulo con las multiplicaciones

$$h \cdot m = (h,1)m \quad \text{y} \quad m \cdot g = (1, g^{-1})m.$$

Además, se verifica que $r \cdot m = r(1,1)m = m \cdot r$ para todo $r \in R$ y $m \in M$.

Recíprocamente, si M es un (RH, RG)-bimódulo tal que $r \cdot m = m \cdot r$ para todo $r \in R$ y $m \in M$, entonces M es un $R\Gamma$-módulo por la izquierda con la multiplicación

$$(h,g)m = hmg^{-1}.$$

En particular, si $\alpha : H \to \mathcal{U}(RG)$ es una representación matricial de H sobre RG de grado 1, entonces $M = RG$ es un (RH, RG)-bimódulo, donde RG_{RG} es el RG-módulo regular por la derecha, y la multiplicación por la

izquierda viene dada por

$$h \cdot m = \alpha(h)m.$$

Denotaremos por M_α el correspondiente $R\Gamma$-módulo, que es libre de rango finito como R-módulo, por lo que podemos considerar el carácter permitido por él, χ_α. Probaremos a continuación que este carácter viene dado por

$$\chi_\alpha(h,g) = |C_G(g)|\, \varepsilon_g(\alpha(h)), \quad h \in H,\ g \in G. \tag{3.1}$$

donde $C_G(g)$ es el centralizador de g en G.

Sabemos que G es una base de RG como R-módulo. Dado un elemento h de H, sea $\alpha(h) = \sum_{y \in G} a_y y$, con $a_y \in R$ para todo $y \in G$. Se tiene que

$$(h,g)x = \alpha(h)xg^{-1} = \sum_{y \in G} a_y\, yxg^{-1} = \sum_{z \in G} a_{zgx^{-1}} z.$$

Por tanto,

$$\chi_\alpha(h,g) = \sum_{x \in G} a_{xgx^{-1}} = |C_G(g)|\, \varepsilon_g(\alpha(h)),$$

puesto que $|g^G| = |G : C_G(g)|$.

3.3.3. Retículos de permutación y Teorema de Weiss

Para comprender la prueba de la Proposición 3.4.1, una de las proposiciones previas al Teorema de Hertweck, necesitamos introducir los retículos de permutación y un resultado de Weiss relativo a ellos. Esto es lo que haremos en este apartado.

Un **retículo de permutación** para un grupo finito G sobre un anillo p-ádico R es una suma directa de RG-módulos de la forma $\mathrm{ind}_H^G(1)$. Por $1 = 1_H$ se entiende el RH-módulo R con acción trivial de H, es decir, el RH-módulo R con multiplicación dada por $hr = r$, para todo $h \in H$ y $r \in R$. También se puede escribir 1_H^G en lugar de $\mathrm{ind}_H^G(1)$.

El resultado de Weiss que necesitaremos es el siguiente:

Teorema 3.3.1 (Teorema de Weiss). *Sean G un p-grupo finito, R un anillo p-ádico, y M un RG-módulo que es libre de rango finito como R-módulo. Supongamos que N es un subgrupo normal de G tal que*

(i) La restricción M_N de M a N es un RN-módulo libre.

(ii) El $R(G/N)$-módulo $\frac{M}{\mathrm{Aug}(RN)M}$, donde $\mathrm{Aug}(RN)$ es el ideal de aumento de RN, es un retículo de permutación para G/N sobre R.

Entonces M es un retículo de permutación para G sobre R.

Demostración. Ver [Wei88]. (En realidad, Weiss probó este resultado únicamente para el caso $R = \mathbb{Z}_p$; en [Seh93, apéndice] podemos encontrar la demostración para cualquier anillo p-ádico.) ■

3.3.4. Resultados de Hertweck

Para concluir la sección de resultados previos al Teorema de Hertweck, en este apartado se exponen los resultados que el autor utiliza de algunos de sus trabajos anteriores. A lo largo de este apartado, G denotará un grupo finito y p un entero primo. Empezaremos definiendo el concepto de semilocalización.

Sea R un dominio de Dedekind, y sea $\mathcal{G}$ un conjunto de ideales primos de R. Se denota por $R_{\mathcal{G}}$ el anillo de los elementos α/β, $\alpha, \beta \in R$, en el cuerpo de cocientes de R, tales que para cualquier $\mathfrak{p} \in \mathcal{G}$ se tiene que $\beta \notin \mathfrak{p}$. $R_{\mathcal{G}}$ se conoce como la **semilocalización de R en $\mathcal{G}$**. Este concepto extiende el de localización $R_{\mathfrak{p}}$ de R en un ideal primo $\mathfrak{p}$, pues $R_{\mathcal{G}}$ coincide con $R_{\mathfrak{p}}$ cuando $\mathcal{G}$ consta del único elemento $\mathfrak{p}$.

Ejemplo 3.3.2. Dado un grupo finito G, sea $\pi(G)$ el conjunto de los divisores primos de $|G|$. Entonces, para todo elemento p de $\pi(G)$, se tiene que $p\mathbb{Z}$ es un ideal primo de $\mathbb{Z}$. Por consiguiente, se puede construir la semilocalización de $\mathbb{Z}$ en el conjunto de ideales primos $\{p\mathbb{Z} : p \in \pi(G)\}$, que será denotada por $\mathbb{Z}_{(G)}$.

Enunciaremos a continuación algunos resultados necesarios para la demostración del Lema 3.3.7, que se abordará posteriormente. R denotará un anillo conmutativo.

Supongamos que A es una R-álgebra artiniana por la izquierda, es decir, una R-álgebra que es un anillo artiniano por la izquierda. Los sumandos directos indescomponibles del módulo regular por la izquierda ${}_AA$ se llaman A-módulos por la izquierda **indescomponibles principales**.

Lema 3.3.3. *Sea A un álgebra artiniana por la izquierda. Un sumando directo P de ${}_AA$ es indescomponible si, y solo si, $P/P\operatorname{rad}A$ es un $A/\operatorname{rad}A$-módulo simple.*

Demostración. Ver [Pie82, secc. 6.3, Lema]. ■

Proposición 3.3.4. *Sea A un álgebra artiniana por la izquierda. La aplicación $P \mapsto P/P\operatorname{rad}A$ define una correspondencia biyectiva entre las clases de isomorfía de los A-módulos por la izquierda indescomponibles principales y las clases de isomorfía de los $A/\operatorname{rad}A$-módulos por la izquierda simples.*

Demostración. Ver [Pie82, secc. 6.3, Proposición]. ■

Teorema 3.3.5. *Si A es un álgebra artiniana por la izquierda, entonces todo A-módulo por la izquierda proyectivo es isomorfo a una suma directa de A-módulos por la izquierda indescomponibles principales. Esta descomposición es única salvo isomorfismo y orden de aparición de los sumandos.*

Demostración. Ver [Pie82, secc. 6.3, Teorema de Estructura]. ■

El siguiente corolario es inmediato:

Corolario 3.3.6. *Si A es un álgebra artiniana por la izquierda, entonces todo A-módulo por la izquierda proyectivo indescomponible es isomorfo a un A-módulo por la izquierda indescomponible principal.*

Comenzamos a presentar los resultados de trabajos de Hertweck. El primero de ellos no es un resultado suyo, aunque incluimos, detallando los aspectos que se consideran oportunos, la demostración que proporciona el autor en [Her06, Lema 3.2]. Antes de ver dicho resultado, observemos que para dar una representación de grado n de un grupo cíclico C de orden m sobre un cuerpo F, basta dar una matriz $A \in M_n(F)$ tal que $A^m = I_n$; más concretamente, A será la imagen de un generador del grupo. Usando Álgebra Lineal, y también el hecho de que dos FC-módulos son isomorfos si, y solo si, sus representaciones matriciales permitidas son equivalentes (Proposiciones 2.1.2 y 2.1.3), se observa que los FC-módulos indescomponibles están determinados

por las matrices elementales de Jordan

$$\begin{pmatrix} \lambda & & & & \\ 1 & \lambda & & & \\ & \ddots & \ddots & & \\ & & 1 & \lambda & \\ & & & 1 & \lambda \end{pmatrix}$$

con $\lambda^m = 1$.

Lema 3.3.7. *Supongamos que C es un p-grupo cíclico no trivial, y sea P el subgrupo de C de orden p. Además, sean F un cuerpo de característica p y M un FC-módulo finitamente generado como F-módulo. Entonces M es proyectivo como FC-módulo si, y solo si, es proyectivo como FP-módulo.*

Demostración. Sabemos que el conjunto de representantes de las clases laterales por la izquierda de P en C constituye una base libre de FC sobre FP (ver 2.5), por lo que FC es libre como FP-módulo. De esto se deduce fácilmente que si ${}_{FC}M$ es proyectivo, también lo es ${}_{FP}M$.

Para probar el recíproco, por el Teorema de K-S-A (1.4.2) podemos suponer que ${}_{FC}M$ es indescomponible; también podemos suponer que $|C| = p^a$, con $a > 1$. Esto significa que si g es un generador de C, entonces, en una base adecuada $\{v_1, v_2, \ldots, v_k\}$ de ${}_FM$, la representación matricial ρ de C permitida por ${}_{FC}M$ viene dada por una matriz elemental de Jordan

$$\rho(g) = J_k(\lambda) = \begin{pmatrix} \lambda & & & & \\ 1 & \lambda & & & \\ & \ddots & \ddots & & \\ & & 1 & \lambda & \\ & & & 1 & \lambda \end{pmatrix} \in \mathcal{M}_k(F),$$

con $1 \leq k \leq p^a$, siendo k la dimensión de ${}_{FC}M$ como espacio vectorial sobre F. Además, se verifica que $\lambda^{p^a} = 1$, de donde se deduce que $\lambda = 1$, debido a que el cuerpo F tiene característica p. Por tanto, $\rho(g) = J_k(1)$.

Veremos a continuación que ${}_{FC}M$ es proyectivo si, y solo si, $k = p^a$. Basta probar que el único FC-módulo proyectivo indescomponible es el propio anillo de grupo ${}_{FC}FC$, cuya dimensión como espacio vectorial sobre F es $|C| = p^a$, y es lo que haremos a continuación.

Claramente, FC es un FC-módulo proyectivo, pues es libre. Veamos que FC es, además, un FC-módulo indescomponible. En una base adecuada de un módulo ${}_FN$, la representación matricial de C permitida por ${}_FN$ viene dada por una matriz de Jordan, es decir, una matriz formada por yuxtaposición de matrices elementales de Jordan (o bloques de Jordan) a lo largo de la diagonal, de la forma

$$\begin{pmatrix} J_{k_1}(\lambda_1) & & & \mathbf{0} \\ & J_{k_2(}\lambda_2) & & \\ & & \ddots & \\ \mathbf{0} & & & J_{k_r}(\lambda_r) \end{pmatrix}.$$

Además, sabemos que el número de bloques de Jordan correspondientes a cada autovalor coincide con el número máximo de autovectores linealmente independientes que tiene la matriz asociados a dicho autovalor. Para ver que FC es un FC-módulo indescomponible, hemos de probar que, para dicho módulo, esta matriz tiene únicamente un bloque de Jordan. En nuestro caso, como hemos comentado, se tiene que $\lambda_1 = \lambda_2 = \cdots = \lambda_r = 1$. Por tanto, para ver que FC es un FC-módulo indescomponible basta ver que cualesquiera dos autovectores asociados al autovalor 1 son linealmente dependientes. Ahora bien, si w es un autovector de la matriz asociado al autovalor 1, se verifica que $gw = w$. Entonces, si llamamos b al elemento de FC asociado a w, este se puede escribir de la forma $b = \sum_{s=0}^{p^a-1} b_{g^s} g^s$, donde $b_{g^s} \in FC$ para cada s, y se verifica que

$$b_0 + b_1 g + b_2 g^2 + \cdots + b_{g^{p^a-1}} g^{p^a-1} = b = gb = b_{g^{p^a-1}} + b_0 g + b_1 g^2 + \cdots + b_{g^{p^a-2}} g^{p^a-1}.$$

De aquí se deduce que b tiene todos los coeficientes iguales y, por tanto, w tiene todas las componentes iguales, luego queda probado que FC es un FC-módulo indescomponible.

Falta probar que no hay más FC-módulos proyectivos indescomponibles aparte del propio FC. Veamos esto. Como FC es un álgebra artiniana, de la Proposición 3.3.4 y el Corolario 3.3.6 se deduce que existe una correspondencia biyectiva entre las clases de isomorfía de los FC-módulos por la izquierda proyectivos indescomponibles y las clases de isomorfía de los $FC/\operatorname{rad} FC$-módulos por la izquierda simples. Ahora, por el Teorema 1.6.3 sabemos que existe un único FC-módulo por la izquierda simple (salvo isomorfismo), concretamente el cuerpo F, sobre el que los elementos de C actúan

trivialmente. Por el mismo teorema, se tiene que $\operatorname{rad} FC$ coincide con el ideal de aumento de FC. Además, como el homomorfismo de aumento es suprayectivo, se cumple que $FC/\operatorname{rad} FC \cong F$. Por consiguiente, del Teorema 1.3.9 se deduce que existe una correspondencia biyectiva entre las clases de isomorfía de los sumandos directos indescomponibles de ${}_{FC}FC$ y las clases de isomorfía de los sumandos directos indescomponibles de ${}_{F}F$. Por tanto, existe un único FC-módulo por la izquierda proyectivo indescomponible, que ya hemos visto que es el propio FC.

Supongamos ahora que ${}_{FP}M$ es proyectivo. Queremos probar que ${}_{FC}M$ es proyectivo. Hemos denotado anteriormente por k la dimensión de M como espacio vectorial sobre F. Por lo que hemos visto, hemos de demostrar que $k = p^a$, y esto es lo que haremos. Sea $q = |C|/p = p^{a-1}$. Entonces $P = \langle g^q \rangle$, y $\rho(g^q) = J_k(1)^q$. Se prueba fácilmente por inducción sobre n que para cada $1 \leq i \leq k$ y cada $1 \leq n \leq |C|$,

$$g^n v_i = \sum_{m=0}^{k-i} \binom{n}{m} v_{i+m}.$$

En particular, para $n = q$, al ser F un cuerpo de característica p y ser q una potencia de p, se tiene que

$$g^q v_i = \begin{cases} v_i + v_{i+q} & \text{si } i+q \leq k, \\ v_i & \text{en otro caso.} \end{cases}$$

Ahora, como ${}_{FP}M$ es proyectivo, la acción de P sobre M no puede ser trivial, luego $J_k(1)^q$ no es la matriz identidad. Por consiguiente, $k > q$. Como consecuencia, existen dos enteros no negativos s y t, con $t < q$, tales que $k - q + 1 = sq + t$. Sean $I = \{t + iq : i = 0, 1, \ldots, s\}$ y $J = \{1, 2, \ldots, k\} \setminus I$, y sean $M_I = \sum_{i \in I} Fv_i$ y $M_J = \sum_{j \in J} Fv_j$. Claramente,

$$M = M_I \oplus M_J,$$

y la expresión de $g^q v_i$ dada anteriormente implica que M_I y M_J son submódulos de FP. Como ${}_{FP}M$ es proyectivo, también lo son M_I y M_J. Por tanto, la dimensión de cada uno de ellos es un múltiplo de la dimensión del único módulo indescomponible proyectivo ${}_{FP}M$. Por lo que hemos visto, esta dimensión es p, luego $p \mid s+1$ y $p \mid k$. Ahora, como $t = k - (s+1)q + 1$, se tiene que $t \equiv 1 \pmod{p}$, por lo que $t \geq 1$. Por consiguiente, se llega a que

$$p^a = pq \leq (s+1)q = k + 1 - t \leq k,$$

luego $k = p^a$, como queríamos probar. ∎

Se dice que dos grupos U y H son **racionalmente conjugados** si son conjugados en $\mathbb{Q}G$, es decir, si existe $\alpha \in \mathcal{U}(\mathbb{Q}G)$ tal que $U = \alpha^{-1}H\alpha$.

Proposición 3.3.8. *Sea N un p-subgrupo normal de G. Supongamos que U es un subgrupo finito de $V\left(\mathbb{Z}_{(G)}G\right)$ cuya imagen es 1 por la aplicación natural $\mathbb{Z}_{(G)}G \to \mathbb{Z}_{(G)}G/N$. Entonces U es racionalmente conjugado de un subgrupo de N.*

Demostración. Ver [Her06, Proposición 4.2]. ∎

El siguiente resultado de Hertweck, [Her07, Teorema 2.3], está precedido de un lema necesario para su demostración:

Lema 3.3.9. *Sea R un dominio de Dedekind de característica 0, y sea M un RG-módulo por la izquierda. Se verifican las siguientes afirmaciones:*

(i) Si H es un subgrupo de G, entonces ${}_{RG}M$ es proyectivo si, y solo si, ${}_{RH}M$ es proyectivo y $R/P \otimes_R M$ es proyectivo como $(R/P)G$-módulo para todo ideal maximal P de R que contiene a $|G : H|$.

(ii) Si ${}_{RG}M$ es proyectivo, χ es el carácter permitido por M y g es un elemento de G tal que $o(g)$ no es invertible en R, entonces $\chi(g) = 0$.

Demostración. (i) Ver [BG00, Teorema 9.1].

(ii) Ver [CR81, Teorema 32.15]. ∎

Teorema 3.3.10. *Sea u una unidad de torsión de $V(\mathbb{Z}G)$ y sea g un elemento de G. Si el orden de g no divide al orden de u, entonces $\varepsilon_g(u) = 0$.*

Demostración. Supongamos que $o(g)$ no divide a $o(u)$. Entonces existe un entero primo p tal que una potencia de p divide a $o(g)$, pero no divide a $o(u)$. Sea

$$R = \mathbb{Z}_{(p)} = \{x/y : x, y \in \mathbb{Z}, p \nmid y\},$$

la localización de $\mathbb{Z}$ en $p\mathbb{Z}$, y sea $F = R/pR \cong \mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$, el cuerpo de p elementos. Consideramos la inclusión $\alpha : \langle u \rangle \to V(\mathbb{Z}G) \subseteq V(RG)$, y definimos $M = M_\alpha = RG$ visto como $R\Gamma$-módulo, con $\Gamma = \langle u \rangle \times G$ (ver sección 3.3.2).

Sea ahora $C = \langle (u, g) \rangle$. Como C es un grupo abeliano finito, se puede escribir de la forma $C = P \times H$ para dos subgrupos P y H de C, siendo P el

p-subgrupo de Sylow de C. Además, llamaremos Q al subgrupo de P de orden p. Por las hipótesis sobre los órdenes de u y g, se cumple que $Q = \langle (1,k) \rangle$, con $\langle k \rangle$ el subgrupo de orden p de $\langle g \rangle$. Entonces se tiene que

$$ {}_{FQ}(F \otimes_R M) \cong {}_{F\langle k \rangle}(F \otimes_R RG) \cong {}_{F\langle k \rangle}FG \cong F\langle k \rangle^{|G:\langle k \rangle|}, $$

puesto que un conjunto de representantes de clases laterales por la izquierda de $\langle k \rangle$ en G constituye una base libre de FG como $F\langle k \rangle$-módulo (ver (2.5)). Por consiguiente, ${}_{FQ}(F \otimes_R M)$ es libre y, como consecuencia, proyectivo. Entonces, por el Lema 3.3.7 se cumple que ${}_{FP}(F \otimes_R M)$ es también proyectivo. Además, se tiene que

$$ {}_{RQ}M \cong {}_{R\langle k \rangle}RG \cong R\langle k \rangle^{|G:\langle k \rangle|}, $$

luego ${}_{RQ}M$ es libre y, por tanto, proyectivo. Como $R = \mathbb{Z}_{(p)}$ es un AVD, se tiene que R es un dominio de Dedekind, y pR es su único ideal maximal. Además, R tiene característica 0, y del Lema 3.3.9 (i) se deduce que ${}_{RP}M$ es proyectivo.

Ahora, como p no divide a $|C:P|$, se tiene que $|C:P|$ es invertible en R, y ${}_{RC}M$ es (C,P)-proyectivo por la Proposición 2.3.5 (iv). Por consiguiente, ${}_{RC}M$ es proyectivo, puesto que ${}_{RP}M$ es proyectivo. Además, el orden de (u,g) es divisible por p, luego $o(u,g)$ no es invertible en R. Por tanto, si denotamos por χ el carácter permitido por ${}_{RC}M$, se verifica que $\chi(u,g) = 0$ por el Lema 3.3.9 (ii). Finalmente, basta aplicar (3.1) para concluir que

$$ \varepsilon_g(u) = \frac{\chi(u,g)}{|C_G(g)|} = 0. $$

■

Finalmente, el resultado que se enuncia a continuación, aunque se ha tomado de [Seh93, Lema 38.11], es realmente una consecuencia del teorema anterior.

Corolario 3.3.11. *Sea u una unidad de torsión de $V(\mathbb{Z}G)$ y sea g un elemento de G. Si existe un primo p tal que $p \mid o(g)$ pero $p \nmid o(u)$, entonces $\varepsilon_g(u) = 0$.*

Demostración. Se deduce de las hipótesis que $o(g) \nmid o(u)$. Por tanto, basta aplicar el Teorema 3.3.10 para concluir que $\varepsilon_g(u) = 0$. ■

3.4. Teorema de Hertweck

Estamos ya en condiciones de probar el Teorema de Hertweck. Lo haremos siguiendo el artículo [Her08b], en el que dos proposiciones preceden al teorema. La primera de ellas sirve para probar la segunda, y la segunda se utiliza para demostrar el Teorema de Hertweck. Observemos la aplicación del Teorema de Weiss en la demostración de la primera proposición (Proposición 3.4.1), y la aplicación del Teorema de Green de los Ceros de Caracteres en la prueba de la segunda (Proposición 3.4.2). En ambas proposiciones, G denotará un grupo finito arbitrario, mientras que en el teorema se exigirá, además, que sea resoluble. A lo largo de la sección, p denotará un entero primo.

Proposición 3.4.1. *Supongamos que G tiene un p-subgrupo normal N y que U es un subgrupo finito de $V(\mathbb{Z}G)$ cuya imagen es 1 por la aplicación natural $\mathbb{Z}G \to \mathbb{Z}G/N$. Entonces U es un p-grupo, y $\mathbb{Z}_pG$, cuando se considera como $\mathbb{Z}_pU$-retículo vía la acción de la multiplicación (por la derecha) de U, es proyectivo.*

Demostración. Comenzaremos viendo que U es un p-grupo. Lo haremos a partir de una propiedad más general.

Sea u una unidad de torsión de $V(\mathbb{Z}G)$. Sea $\overline{G} = G/N$, y sea $\bar{u}$ la imagen de u por la aplicación natural $V(\mathbb{Z}G) \to V(\mathbb{Z}\overline{G})$, que es un homomorfismo de grupos.

Sabemos que el orden de la p'-parte de u es mayor o igual que el orden de la p'-parte de $\bar{u}$; de hecho, el orden de la p'-parte de u es un múltiplo del orden de la p'-parte de $\bar{u}$. Veamos que en realidad ambos coinciden. Sea v la p'-parte de u, y supongamos que $\bar{v}^k = 1_{G/N} = N$, con $k \geq 0$. Basta probar que $v^k = 1$. Como $\overline{v^k} = \bar{v}^k$, si $v^k = \sum_{g\in G} a_g g$, se tiene que $N = \overline{v^k} = \sum_{g\in G} a_g \bar{g} = \sum_{\bar{g}\in\bar{G}} \left(\sum_{x\in\bar{g}} a_x\right) \bar{g}$ y, por consiguiente,

$$1 = \sum_{x\in N} a_x = \sum_{x^G:\, x\in N} \varepsilon_x(v^k).$$

Como consecuencia, existe un elemento x de N (y, por tanto, de G) tal que $o(x)$ es una potencia de p (por ser N un p-grupo) y $\varepsilon_x(v^k) \neq 0$. Si se tuviera que $v^k \neq 1$, entonces, por el Teorema de Berman-Higman (Teorema 3.1.1), $\varepsilon_1(v^k) = 0$. Por consiguiente, $x \neq 1$, luego $p \mid o(x)$. Como $p \nmid o(v^k)$, por ser

v^k la p'-parte de u^k, aplicando el Corolario 3.3.11 se concluye que $\varepsilon_x(v^k) = 0$, lo que supone una contradicción. Por tanto, se ha de cumplir que $v^k = 1$, y queda probado que el orden de la p'-parte de u coincide con el orden de la p'-parte de $\bar{u}$.

Tomamos ahora un elemento u de U, que es un subgrupo finito de $V(\mathbb{Z}G)$. Por hipótesis, se tiene que $\bar{u} = 1$. Por tanto, se deduce de lo anterior que la p'-parte de u es 1 y, como consecuencia, U es un p-grupo.

Ahora bien, el Teorema de Weiss (Teorema 3.3.1) garantiza que $\mathbb{Z}_pG$ es un retículo de permutación para U sobre $\mathbb{Z}_p$. (Se ha de tomar, con la notación del teorema, $R = \mathbb{Z}_p$ y $M = \mathbb{Z}_pG$, y se ha de considerar el grupo U y el subgrupo normal trivial.)

Por la Proposición 3.3.8 aplicada al anillo $\mathbb{Z}$, que es un subanillo de $\mathbb{Z}_{(G)}$, tenemos que U es racionalmente conjugado de un subgrupo de N, al que llamaremos V. Por tanto, $U = \alpha^{-1}V\alpha$ para algún $\alpha \in \mathcal{U}(\mathbb{Q}G)$ y, como consecuencia, podemos definir un isomorfismo $V \to U$, dado por $v \mapsto \alpha^{-1}v\alpha$. También podemos definir $M = \mathbb{Z}_pG$ visto como $\mathbb{Z}_pU$-módulo, y $L = \mathbb{Z}_pG$ visto como $\mathbb{Z}_pV$-módulo.

Tenemos como objetivo probar que M es proyectivo. Denotaremos por ρ_M y ρ_L las representaciones asociadas a M y L, respectivamente, y por χ_M y χ_L los caracteres permitidos por los correspondientes módulos. En realidad, $\chi_M : \mathbb{Q}_pU \to \mathbb{Q}_p$ denotará el carácter de U permitido por M extendido por linealidad sobre $\mathbb{Q}_pU$, y $\chi_L : \mathbb{Q}_pV \to \mathbb{Q}_p$ el carácter de V permitido por L extendido por linealidad sobre $\mathbb{Q}_pV$, donde $\mathbb{Q}_p$ es el cuerpo de los números p-ádicos. Consideramos ahora un elemento u de U. Por lo anterior, existe un elemento v de V tal que $u = \alpha^{-1}v\alpha$, y se verifica que

$$\chi_M(u) = \mathrm{tr}(\rho_M(u)) = \mathrm{tr}(\rho_M(\alpha^{-1}v\alpha)) = \mathrm{tr}(\rho_L(v)) = \chi_L(v)$$

debido a las propiedades de la traza. Además, χ_L toma el valor 0 sobre elementos no triviales, ya que L es el $\mathbb{Z}_pV$-módulo restringido de la representación regular de G sobre $\mathbb{Z}_p$ (ver Ejemplos 2.1.6 (ii)). Como $u = 1$ si, y solo si, $v = 1$, también χ_M toma el valor 0 sobre elementos no triviales.

Ahora usamos el hecho de que M es un retículo de permutación, por lo

que lo podemos escribir como

$$M = \bigoplus_{i=1}^{m} \mathrm{ind}_{U_i}^{U}(1)$$

para algunos subgrupos U_i de U. Sabemos, por la Proposición 2.1.7, que el carácter de U permitido por M, al que llamaremos a partir de ahora simplemente χ, viene dado por $\sum_{i=1}^{m} \chi_i^U$, donde χ_i es el carácter de U_i permitido por 1 para cada i, y χ_i^U denota el carácter inducido. Como $1 = 1_{U_i}$ es el $\mathbb{Z}_pU_i$-módulo $\mathbb{Z}_p$ con acción trivial de U_i, por el apartado (i) de Ejemplos 2.1.6 se tiene que para cada i, $\chi_i(x) > 0$ para todo $x \in U_i$.

Sea ahora $1 \leq i \leq m$, y sea $\{g_j : 1 \leq j \leq n\}$ un conjunto de representantes de las clases laterales por la izquierda de U_i en U, con $g_1 = 1$. Sabemos por (2.10) que el carácter inducido viene dado por

$$\chi_i^U(x) = \sum_{j=1}^{n} \dot{\chi}_i(g_j^{-1} x g_j), \quad x \in U,$$

donde

$$\dot{\chi}_i(y) = \begin{cases} \chi_i(y) > 0 & \text{si } y \in U_i, \\ 0 & \text{si } y \notin U_i. \end{cases}$$

Ahora, si existiera algún i tal que U_i no fuera el subgrupo trivial, entonces existiría algún elemento x de U_i tal que $x \neq 1$, y se cumpliría que $\chi(x) = 0$. Por lo anterior, se tendría que $\chi_i^U(x) = 0$, y se llegaría a que $\dot{\chi}_i(g_j^{-1} x g_j) = 0$ para todo j. En particular, se tendría que

$$\dot{\chi}_i(x) = \dot{\chi}_i(g_1^{-1} x g_1) = 0.$$

Sin embargo, puesto que $x \in U_i$, también se cumpliría que

$$\dot{\chi}_i(x) = \chi_i(x) > 0,$$

lo que supondría una contradicción. Así, se concluye que $U_i = 1$ para todo i.

La expresión de M es, por tanto,

$$M = \bigoplus_{i=1}^{m} \mathrm{ind}_{1}^{U}(1).$$

Ahora bien,

$$\mathrm{ind}_{1}^{U}(1) \cong \mathbb{Z}_pU \otimes_{\mathbb{Z}_p} \mathbb{Z}_p \cong \mathbb{Z}_pU,$$

luego

$$M \cong (\mathbb{Z}_p U)^m,$$

por lo que M es un $\mathbb{Z}_p U$-módulo libre y, por consiguiente, proyectivo. ■

Proposición 3.4.2. *Supongamos que G tiene un p-subgrupo normal N y que u es una unidad de torsión de $V(\mathbb{Z}G)$ cuya imagen por la aplicación natural $\mathbb{Z}G \to \mathbb{Z}G/N$ tiene orden estrictamente menor que u. Si g es un elemento de G tal que $\varepsilon_g(u) \neq 0$, entonces las p-partes de g y de u tienen el mismo orden.*

Demostración. En primer lugar, veremos que $\langle u \rangle$ tiene un subgrupo de orden p cuya imagen es 1 por la aplicación natural $\mathbb{Z}G \to \mathbb{Z}G/N$.

Utilizando la misma notación que en la Proposición 3.4.1, y de acuerdo con lo que vimos en su demostración, el orden de la p'-parte de $\bar{u}$ es el mismo que el de la p'-parte de u. De esto se deduce que el orden de la p-parte de $\bar{u}$ es estrictamente menor que el de la p-parte de u. Por tanto, el orden de la p-parte de u es mayor que 1, luego $p \mid o(u)$. Por consiguiente, $\langle u \rangle$ tiene un (único) subgrupo de orden p, que está generado por $u^{o(u)/p}$. Ahora, como el orden de la p-parte de $\bar{u}$ es menor que el de la p-parte de u, se tiene que $\bar{u}^{o(u)/p} = 1$, lo que implica que $\overline{u^{o(u)/p}} = 1$. Como consecuencia, la imagen de $\langle u^{o(u)/p} \rangle$ por la aplicación natural $\mathbb{Z}G \to \mathbb{Z}G/N$ es 1.

Por reducción al absurdo, supongamos que g es un elemento de G tal que $\varepsilon_g(u) \neq 0$, y que las p-partes de g y de u tienen distinto orden. Por el Teorema 3.3.10, se tiene que $o(g) \mid o(u)$, luego el orden de la p-parte de g divide al orden de la p-parte de u. Por tanto, la p-parte de g tiene orden estrictamente menor que la p-parte de u.

Sea C un grupo cíclico (abstracto) cuyo orden es el orden de u. Sea $M = \mathbb{Z}_p G$ visto como $\mathbb{Z}_p C$-retículo, haciendo actuar a un generador c de C de la forma

$$m \cdot c = g^{-1} m u, \quad m \in M.$$

Llegaremos a una contradicción demostrando que $\varepsilon_g(u) = 0$. Por (3.1), para ver esto basta probar que $\chi(c) = 0$, siendo χ el carácter de C permitido por M.

Observemos que c es p-singular, ya que $p \mid o(u)$, que coincide con $|C| = o(c)$. Lo que haremos será probar que M es un $\mathbb{Z}_p C$-retículo proyectivo, pues entonces podremos aplicar el Teorema de Green de los Ceros de Caracteres

(Teorema 2.5.2) para deducir que $\chi(c) = 0$. En efecto, si suponemos probado que M es un $\mathbb{Z}_pC$-retículo proyectivo, se cumplen las hipótesis que aparecen en este teorema:

- $\mathbb{Z}_p$ es un AVD completo con cuerpo de clases de residuos $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$, que es un cuerpo perfecto por ser finito (ver Proposición 1.1.2), y tiene característica p.
- M es un $\mathbb{Z}_pC$-retículo (C, H)-proyectivo para cualquier subgrupo H de C y, en particular, es (C, D)-proyectivo para el p-subgrupo D de C cuyo orden es el orden de la p-parte de g.
- La p-parte de c no es conjugada de ningún elemento de D; en caso contrario, se tendría que el orden de la p-parte de u, que coincide con el orden de la p-parte de c, dividiría al orden de D, es decir, al orden de la p-parte de g, por lo que se llegaría a una contradicción.

Para probar que M es un $\mathbb{Z}_pC$-retículo proyectivo, veremos primero que es un $\mathbb{Z}_pP$-retículo proyectivo, donde P es el subgrupo de orden p de C. Hemos visto que el orden de la p-parte de g es estrictamente menor que el de la p-parte de u. Por tanto, se verifica que

$$m \cdot c^{o(c)/p} = g^{-o(c)/p} m u^{o(c)/p} = m u^{o(c)/p} = m u^{o(u)/p}.$$

Como consecuencia, la acción del subgrupo P viene dada por la acción de la multiplicación (por la derecha) del subgrupo de orden p de $\langle u \rangle$, y se deduce de la Proposición 3.4.1 que M es un $\mathbb{Z}_pP$-retículo proyectivo.

Sea ahora Q el p-subgrupo de Sylow de C. Veremos a continuación que M es también un $\mathbb{Z}_pQ$-retículo proyectivo. Aplicaremos el Teorema 1.3.16, tomando $R = \mathbb{Z}_p$, $\mathfrak{p} = p\mathbb{Z}_p$ y $\Lambda = \mathbb{Z}_pP$. (Observemos que Λ es un R-orden, pues lo es todo anillo de grupo de un grupo finito con coeficientes en un dominio de Dedekind.) Con la notación de este resultado, se tiene que $\overline{R} = \mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$ y $\overline{\Lambda} \cong \overline{R}P$. Por dicho teorema, como M es un $\mathbb{Z}_pP$-módulo proyectivo, tenemos que $\overline{M}$ es un $\overline{R}P$-módulo proyectivo. Ahora, del Lema 3.3.7 se deduce que $\overline{M}$ es un $\overline{R}Q$-módulo proyectivo. Observemos que se cumplen las hipótesis de este lema, pues P es el subgrupo de orden p de Q, que es un grupo cíclico (por ser un subgrupo del grupo cíclico C), y $\overline{R} \cong \mathbb{F}_p$ es un cuerpo de característica p.

Podemos aplicar de nuevo el Teorema 1.3.16 para obtener que M es un

$\mathbb{Z}_pQ$-retículo proyectivo, tomando en este caso $\Lambda = \mathbb{Z}_pQ$. Ahora bien, al ser Q el p-subgrupo de Sylow de C, el índice $|C : Q|$ es coprimo con p, luego $|C : Q|$ es una unidad en $\mathbb{Z}_p$. Entonces, por la Proposición 2.3.5 (iv) se llega a que M es (C, Q)-proyectivo. Por tanto, M es un $\mathbb{Z}_pC$-módulo proyectivo, puesto que M es proyectivo como $\mathbb{Z}_pQ$-módulo, y queda probado el resultado. ■

Hagamos primero una observación antes de proceder a la prueba del Teorema de Hertweck:

Observación 3.4.3. Sea N un subgrupo normal de G y sea $\overline{G} = G/N$. Al igual que en las proposiciones anteriores, dada una unidad de torsión u, denotaremos por $\bar{u}$ la imagen de u por la aplicación natural $\mathbb{Z}G \to \mathbb{Z}\overline{G}$. Además, representaremos por $\sim$ la relación de conjugación en un grupo. Como cualquier clase de conjugación de G se aplica sobre una clase de conjugación de $\overline{G}$, se tiene que, para cualquier elemento x de G,

$$\varepsilon_{\bar{x}}(\bar{u}) = \sum_{g^G:\, \bar{g}\sim\bar{x}} \varepsilon_g(u). \tag{3.2}$$

En efecto, si tomamos $u = \sum_{g\in G} u_g g$, entonces $\bar{u} = \sum_{g\in G} u_g \bar{g} = \sum_{\bar{g}\in\overline{G}} \left(\sum_{h\in\bar{g}} u_h\right) \bar{g}$, y se tiene que

$$\varepsilon_{\bar{x}}(\bar{u}) = \sum_{\bar{g}\sim\bar{x}} \left(\sum_{h\in\bar{g}} u_h\right) = \sum_{g^G:\, \bar{g}\sim\bar{x}} \left(\sum_{h\in g^G} u_h\right) = \sum_{g^G:\, \bar{g}\sim\bar{x}} \varepsilon_g(u).$$

Teorema 3.4.4 (Teorema de Hertweck). *Sea G un grupo finito resoluble. Entonces cualquier unidad de torsión de $V(\mathbb{Z}G)$ tiene un aumento parcial no nulo con respecto a la clase de conjugación de un elemento del grupo del mismo orden. En particular, los órdenes de las unidades de torsión de $V(\mathbb{Z}G)$ son los órdenes de los elementos de G.*

Demostración. Sea G un grupo finito resoluble y sea u una unidad de torsión de $V(\mathbb{Z}G)$. La prueba es por inducción sobre el orden de G. El resultado es evidente cuando G es el grupo trivial. Supongamos entonces que G no es trivial. En este caso, como G es resoluble, tenemos que

$$G \geq G^{(1)} \geq G^{(2)} \geq \cdots \geq G^{(n-1)} \geq G^{(n)} = 1,$$

donde para cada $i = 1, 2, \ldots, n$, $G^{(i)}$ es el i-ésimo subgrupo derivado de G. Sabemos que todos los subgrupos de la serie derivada son normales en G,

y que $G^{(n-1)}$ es abeliano (finito). Por tanto, $G^{(n-1)}$ es isomorfo al producto directo de sus p_j-subgrupos de Sylow, siendo $|G| = {p_1}^{k_1} \cdots {p_l}^{k_l}$ la descomposición de $|G|$ en factores primos, y podemos elegir uno de estos p_j-subgrupos de Sylow. Si llamamos p a p_j, el subgrupo elegido será un p-subgrupo normal no trivial N de G.

Sea ahora $\overline{G} = G/N$, y sea $\bar{u}$ la imagen de u por la aplicación natural $V(\mathbb{Z}G) \to V(\mathbb{Z}\overline{G})$, que es un homomorfismo de grupos. Supongamos que el resultado del teorema es cierto para cualquier grupo finito resoluble de orden estrictamente menor que el orden de G. En particular, se cumple para el grupo $\overline{G}$, que es un grupo resoluble por serlo G. Por tanto, existe un elemento x de G tal que $o(\bar{x}) = o(\bar{u})$ y $\varepsilon_{\bar{x}}(\bar{u}) \neq 0$. Sea g un elemento de G tal que $\bar{g} \sim \bar{x}$. Tendremos en cuenta que si $o(g) > o(u)$, entonces $\varepsilon_g(u) = 0$ por el Teorema 3.3.10.

Como $o(\bar{u}) \leq o(u)$ (de hecho, se tiene que $o(\bar{u}) \mid o(u)$), se pueden dar dos casos:

- Caso (i). $o(\bar{u}) = o(u)$.

  En este caso se tiene que

  $$o(g) \geq o(\bar{g}) = o(\bar{x}) = o(\bar{u}) = o(u).$$

  Por tanto, la suma que aparece en (3.2) se extiende solamente sobre las clases de conjugación g^G para las que $o(g) = o(u)$, y como $\varepsilon_{\bar{x}}(\bar{u}) \neq 0$, al menos un sumando $\varepsilon_g(u)$ ha de ser también distinto de cero, tal como queríamos demostrar.

- Caso (ii). $o(\bar{u}) < o(u)$.

  De acuerdo con lo que vimos en la prueba de la Proposición 3.4.1, el orden de la p'-parte de u coincide con el orden de la p'-parte de $\bar{u}$. El mismo argumento nos serviría para demostrar que el orden de la p'-parte de un elemento g de G (y, por tanto, de $V(\mathbb{Z}G)$) coincide con el orden de la p'-parte de $\bar{g}$. Sin embargo, este caso es más sencillo, pues si denotamos por v la p'-parte de g y suponemos que $\bar{v}^k = 1_{G/N} = N$, entonces $v^k \in N$, luego o bien $v^k = 1$ o bien $p \mid o(v^k)$, al ser N un p-grupo, por lo que $p \mid o(v)$, en contra de que v es la p'-parte de g.

  Como $o(\bar{g}) = o(\bar{x}) = o(\bar{u})$, las p'-partes de $\bar{g}$ y $\bar{u}$ tienen el mismo orden.

Por lo anterior, también coincide el orden de las p'-partes de g y u. Ahora bien, si $o(g) < o(u)$, entonces el orden de la p-parte de g es estrictamente menor que el orden de la p-parte de u, luego $\varepsilon_g(u) = 0$ por la Proposición 3.4.2. Por tanto, la suma que aparece en (3.2) se extiende de nuevo solamente sobre las clases de conjugación g^G para las que $o(g) = o(u)$, y se llega al resultado deseado. ■

Observación 3.4.5. El autor señala en su artículo que el Teorema de Hertweck se puede formular para anillos de coeficientes más generales que $\mathbb{Z}$, como $\mathbb{Z}_{(G)}$.

Para la redacción de la sección 3.1 nos hemos basado en [Rio16, seccs. 1, 2, 5] y [Seh93, secc. 1], mientras que la sección 3.2 ha sido elaborada a partir de [Rio16, secc. 4], [Her08b, secc. 1] y [Seh93, secc. 49].

En el caso de la sección 3.3, se han empleado [CR81, secc. 1] y [CR62, secc. 5] para redactar el apartado 3.3.1, [Rio16, secc. 6] para el apartado 3.3.2, [Seh93, secc. 38, apéndice] y [CR81, secc. 8B] para el apartado 3.3.3 y, finalmente, [Her06, seccs. 1, 3, 4], [Her07, secc. 2], [Koc97, secc. 3.3], [Alp86, secc. 4], [Rio16, secc. 6] y [Pie82, secc. 6.3] para el apartado 3.3.4.

Por último, la sección 3.4 está basada en [Her08b].

Capítulo 4

Otros problemas en el campo de los anillos de grupo y su relación con el Problema del Espectro

Como ya hemos comentado en varias ocasiones, el objetivo principal de este trabajo era utilizar la Teoría de Representaciones para resolver el Problema del Espectro en el caso particular de que el grupo considerado sea resoluble. Si bien podemos decir que esto ya lo hemos logrado en el capítulo anterior, dedicaremos este último capítulo a mencionar otros problemas relativos a los anillos de grupo enteros y a estudiar las conexiones entre ellos, así como su relación con el Problema del Espectro.

Consideraremos a lo largo del capítulo que G es un grupo finito. Los problemas que vamos a tratar surgen al preguntarse hasta qué punto el anillo de grupo $\mathbb{Z}G$ refleja las propiedades del grupo G sobre el que se construye. Entre ellos destaca el llamado **Problema del Isomorfismo** para anillos de grupo enteros, que plantea si el anillo de grupo determina el grupo salvo isomorfismos. Dicho problema se enuncia de la siguiente manera, donde H denota cualquier grupo finito:

(Iso) ¿El isomorfismo de $\mathbb{Z}$-álgebras $\mathbb{Z}G \cong \mathbb{Z}H$ implica que $G \cong H$?

Este problema fue planteado por primera vez por Graham Higman en su tesis doctoral ([Hig40a]). Además, Higman demostró en [Hig40a, Hig40b]

que si G es abeliano, entonces las únicas unidades de torsión de $\mathbb{Z}G$ son las triviales, es decir, los elementos de G y sus opuestos. (Esto se recoge en este trabajo en el Corolario 3.1.2, consecuencia del Teorema de Berman-Higman (Teorema 3.1.1).) Por tanto, si G es abeliano y existe un isomorfismo de $\mathbb{Z}$-álgebras $\mathbb{Z}G \cong \mathbb{Z}H$, entonces la restricción de este isomorfismo a G proporciona un isomorfismo $G \cong H$. Por consiguiente, (Iso) tiene solución positiva para grupos abelianos.

En general, es conocido que el Problema del Isomorfismo tiene solución positiva para grupos metabelianos, y también para p-grupos y grupos nilpotentes. (La definición de grupo nilpotente la podemos encontrar, por ejemplo, en [CR81, secc. 1B].) El primero de los casos fue probado por Whitcomb ([Whi68]), y el segundo, por Roggenkamp y Scott ([RS87]); el resultado para grupos nilpotentes se deduce del resultado para p-grupos y de [Seh93, Teorema 36.12]. Sin embargo, (Iso) no tiene solución positiva en todos los casos, como demostró Hertweck en [Her01]; para ello consideró grupos resolubles de longitud derivada 4.

Relacionadas con el Problema del Isomorfismo se encuentran las llamadas **Conjeturas de Zassenhaus**, tres fuertes conjeturas que Hans J. Zassenhaus planteó a mediados de los años setenta ([Zas74, Seh93]). Estas tres conjeturas, que se suelen llamar Primera, Segunda y Tercera Conjetura de Zassenhaus, y que abreviaremos como (ZC1), (ZC2) y (ZC3), son las siguientes:

(ZC1) Todo elemento de torsión u de $V(\mathbb{Z}G)$ es conjugado en $\mathbb{Q}G$ de un elemento de G (es decir, $\alpha^{-1}u\alpha \in G$ para algún $\alpha \in \mathcal{U}(\mathbb{Q}G)$).

(ZC2) Todo subgrupo finito H de $V(\mathbb{Z}G)$ con la misma cardinalidad que G es conjugado en $\mathbb{Q}G$ de G (es decir, $\alpha^{-1}H\alpha = G$ para algún elemento $\alpha \in \mathcal{U}(\mathbb{Q}G)$).

(ZC3) Todo subgrupo finito H de $V(\mathbb{Z}G)$ es conjugado en $\mathbb{Q}G$ de un subgrupo de G (es decir, $\alpha^{-1}H\alpha \subseteq G$ para algún $\alpha \in \mathcal{U}(\mathbb{Q}G)$).

Veremos en primer lugar que la última conjetura es más fuerte que las otras dos. Claramente, (ZC3) implica (ZC2), ya que un grupo conjugado tiene la misma cardinalidad que el original, pues si H es el subgrupo de $V(\mathbb{Z}G)$ conjugado de G por el elemento α de $\mathcal{U}(\mathbb{Q}G)$, entonces la aplicación $\theta : G \to H$ definida por $\theta(g) = \alpha^{-1}g\alpha$ es un isomorfismo de grupos. Además, (ZC3) también implica (ZC1), ya que para cada elemento de torsión de

$V(\mathbb{Z}G)$ se puede construir el grupo cíclico generado por dicho elemento, que es un subgrupo finito de $V(\mathbb{Z}G)$.

En las tres Conjeturas de Zassenhaus se habla de elementos o subgrupos conjugados en el anillo de grupo $\mathbb{Q}G$. Sin embargo, de acuerdo con la siguiente proposición, en dichas conjeturas se puede reemplazar el cuerpo de los números racionales por cualquier otro cuerpo de característica 0:

Proposición 4.1. *Sea F/K una extensión de cuerpos infinitos, y sea G un grupo finito. Supongamos que H_1 y H_2 son dos subgrupos finitos de unidades de KG. Si H_1 y H_2 son conjugados en FG, entonces son conjugados en KG.*

Demostración. Ver [Seh93, Lema 37.5]. ∎

Para comprobar la afirmación que precede a la proposición anterior, basta tomar $K = \mathbb{Q}$ y F cualquier cuerpo de característica 0, el cual contendrá un subcuerpo isomorfo a $\mathbb{Q}$.

Observemos ahora que si (ZC3) fuera cierta, entonces el orden de todo subgrupo finito de $V(\mathbb{Z}G)$ dividiría a $|G|$, pues dos subgrupos conjugados tienen el mismo orden. Ahora bien, esto último se cumple independientemente de si (ZC3) se verifica o no. Esta propiedad viene enunciada a continuación en forma de proposición, y para su demostración se necesita el siguiente lema previo:

Lema 4.2. *Todo subgrupo finito de $V(\mathbb{Z}G)$ es linealmente independiente sobre $\mathbb{Q}$ (equivalentemente, sobre $\mathbb{Z}$).*

Demostración. Sea $H = \{u_1, \ldots, u_n\}$ un subgrupo finito de $V(\mathbb{Z}G)$, y supongamos que $c_1u_1 + c_2u_2 + \cdots + c_nu_n = 0$, con $c_i \in \mathbb{Z}$ para todo $i = 1, \ldots, n$. Entonces $c_1 + c_2u_2u_1^{-1} + \cdots + c_nu_nu_1^{-1} = 0$, y para todo $i = 2, \ldots, n$, se tiene que $u_iu_1^{-1}$ es un elemento de torsión no trivial de $V(\mathbb{Z}G)$. Del Teorema de Berman-Higman (Teorema 3.1.1) se deduce que para todo $i \neq 1$, $1 \notin \mathrm{Supp}(u_iu_1^{-1})$ y, por tanto, $c_1 = 0$. Repitiendo el argumento, se llega a que $c_i = 0$ para todo $i = 1, \ldots, n$. ∎

Proposición 4.3. *El orden de todo subgrupo finito de $V(\mathbb{Z}G)$ divide a $|G|$.*

Demostración. Ver [Seh93, Lema 37.3]. ∎

Además, como consecuencia del Lema 4.2 se tiene que un subgrupo H

de $V(\mathbb{Z}G)$ de orden $|G|$ es una base de $\mathbb{Q}G$ sobre $\mathbb{Q}$ o, equivalentemente, se cumple que $\mathbb{Q}G = \mathbb{Q}H$. Más aún, por la siguiente proposición, es también una base de $\mathbb{Z}G$ sobre $\mathbb{Z}$:

Proposición 4.4. *Si H es un subgrupo de $V(\mathbb{Z}G)$ con $|H| = |G|$, entonces $\mathbb{Z}G = \mathbb{Z}H$.*

Demostración. Claramente, $\mathbb{Z}H \subseteq \mathbb{Z}G$. Además, acabamos de observar que $\mathbb{Q}G = \mathbb{Q}H$, así que si tomamos un elemento g de G, entonces $g \in \mathbb{Q}H$, por lo que existe un entero positivo n tal que $ng = \sum_{h\in H} m_h h$ para algunos $m_h \in \mathbb{Z}$. Por tanto, para cada $h \in H$, se tiene que $ngh^{-1} = m_h + \sum_{k\in H\setminus\{h\}} m_k kh^{-1}$. Por el Teorema de Berman-Higman (Teorema 3.1.1), el coeficiente del 1 en gh^{-1} es 1 ó 0, luego el coeficiente del 1 en ngh^{-1}, el lado izquierdo de la igualdad anterior, es n ó 0. Además, el coeficiente del 1 en el lado derecho de dicha igualdad es m_h. Por consiguiente, m_h es n ó 0 y, en cualquier caso, es un múltiplo de n, luego $g = \sum_{h\in H} \frac{m_h}{n} h \in \mathbb{Z}H$. Queda probado que $G \subseteq \mathbb{Z}H$, lo que implica que $\mathbb{Z}G \subseteq \mathbb{Z}H$. ∎

Este último resultado nos sirve para demostrar que (ZC2) se puede reformular de la siguiente manera equivalente, tal como aparece en [Seh93, secc. 37]:

(ZC2)′ Si $\mathbb{Z}G = \mathbb{Z}H$ y $\varepsilon_G(H) = 1$, entonces $\alpha^{-1}H\alpha = G$ para algún elemento $\alpha \in \mathcal{U}(\mathbb{Q}G)$,

donde $\varepsilon_G : \mathbb{Z}G \to \mathbb{Z}$ es el homomorfismo de aumento.

Para demostrar la equivalencia entre (ZC2) y (ZC2)′, basta probar que H es un subgrupo finito de $V(\mathbb{Z}G)$ con la misma cardinalidad que G si, y solo si, $\mathbb{Z}G = \mathbb{Z}H$ y $\varepsilon_G(H) = 1$, y esto es cierto:

$\boxed{\Rightarrow}$ Como H es un subgrupo finito de $V(\mathbb{Z}G)$, se tiene que $\varepsilon_G(H) = 1$. Además, como $|H| = |G|$, se cumple que $\mathbb{Z}G = \mathbb{Z}H$ por la Proposición 4.4.

$\boxed{\Leftarrow}$ Como H es base de $\mathbb{Z}H = \mathbb{Z}G$ sobre $\mathbb{Z}$, al igual que G, se tiene que $|H| = |G| < \infty$. Además, como $\varepsilon_G(H) = 1$, se tiene que H es un subgrupo de $V(\mathbb{Z}H) = V(\mathbb{Z}G)$.

Vamos a establecer a continuación una relación entre las Conjeturas de Zassenhaus y el Problema del Isomorfismo. En concreto, probaremos que

(ZC2) implica una solución positiva de (Iso). Supongamos que G y H son dos grupos finitos y que existe un isomorfismo de $\mathbb{Z}$-álgebras $\theta : \mathbb{Z}G \to \mathbb{Z}H$. Entonces la aplicación $\theta^* : \mathbb{Z}G \to \mathbb{Z}H$ definida por

$$\theta^*\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g(\varepsilon_H(\theta(g)))^{-1}\theta(g),$$

donde $\varepsilon_H : \mathbb{Z}H \to \mathbb{Z}$ es el homomorfismo de aumento, es también un isomorfismo. Además, se verifica que para todo $g \in G$,

$$\theta^*(g) = (\varepsilon_H(\theta(g)))^{-1}\theta(g) \in V(\mathbb{Z}H),$$

ya que

$$\varepsilon_H(\theta^*(g)) = (\varepsilon_H(\theta(g)))^{-1}\varepsilon_H(\theta(g)) = 1.$$

Por tanto, $\theta^*(G)$ es un subgrupo de $V(\mathbb{Z}H)$. También se cumple que $\theta^*(G)$ tiene la misma cardinalidad que H, puesto que G es una base de $\mathbb{Z}G$ sobre $\mathbb{Z}$ y, por consiguiente, $\theta^*(G)$ lo es de $\mathbb{Z}H$ sobre $\mathbb{Z}$, al igual que lo es H. Así, si (ZC2) fuera cierta, $\theta^*(G)$ sería conjugado de H en $\mathbb{Q}H$ y, por tanto, se cumpliría que $G \cong \theta^*(G) \cong H$.

Roggenkamp y Scott proporcionaron el primer contraejemplo para (ZC2) en [Rog91, Sco92], el cual constituye también un contraejemplo para (ZC3). Además, por lo que acabamos de ver, también el caso descrito por Hertweck en [Her01] en el que (Iso) tenía una respuesta negativa constituye un contraejemplo tanto para (ZC2) como para (ZC3). En cuanto a la Primera Conjetura de Zassenhaus, esta se ha conseguido probar en ciertos casos particulares, al igual que el Problema del Isomorfismo. Por ejemplo, Weiss ([Wei91]) la demostró para grupos nilpotentes, y se ha probado también para ciertas clases de grupos metabelianos ([CMR13, Her08a, MRSW87]).

Ha sido muy recientemente cuando se han presentado los primeros contraejemplos de (ZC1), obtenidos por Florian Eisele y Leo Margolis, que podemos encontrar en [EM17] (pendiente de publicación). En este artículo se demuestra que son contraejemplos los candidatos propuestos por Leo Margolis y Ángel del Río en [MR17a]. El contraejemplo más pequeño que se ofrece en el artículo [EM17] es el caso de un grupo metabeliano de orden $2^7 \cdot 3^2 \cdot 5 \cdot 7^2 \cdot 19^2$. A pesar de existir estos contraejemplos, se pueden continuar estudiando las clases de grupos para los que (ZC1) y las demás Conjeturas de Zassenhaus

son ciertas, así como las clases de grupos para los que los problemas expuestos tienen una solución positiva, aunque puedan no tenerla en general para cualquier grupo finito G.

Otro problema que nos podemos plantear es cómo describir los automorfismos de $\mathbb{Z}G$. Esta cuestión se conoce como el **Problema del Automorfismo** (ver [Seh93, secc. 37]):

(Aut) Si $\theta \in \mathrm{Aut}(\mathbb{Z}G)$, entonces ¿existen $\beta \in \mathrm{Aut}(G)$ y $\alpha \in \mathcal{U}(\mathbb{Q}G)$ tales que $\theta(g) = \alpha^{-1}\beta(g)\alpha$ para todo $g \in G$?

Un homomorfismo $\theta : \mathbb{Z}G \to \mathbb{Z}H$ se llama **normalizado** o se dice que preserva el aumento si se verifica que $\varepsilon(\theta(g)) = 1$ para todo $g \in G$. En el Problema del Automorfismo se considerarán únicamente automorfismos normalizados, puesto que para cualquier automorfismo de $\mathbb{Z}G$ se puede encontrar otro normalizado a partir de él, como hemos visto en la prueba de que (ZC2) implica una solución positiva de (Iso).

Veremos a continuación que (ZC2) también implica una solución positiva de (Aut). Supongamos que (ZC2) es cierta, y sea $\theta \in \mathrm{Aut}(\mathbb{Z}G)$ (normalizado). Por el mismo argumento de la demostración de que (ZC2) implica una solución positiva de (Iso), llegamos a que $\theta(G)$ es conjugado de G en $\mathbb{Q}G$, es decir, existe un elemento α de $\mathcal{U}(\mathbb{Q}G)$ tal que $\theta(G) = \alpha^{-1}G\alpha$. Por tanto, para cada elemento g de G existe un elemento g_1 de G tal que $\theta(g) = \alpha^{-1}g_1\alpha$. Claramente, $g \mapsto g_1$ es un automorfismo de G, con lo que la prueba queda concluida.

En realidad, Roggenkamp y Scott ([Rog91, Sco92]) encontraron un caso en el que el Problema del Automorfismo tenía respuesta negativa, y es de aquí de donde se obtuvo el primer contraejemplo para (ZC2).

También se cumple que soluciones positivas de (Aut) + (Iso) implican (ZC2) o, equivalentemente, (ZC2)′. Vamos a demostrar esto último. Supongamos que se tienen soluciones positivas de ambos problemas, (Aut) e (Iso), para un grupo finito G, y que se verifica $\mathbb{Z}G = \mathbb{Z}H$. Como (Iso) tiene una solución positiva, existe un isomorfismo $\theta : G \to H$, que se puede extender a un isomorfismo $\theta : \mathbb{Z}G \to \mathbb{Z}H$. Como (Aut) tiene también una solución positiva, existen $\alpha \in \mathcal{U}(\mathbb{Q}G)$ y $\sigma \in \mathrm{Aut}(G)$ tales que $\theta(g) = \alpha^{-1}\sigma(g)\alpha$. Por consiguiente, $H = \theta(G) = \alpha^{-1}\sigma(G)\alpha = \alpha^{-1}G\alpha$, como queríamos probar.

Recordemos ahora el **Problema del Espectro**, que se ha tratado en la sección 3.2:

(PE) ¿Tienen G y $V(\mathbb{Z}G)$ el mismo espectro?

Claramente, existe una relación entre la Primera Conjetura de Zassenhaus y el Problema del Espectro: puesto que dos elementos conjugados tienen el mismo orden, si se cumple (ZC1) para un grupo finito G, el Problema del Espectro tendrá una solución positiva para dicho grupo. (PE) se ha resuelto para más clases de grupos que (ZC1). En el capítulo 3 y, en concreto, en la sección 3.4, hemos visto con detalle la demostración del Problema del Espectro en el caso particular de que el grupo considerado sea resoluble, que debemos a Hertweck ([Her08b]). Además, este problema también tiene una solución positiva para los grupos de Frobenius ([KK17, Corolario 2.5]). (Podemos encontrar una definición de este tipo de grupos en [CR81, secc. 14A]).

El último problema que mencionaremos será el Problema del Grafo Primo, propuesto por Kimmerle en [Kim06]. Dado un grupo finito G, se llama **grafo primo** de G al grafo no dirigido cuyos vértices son los enteros primos del espectro de G y cuyos ejes son los pares $\{p,q\}$ de primos p y q tales que $pq = o(g)$ para algún elemento g de G. El **Problema del Grafo Primo** es el siguiente:

(PGP) ¿Tienen G y $V(\mathbb{Z}G)$ el mismo grafo primo?

Es evidente que si el Problema del Espectro tiene una solución positiva para un grupo finito G, también la tendrá el Problema del Grafo Primo para dicho grupo, puesto que si los espectros de dos grupos finitos coinciden, también lo harán sus grafos primos. Además, fue el estudio de Höfert y Kimmerle ([Kim06, secc. 4]) sobre el grafo primo de $V(\mathbb{Z}G)$, con G un grupo finito resoluble, lo que despertó el interés de Hertweck en probar el Problema del Espectro para esta clase de grupos. Por último, se ha demostrado que el Problema del Grafo Primo tiene solución positiva para algunos grupos simples (ver, por ejemplo, [BKL11]), si bien continúa siendo un problema abierto, al igual que el Problema del Espectro. (Para obtener algunos detalles más sobre estos dos últimos problemas, se puede consultar [MR17b, secc. 1].)

El siguiente gráfico recoge las conjeturas y los problemas tratados en este último capítulo, así como las implicaciones entre ellos, en caso de que los

problemas fueran formulados en forma de conjetura:

$$\begin{array}{ccccc} & & \left\{\begin{array}{c}\text{(Iso)}\\ + \\ \text{(Aut)}\end{array}\right. & & \\ \text{(ZC2)} & \Leftrightarrow & & & \\ \Uparrow & & & & \\ \text{(ZC3)} & & & & \\ \Downarrow & & & & \\ \text{(ZC1)} & \Rightarrow & \text{(PE)} & \Rightarrow & \text{(PGP)} \end{array}$$

Para finalizar, cabe mencionar que en [Seh93, secc. 49] aparecen muchos otros problemas planteados en el campo de los anillos de grupo enteros.

Para la redacción de este capítulo se han utilizado fundamentalmente [Rio16, secc. 4] y [Seh93, seccs. 36–37], aunque también se ha empleado [MR17b, secc. 1].

Bibliografía

[Alp86] Alperin, J. L. (1986). *Local representation theory: Modular representations as an introduction to the local representation theory of finite groups*. (Cambridge Studies in Advanced Mathematics, Vol. 11). Cambridge: Cambridge University Press. (Citado en la página 102.)

[BG00] Benson, D. J. y Goodearl, K. R. (2000). Periodic flat modules, and flat modules for finite groups. *Pacific J. Math.*, *196*(1), 45–67. (Citado en la página 93.)

[BKL11] Bovdi, V. A., Konovalov, A. B. y Linton, S. (2011). Torsion units in integral group rings of Conway simple groups. *Internat. J. Algebra Comput.*, *21*(4), 615–634. (Citado en la página 109.)

[CMR13] Caicedo, M., Margolis, L. y Río, Á. del (2013). Zassenhaus Conjecture for cyclic-by-abelian groups. *J. Lond. Math. Soc. (2)*, *88*(1), 65–78. (Citado en las páginas 2 y 107.)

[CL65] Cohn, J. A. y Livingstone, D. (1965). On the structure of group algebras. I. *Can. J. Math.*, *17*, 583–593. (Citado en la página 84.)

[CR62] Curtis, C. W. y Reiner, I. (1962). *Representation theory of finite groups and associative algebras*. Nueva York: Interscience. (Citado en las páginas 14, 47, 57, 80, 86 y 102.)

[CR81] ——— (1981). *Methods of representation theory with applications to finite groups and orders. Vol. I*. Nueva York: John Wiley & Sons. (Citado en las páginas 13, 17, 18, 22, 28, 29, 30, 32, 33, 36, 46, 47, 69, 71, 73, 80, 93, 102, 104 y 109.)

[Dad71] Dade, E. C. (1971). Deux groupes finis distincts ayant la même algèbre de groupe sur tout corps. *Math. Z.*, *119*, 345–348. (Citado en la página 1.)

[EM17] Eisele, F. y Margolis, L. (2017). A counterexample to the first Zassenhaus Conjecture. Recuperado de https://arxiv.org/abs/1710.08780v2 (Citado en las páginas 2, 3 y 107.)

[FD93] Farb, B. y Dennis, R. K. (1993). *Noncommutative algebra.* (Graduate Texts in Mathematics, Vol. 144). Nueva York: Springer-Verlag. (Citado en las páginas 47 y 80.)

[Gou93] Gouvêa, F. Q. (1993). *p-adic numbers: An introduction.* Berlín-Heidelberg: Springer-Verlag. (Citado en las páginas 18, 25, 26 y 47.)

[Her01] Hertweck, M. (2001). A counterexample to the isomorphism problem for integral group rings. *Ann. of Math.*, *154*, 115–138. (Citado en las páginas 1, 104 y 107.)

[Her06] ——— (2006). On the torsion units of some integral group rings. *Algebra Colloq.*, *13*(2), 329–348. (Citado en las páginas 2, 89, 93 y 102.)

[Her07] ——— (2007). Partial augmentations and Brauer character values of torsion units in group rings. Recuperado de https://arxiv.org/abs/math/0612429v2 (Citado en las páginas 2, 93 y 102.)

[Her08a] ——— (2008). Torsion units in integral group rings of certain metabelian groups. *Proc. Edinb. Math. Soc. (2)*, *51*(2), 363–385. (Citado en las páginas 2 y 107.)

[Her08b] ——— (2008). The orders of torsion units in integral group rings of finite solvable groups. *Comm. Algebra*, *36*(10), 3585–3588. (Citado en las páginas 2, 81, 85, 95, 102 y 109.)

[Hig40a] Higman, G. (1940). *Units in group rings.* (Tesis doctoral). Universidad de Oxford. (Citado en las páginas 1 y 103.)

[Hig40b] ——— (1940). The units of group rings. *Proc. London Math. Soc.*, *46*, 231–248. (Citado en las páginas 1 y 103.)

[HP72] Hughes, I. y Pearson, K. R. (1972). The group of units of the integral group ring $\mathbb{Z}\mathcal{S}_3$. *Canad. Math. Bull.*, *15*, 529–534. (Citado en la página 2.)

[Jan73] Janusz, G. J. (1973). *Algebraic number fields.* (2.ª ed.). Londres: Academic Press. (Citado en las páginas 16, 17, 18, 19, 21, 24 y 47.)

[Kar92] Karpilovsky, G. (1992). *Group representations. Vol 1.* (North-Holland Mathematics Studies, Vol. 175). Amsterdam: Elsevier Science. (Citado en la página 80.)

[Kim06] Kimmerle, W. (2006). On the prime graph of the unit group of integral group rings of finite groups. En W. Chin, J. Osterburg y D. Quinn (Eds.), *Groups, rings and algebras* (pp. 215–228). (Contemporary Mathematics, Vol. 420). Providence, Rhode Island: American Mathematical Society. (Citado en la página 109.)

[KK17] Kimmerle, W. y Konovalov, A. B. (2017). On the Gruenberg-Kegel graph of integral group rings of finite groups. *Internat. J. Algebra Comput.*, *27*(6), 619–631. (Citado en la página 109.)

[Koc97] Koch, H. (1997). *Algebraic number theory.* Berlín-Heidelberg: Springer-Verlag. (Reimpresión del original de 1992). (Citado en la página 102.)

[LP89] Luthar, I. S. y Passi, I. B. S. (1989). Zassenhaus conjecture for $\mathcal{A}_5$. *Proc. Indian Acad. Sci. Math. Sci.*, *99*(1), 1–5. (Citado en la página 2.)

[MR17a] Margolis, L. y Río, Á. del (2017). An algorithm to construct candidates to counterexamples to the Zassenhaus Conjecture. Recuperado de `https://arxiv.org/abs/1710.05629v3` (Citado en la página 107.)

[MR17b] ——– (2017). Partial augmentations power property: a Zassenhaus Conjecture related problem. Recuperado de `https://arxiv.org/abs/1706.04787v2` (Citado en las páginas 109 y 110.)

[MRSW87] Marciniak, Z., Ritter, J., Sehgal, S. K. y Weiss, A. (1987). Torsion units in integral group rings of some metabelian groups II. *J. Number Theory*, *25*(3), 340–352. (Citado en la página 107.)

[Neu99] Neukirch, J. (1999). *Algebraic number theory.* (N. Schappacher, Trad.). Berlín-Heidelberg: Springer-Verlag. (Obra original publicada en 1992). (Citado en las páginas 18 y 47.)

[Pas89] Passman, D. S. (1989). *Infinite crossed products.* (Pure and Applied Mathematics, Vol. 135). San Diego: Academic Press. (Citado en la página 47.)

[Pie82] Pierce, R. S. (1982). *Associative algebras.* (Graduate Texts in Mathematics, Vol. 88). Nueva York: Springer-Verlag. (Citado en las páginas 89 y 102.)

[Rei03] Reiner, I. (2003). *Maximal orders.* (London Mathematical Society Monographs, New series, Vol. 28). Oxford: Clarendon Press. (Reimpresión corregida del original de 1975). (Citado en las páginas 10, 46 y 47.)

[Rio16] Río, Á. del (2016, junio). Finite subgroups of integral group rings. Minicurso dado en *Advances in Group Theory and Applications 2016.* Vietri Sul Mare, Salerno, Italia. (Citado en las páginas 47, 80, 102 y 110.)

[Rog91] Roggenkamp, K. W. (1991). Observations to a conjecture of H. Zassenhaus. En *Groups St. Andrews 1989. Vol. 2* (pp. 427–444). (London Mathematical Society Lecture Note Series, Vol.160). Cambridge: Cambridge University Press. (Citado en las páginas 107 y 108.)

[RS87] Roggenkamp, K. W. y Scott, L. L. (1987). Isomorphisms for p-adic group rings. *Ann. of Math.*, *126*, 593–647. (Citado en la página 104.)

[Seh93] Sehgal, S. K. (1993). *Units in integral group rings.* (Pitman Monographs and Surveys in Pure and Applied Mathematics, Vol. 69). Harlow: Longman Scientific & Techical. (Citado en las páginas 84, 88, 94, 102, 104, 105, 106, 108 y 110.)

[Ser79] Serre, J.-P. (1979). *Local fields.* (Graduate Texts in Mathematics, Vol. 67). Nueva York: Springer-Verlag. (Citado en las páginas 18, 31, 33 y 47.)

[Sco92] Scott, L. L. (1992). On a conjecture of Zassenhaus, and beyond. En L. A. Bokut, Yu L. Ershov y A. I. Kostrikin (Eds.), *Proceedings of the International Conference on Algebra. Part 1 (Novosibirsk, 1989)* (pp. 325–343). (Contemporary Mathematics, Vol. 131, Part 1). Providence, Rhode Island: American Mathematical Society. (Citado en las páginas 107 y 108.)

[Wei88] Weiss, A. (1988). Rigidity of p-adic torsion. *Ann. of Math.*, *127*, 317–332. (Citado en la página 88.)

[Wei91] ——– (1991). Torsion units in integral group rings. *J. Reine Angew. Math.*, *415*, 175–187. (Citado en las páginas 2 y 107.)

[Whi68] Whitcomb, A. (1968). *The group ring problem.* (Tesis doctoral). Universidad de Chicago. (Citado en la página 104.)

[Zas74] Zassenhaus, H. (1974). On the torsion units of finite group rings. En *Studies in Mathematics (in honour of A. Almeida Costa)* (pp. 119–126). Lisboa: Instituto de Alta Cultura. (Citado en las páginas 2 y 104.)

[ZS75] Zariski, O. y Samuel, P. (1975). *Commutative Algebra. Vol. I.* (Graduate Texts in Mathematics, Vol. 28). Nueva York: Springer-Verlag. (Citado en las páginas 7 y 47.)

Notación

$A \cong B$	isomorfismo (de grupos, anillos, módulos o álgebras)

Conjuntos numéricos

$\mathbb{Z}$	anillo de los números enteros
$\mathbb{Q}$	cuerpo de los números racionales
$\mathbb{R}$	cuerpo de los números reales
$\mathbb{C}$	cuerpo de los números complejos
$\mathbb{R}_+$	conjunto de los números reales no negativos
$\mathbb{Z}_p$	anillo de los enteros p-ádicos
$\mathbb{Q}_p$	cuerpo de los números p-ádicos

Teoría de Números

$a \mid b$	a divide a b
$a \nmid b$	a no divide a b
$a \equiv b \pmod{p}$	congruencia módulo p

Teoría de Conjuntos y símbolos lógicos

$\lvert A \rvert$	cardinalidad de A
$A \subseteq B$	inclusión de conjuntos
$A \setminus B$	complementario de B en A
$\dot{\cup}$	unión disjunta
$\Rightarrow$	implica
$\Leftrightarrow$	si, y solo si

Abreviaturas

AVD	anillo de valoración discreta
deg	grado
DFU	dominio de factorización única

DIP	dominio de ideales principales
K-S-A	Krull-Schmidt-Azumaya
rad	radical
tr	traza
(Aut)	Problema del Automorfismo
(Iso)	Problema del Isomorfismo
(PE)	Problema del Espectro
(PGP)	Problema del Grafo Primo
(ZC1), (ZC2), (ZC3)	Conjeturas de Zassenhaus

Álgebra Lineal

$\mathcal{M}_n(R)$	anillo de las matrices cuadradas de orden n sobre R
$GL_n(R)$	grupo de las matrices de orden n invertibles sobre R
I_n	matriz identidad de orden n
$\mathrm{diag}(a_1, \ldots, a_n)$	matriz diagonal con entradas $a_1, \ldots, a_n$ en la diagonal
$J_k(a)$	matriz elemental de Jordan de orden k y autovalor a
$\mathrm{tr}(x, M)$	traza de x actuando sobre M

Teoría de Grupos

$H \leq G$	inclusión de subgrupos
$H \trianglelefteq G$	H es un subgrupo normal de G
$\lvert G : H \rvert$	índice de H en G
1_G	elemento neutro de un grupo G
$\langle x \rangle$	grupo cíclico generado por x
$G_1 \times G_2$	producto directo de grupos
G/H	clases laterales por la izquierda de H en G
$H \setminus G \,/\, K$	clases laterales dobles HgK en G
$o(g)$	orden de un elemento g de G
$Z(G)$	centro de un grupo G
$C_G(g)$	centralizador de g en G
G'	subgrupo derivado o conmutador de G
$G^{(i)}$	i-ésimo subgrupo derivado de G
${}^a h = aha^{-1} = h^{a^{-1}}$	conjugados de un elemento h de un subgrupo H
${}^a H = aHa^{-1} = H^{a^{-1}}$	conjugados de un subgrupo H
$g \sim h$	relación de conjugación en un grupo
g^G	clase de conjugación de un elemento g de G
$\mathrm{End}(G)$	anillo de endomorfismos de G

$\mathrm{Aut}(G)$	grupo de automorfismos de G

Anillos y módulos

1_A	elemento neutro para la multiplicación de un anillo A
1_M	aplicación identidad sobre un módulo M
$\prod_{i\in I} M_i$	producto directo de módulos
$\bigoplus_{i\in I} M_i$	suma directa de módulos
$M \mid N$	M es isomorfo a un sumando directo de N
A^n	suma directa de n copias de un anillo A o A-módulo de las matrices de tamaño $n \times 1$ sobre A
${}_AA$	A-módulo regular por la izquierda
${}_AM$	M visto como A-módulo
$Z(A)$	centro de un anillo A
$\mathcal{U}(A)$	grupo de unidades de un anillo A
$\mathrm{Hom}_A(M,N)$	grupo de homomorfismos de A-módulos de M en N
$\mathrm{End}_A(M)$	anillo o álgebra de endomorfismos de un A-módulo M
$\mathrm{Aut}_A(M)$	grupo de automorfismos de un A-módulo M
A^{op}	anillo o álgebra opuesta de A
$L \otimes_A M$	producto tensorial de módulos
$R[X_1,\ldots,X_n]$	anillo de polinomios en $X_1,\ldots,X_n$ con coeficientes en R
$\mathrm{ann}\, M$	anulador de un módulo M
$\mathfrak{B} \mid \mathfrak{p}$	$\mathfrak{B}$ divide a $\mathfrak{p}$ ($\mathfrak{B}$ y $\mathfrak{p}$ ideales de dominios de Dedekind)
$e_{\mathfrak{B}}$	índice de ramificación de un ideal primo $\mathfrak{B}$
$f_{\mathfrak{B}}$	grado de residuos de un ideal primo $\mathfrak{B}$
${}^aL$	módulo conjugado
R_P	localización de un anillo R en un ideal primo P
$\mathbb{Z}_{(p)}$	localización de $\mathbb{Z}$ en un ideal primo $p\mathbb{Z}$
$R_{\mathcal{G}}$	semilocalización de R en un conjunto $\mathcal{G}$ de ideales primos
$\pi(G)$	conjunto de los divisores primos de $\lvert G\rvert$
$\mathbb{Z}_{(G)}$	semilocalización de $\mathbb{Z}$ en $\{p\mathbb{Z} : p \in \pi(G)\}$
φ_P	valoración P-ádica
v_P	valoración exponencial P-ádica
$\lvert\ \rvert_p$	valoración p-ádica
v_p	valoración exponencial p-ádica
$\overline{R}$	cuerpo de clases de residuos de un AVD R
RG	anillo de grupo de un grupo G sobre un anillo R
$\mathrm{Supp}(a)$	soporte de un elemento a de RG

ε_G	homomorfismo de aumento
$\mathrm{Aug}(RG)$	ideal de aumento de RG
$\varepsilon_{G,N}$	homomorfismo $RG \to R(G/N)$ que extiende la aplicación natural $G \to G/N$
$\mathrm{Aug}_N(RG)$	núcleo del homomorfismo $\varepsilon_{G,N}$
$V(\mathbb{Z}G)$	subgrupo de unidades de aumento 1 de $\mathbb{Z}G$
$\varepsilon_g(a)$	aumento parcial de a en g, con $a \in RG$ y $g \in G$
$\pm G$	conjunto de las unidades triviales de $\mathbb{Z}G$
$1 = 1_G$	RG-módulo R con acción trivial de G
$R^\sigma_\alpha G$	producto cruzado de G sobre R, relativo a la acción σ y al conjunto de factores α
$R_\alpha G$	anillo de grupo torcido de G sobre R

Teoría de Cohomología

$Z^2_\sigma(G,\mathcal{U}(R))$	conjuntos de factores o 2-cociclos
$B^1_\sigma(G,\mathcal{U}(R))$	derivaciones o 1-cobordes
$B^2_\sigma(G,\mathcal{U}(R))$	conjuntos de factores principales o 2-cobordes
$H^2_\sigma(G,\mathcal{U}(R))$	segundo grupo de cohomología

Teoría de Cuerpos

K^*	grupo de unidades de un cuerpo K
L/K	extensión de cuerpos
$\mathbb{F}_p$	cuerpo cíclico de p elementos

Teoría de Representaciones

ρ_M	representación asociada al módulo M
$\rho_1 \sim \rho_2$	representaciones equivalentes
ρ^*	representación matricial correspondiente a ρ
$\mathrm{res}^G_H(M)$, $M\|_H$, M_H	módulo restringido de RG a RH
$\mathrm{res}^A_{A_1}(M)$, M_{A_1}	módulo restringido de A a A_1
$\mathrm{ind}^G_H(L)$, L^G	módulo inducido de RH a RG
$\mathrm{ind}^A_{A_1}(L)$, L^A	módulo inducido de A_1 a A
$\mathbf{L}^G$	representación (matricial) inducida
χ^G	carácter inducido
${}^a\mathbf{L}$	representación (matricial) conjugada
${}^a\chi$	carácter conjugado
$\mathrm{Ind}\, RG$	conjunto de los RG-retículos indescomponibles

Índice alfabético

álgebra, 7
    de endomorfismos, 9
    de grupo, 35
    graduada, 37
    opuesta, 10
    sobre un anillo conmutativo, 7
anillo
    base de un anillo graduado, 37
    completo, 22
      en la topología N-ádica, 22
    de Dedekind, 18, 19
    de grupo, 33
      entero, 81
      inclinado, 41
      torcido, 41
    de valoración, 16
      discreta, 16, 17
    fuertemente graduado, 37
    graduado, 37
    p-ádico, 28
anulador, 13
aumento, 36
    homomorfismo de, 35
    ideal de, 36
    parcial, 84
AVD = anillo de valoración discreta, 16

cambio de base diagonal, 44
carácter, 54
    conjugado, 64
    de una representación, 54
    de una representación matricial, 54
    inducido, 59
    permitido por un RG-módulo, 54
clausura entera en una R-álgebra, 11
coborde, 45
cociclo, 45
cociente de una serie normal, 85
completación, 20
    p-ádica, 23
    φ-ádica, 20
componente homogénea, 37
Conjeturas de Zassenhaus, 104
conjunto de factores, 41, 45
    equivalente, 45
    principal, 45
    trivial, 41
cuerpo
    de clases de residuos, 16
    de números, 10
    de residuos, 16
    perfecto, 6

derivación, 45
dividir (ideal), 31
dominio de Dedekind, 18, 19

elemento
    de torsión (de un grupo), 82

de torsión (de un módulo), 13
libre de torsión, 13
p-, 46
p-regular, 47
p-singular, 47
p'-, 47
primo (de un AVD), 17
uniformizador, 17
entero
algebraico, 11
sobre R, 10
enteros p-ádicos, 24
anillo de los, 24
espectro, 84
expansión p-ádica, 28
extensión
de un AVD, 32
no ramificada, 31
en un ideal, 31
totalmente ramificada, 31

grado
de residuos, 31
de una representación, 52
de una representación matricial, 52
grafo primo, 109
grupo
resoluble, 86
valor, 15

homomorfismo
de R-álgebras, 9
normalizado, 108

idempotentes ortogonales, 12
índice de ramificación, 31
inducción, 58
íntegramente cerrado, 11
en una R-álgebra, 11

longitud derivada, 86

métrica φ-ádica, 15
módulo
absolutamente indescomponible, 32
conjugado, 64
de torsión, 13
estable o estable relativo a A, 68
(G, H)-inyectivo, 70
(G, H)-proyectivo, 70
indescomponible, 29
principal, 88
inducido, 58, 68
inyectivo relativo, 70
libre de torsión, 13
proyectivo relativo, 70
restringido, 58, 68
subyacente, 9

números p-ádicos, 23
cuerpo de los, 23

orden, 28

parte
p-, 77
p-regular, 77
p'-, 77
Problema
del Automorfismo, 108
del Espectro, 84, 109
del Grafo Primo, 109
del Isomorfismo, 103
producto cruzado, 41

racionalmente conjugado, 93
radical
de Jacobson, 13
de un módulo, 13
representación, 50

asociada a un RG-módulo, 50
equivalente, 50
regular, 55
trivial, 55
representación matricial, 52
conjugada, 64
correspondiente a una representación, 53
equivalente, 53
inducida, 59
permitida por un RG-módulo, 53
restricción de escalares, 58
retículo, 71
de permutación, 87

segundo grupo de cohomología, 46
semilocalización, 88
serie
derivada, 86
normal, 85
soporte de un elemento de RG, 34
subálgebra, 8
submódulo conjugado de L en L^A, 68
sucesión coherente, 25

Teorema
de Berman-Higman, 82
de Green de los Ceros de Caracteres, 77
de Hertweck, 85, 100
de Indescomponibilidad de Green, 73
de Krull-Schmidt-Azumaya (K-S-A), 29
de Weiss, 87
del Subgrupo de Mackey, 66
topología N-ádica, 22
traza, 53

unidad de $\mathbb{Z}G$
trivial, 82

valoración, 14
arquimediana, 15
discreta, 15
equivalente, 16
exponencial, 17
P-ádica, 19
p-ádica, 23
no arquimediana, 15
P-ádica, 19
p-ádica, 23
trivial, 15