Teoría de representación de álgebras asociativas

Marcos Caso Huerta

Tutora: Consuelo Martínez López

Universidad de Oviedo
Curso 2017/18

Índice

1. Introducción

La teoría de Galois, comenzada por el archiconocido prodigio de las matemáticas Évariste Galois (1811-1832) supuso una auténtica revolución en el campo de las matemáticas. Partiendo de la búsqueda de soluciones de ecuaciones polinómicas y de fórmulas para la resolución de polinomios de grado cinco o superior (ya se habían encontrado fórmulas hasta grado cuatro por simple fuerza bruta), desarrolló resultados que dieron origen a las modernas teoría de cuerpos y teoría de grupos, y es que sus resultados permitían relacionar las propiedades de los cuerpos (en particular conceptos como irreducibilidad o separabilidad) con la naturaleza de los que se llamaron grupos de Galois, que no son sino subgrupos del grupo de permutaciones de las raíces del polinomio en estudio.

Así, los avances durante el mismo siglo XIX de matemáticos como Niels Henrik Abel, Richard Dedekind, Leopold Kronecker o Heinrich Martin Weber, y ya en el siglo XX de Emil Artin principalmente permitieron desarrollar lo que ahora llamamos teoría de cuerpos partiendo del trabajo de Galois. Por su parte, matemáticos como Augustin-Louis Cauchy, Camille Jordan, Ludwig Sylow y especialmente Ferdinand G. Frobenius, que formalizó la definición de grupo sin acudir al grupo de permutaciones, hicieron lo propio con la teoría de grupos, mientras que Élie Cartan abrió todo un nuevo campo de investigación con su trabajo en grupos de Lie.

Sin embargo, dos de las principales ramas del álgebra vieron su desarrollo más tardío, la teoría de anillos y la teoría de álgebras (que, a la postre, no será sino una generalización de los anillos). Al contrario que las anteriores, la teoría de anillos no surgió directamente de la teoría de Galois, sino que se desarrolló sobre la teoría de números algebraica, sobre la geometría algebraica y sobre la teoría de invariancia, mucho más avanzadas. Su origen estuvo en el desarrollo de lo que se llamó números hipercomplejos, una idea de extensión de los números complejos. Como los números complejos son algebraicamente cerrados, no existe ningún cuerpo que sea extensión finita suya, por lo que los desarrollos finitos sobre ellos constituirían una estructura algebraica diferente. William Rowan Hamilton desarrolló los cuaternios y los bicuaternios; James Cockle, los

tesarines y cocuaternios, y William K. Clifford lo que se conoce como bicuaternios de Clifford.

Inicialmente, todas estas estructuras se estudiaban desde la rama del álgebra universal, que no se centra en las clases de estructuras sino en cada estructura individualmente. Fue con el trabajo de Joseph Wedderburn y Emil Artin con el que se plantearon con rigor los fundamentos de la teoría de anillos, mientras que Emmy Noether introduciría el concepto de ideales.

La teoría de álgebras sobre cuerpos (y posteriormente y de forma más general, sobre anillos) fue desarrollada a finales del siglo XIX por matemáticos como Sophus Lie, Wilhelm Killing o Élie Cartan, aunque su mayor desarrollo se daría en la primera mitad del siglo XX con los revolucionarios trabajos de Burnside, Noether, Artin, Brauer, Wedderburn o Jacobson, entre otros, y pasaría a verse como una teoría particular de módulos sobre anillos.

Esta teoría, y en particular el trabajo en representaciones de álgebras, tuvo y sigue teniendo una importancia capital en la matemática moderna, y es una herramienta básica en campos como teoría de números algebraica, geometría algebraica, álgebra homológica, teoría de categorías y por supuesto teoría de grupos, de anillos conmutativos y de cuerpos.

Además, con el gran desarrollo del campo de la física matemática desde la segunda mitad del siglo XX, la teoría de álgebras y su aplicación a teoría de grupos han tenido un enorme impacto en la física, en campos que van desde la mecánica teórica o la hidrodinámica hasta la física más abstracta como pueda ser la mecánica cuántica o la teoría de cuerdas.

La teoría de representación de grupos, por su parte, llevó un desarrollo paralelo aunque confluyente, con una influencia capital del completo trabajo de Frobenius en las dos últimas décadas del siglo XIX, y se unificaría en la teoría de representación más general con el trabajo de Noether en la década de 1920.

Nuestro objetivo en este trabajo será dar una visión resumida de los conceptos clave de las álgebras sobre cuerpos y anillos hasta llegar a poder definir y entender las representaciones de álgebras.

Por razones de espacio, sin embargo, no podremos realizar un estudio completo y sistemático de toda la teoría de álgebras, y quedarán abiertas cuestiones de importancia en lo que se conoce como módulos proyectivos sobre álgebras

artinianas y, sobre todo, en la amplia teoría de cohomología de álgebras, que no trataremos.

2. Definiciones y conceptos básicos

2.1. Álgebras asociativas. Generalidades.

En esta primera sección haremos un breve repaso de diferentes conceptos básicos necesarios para su desarrollo. Nuestro primer paso será definir las estructuras algebraicas que utilizaremos.

Definición 2.1. Un **anillo** es un conjunto no vacío R junto con dos operaciones binarias (denotadas usualmente suma (+) y multiplicación) tales que:

(I). $(R,+)$ es un grupo abeliano.

(II). $(ab)c = a(bc)$ para todo $a,b,c \in R$ (propiedad asociativa de la multiplicación).

(III). $a(b+c) = ab+ac$ y $(a+b)c = ac+bc$ (propiedad distributiva a izquierda y derecha).

Si el producto cumple:

(IV). $ab = ba$ para todo $a,b \in R$,

se dice que R es un **anillo conmutativo**. Si R está dotado de un elemento 1_R tal que

(V). $1_R a = a1_R = a$ para todo $a \in R$,

se dice que R es un **anillo con identidad**.

El elemento neutro de la suma en un anillo se llama elemento cero y se denota 0. Si $a \in R$ y $n \in \mathbb{Z}$, la notación na tiene el significado habitual de grupos abelianos ($na = a+a+...+a$ con $n > 0$).

Definición 2.2. Sea R un anillo. Un R-**módulo** (a izquierda) es un grupo abeliano A junto con una función $R \times A \to A$ (denotaremos la imagen de (r,a) como ra) tal que para todo $r,s \in R$ y $a,b \in A$:

(I). $r(a+b) = ra + rb$.

(II). $(r+s)a = ra + sa$.

(III). $r(sa) = (rs)a$.

Si R tiene elemento identidad 1_R y se cumple que:

(IV). $1_R a = a$ para todo $a \in A$,

se dice que A es un R-**módulo unitario**. Si R es un anillo de división, un R-módulo unitario se denomina **espacio vectorial** (a izquierda).

Las propiedades de R-módulo a derecha se definen de forma análoga.

Una vez definidas estas estructuras fundamentales podemos pasar a definir un álgebra sobre un anillo, que será el objeto fundamental del presente trabajo. A partir de este punto, R denotará siempre un anillo conmutativo con identidad 1.

Definición 2.3. Una R-**álgebra** (o *álgebra sobre* R) es un R-módulo unitario a derecha A sobre el que se define una aplicación bilineal $A \times A \to A$ (denotada $(x, y) \mapsto xy$) que es asociativa ($x(yz) = (xy)z$ para todo $x, y, z \in A$), y para la que existe un elemento unidad 1_A tal que $1_A x = x 1_A = x$ para todo $x \in A$.

La condición de bilinealidad es equivalente a la propiedad distributiva a izquierda y derecha más la propiedad añadida:

$$(xy)a = x(ya) = (xa)y, \quad \forall x, y \in A, \quad \forall a \in R \tag{2.1}$$

Las R-álgebras cumplen la propiedad de ser anillos con identidad, y de forma análoga si A es un anillo con identidad y un R-módulo a derecha que cumple (2.1) entonces A es una R-álgebra.

Se puede definir una R-álgebra no asociativa como un R-módulo A dotado de una aplicación bilineal cualquiera.

Debido a la bilinealidad de la multiplicación y a las identidades de módulos, se tiene que la aplicación $a \mapsto 1_A a$ es un homomorfismo de anillos de R en el centro de A. Análogamente, si R es un anillo con identidad, todo homomorfismo de R en el centro de A induce una estructura de R-módulo en A, lo que lo

convierte en una R-álgebra. Asimismo, si la aplicación $a \mapsto 1_A$ es inyectiva (esto es, A es un R-módulo fiel), se puede identificar R con un subanillo del centro de A. A través de esta identificación, tenemos que $xa = ax$, lo que convierte A en un R-módulo a izquierda. Incluso si A no es fiel como módulo, se puede definir una estructura de R-módulo a izquierda fijando que $ax = xa$, ya que R es conmutativo.

Del mismo modo que todo grupo abeliano es un $\mathbb{Z}$-módulo, todo anillo asociativo con identidad es una $\mathbb{Z}$-álgebra. Por tanto, la categoría de R-álgebras es muy grande.

Denotaremos a partir de ahora por F un cuerpo. En particular F es un anillo, por lo que podemos definir una estructura de F-álgebra, que de forma trivial adquiere la estructura de espacio vectorial sobre F (por ser en particular un F-módulo). La estructura de módulo de A estará determinada por su dimensión como espacio vectorial, que denotaremos $\dim(A)$ o $\dim_F(A)$, que para nuestros propósitos será un número natural o ∞.

La restricción a cuerpos simplificará el trabajo al poder aplicar métodos del álgebra lineal, y permitirá obtener con relativa facilidad interesantes resultados. Un resultado importante en este apartado es que el homomorfismo $a \mapsto 1_A a$ encaja F en A siempre que A sea no trivial ($0 \neq 1_A$), por lo que se puede identificar F con un subanillo del centro de A. Esto en particular provee que $1_A = 1$.

Definición 2.4. Sean A y B dos R-álgebras y f una aplicación de A en B. Decimos que f es un *homomorfismo de álgebras* si es simultáneamente un homomorfismo de módulos y un homomorfismo de anillos que preserva el elemento unidad. Análogamente se definen los conceptos de isomorfismos, endomorfismos y automorfismos de álgebras.

Denotaremos $A \cong B$ si existe un isomorfismo entre A y B. Claramente, $\cong$ es una relación de equivalencia.

Daremos dos definiciones diferentes de la estructura de subálgebra, que son fundamentalmente dos formas de ver un mismo concepto:

Definición 2.5. Sea A una R-álgebra. Diremos que $B \subset A$ es una R-subálgebra si cumple una de las siguientes propiedades:

(I). B es un subconjunto de A que incluye el 0 y el 1 y que es cerrado bajo la suma, multiplicación y operaciones escalares de A.

(II). B es una R-álgebra subconjunto de A tal que la aplicación inclusión de B en A es un homomorfismo de álgebras.

Si $\phi : A \to B$ es un homomorfismo de R-álgebras a derecha, entonces el núcleo de ϕ, que denotaremos $\text{Ker}\phi = \{x \in A : \phi(x) = 0\}$, cumple de forma inmediata que es un ideal bilátero y un R-submódulo de A. Análogamente, si I es un ideal de anillos de A (que denotaremos $I \lhd A$), entonces I es automáticamente un R-submódulo, ya que $xa = x(1_A a) \in I$ con $x \in I$ y $a \in R$. Se observa fácilmente que el anillo cociente A/I es una R-álgebra a derecha, y que la aplicación proyección natural $\pi : A \to A/I$ es un homomorfismo de álgebras con núcleo I. Así, los teoremas y resultados de homomorfismos de anillos y módulos son válidos sin modificación para álgebras.

Uno de los resultados más importantes que se pueden trasladar de forma inmediata a álgebras es el criterio de factorización:

Teorema 2.6. Sean A, B y C tres R-álgebras y sean $\phi : A \to B$ y $\psi : A \to C$ dos homomorfismos de R-álgebras con ϕ suprayectivo. Entonces ψ se factoriza por ϕ (esto es, existe un homomorfismo $\theta : B \to C$ tal que $\psi = \theta\phi$) si y solo si $\text{Ker}\phi \subseteq \text{Ker}\psi$.

Se puede definir un módulo sobre una R-álgebra de forma idéntica a la definición de un módulo unitario sobre un anillo. De esta forma, si A es una R-álgebra y M es un A-módulo a derecha, entonces M hereda una estructura de R-módulo de la siguiente forma: $ua = u(1_A a)$ con $u \in M$ y $a \in R$. Análogamente, si M es un A-módulo a izquierda, es también un R-módulo a izquierda. En particular, todo módulo sobre una F-álgebra es también un espacio vectorial.

Veamos ahora el concepto de bimódulo:

Definición 2.7. Sean A y B dos R-álgebras, se dice que M es un A-B-bimódulo si es un sistema algebraico que es simultáneamente un A-módulo a izquierda y un B-módulo a derecha, tal que:

$$(xu)y = x(uy) \quad \forall x \in A, \quad \forall u \in M, \quad \forall y \in B \tag{2.2}$$

$$au = ua \quad \forall a \in R, \quad \forall u \in M \tag{2.3}$$

A continuación veremos algunos ejemplos de álgebras cuyo estudio resulta de gran interés y de gran aplicación en el campo de las matemáticas y campos relacionados.

2.1.1. Álgebras de endomorfismos

Las álgebras de endomorfismos sobre un anillo dado serán la principal base sobre la que construiremos la teoría de representación, y son de fundamental importancia en su estudio.

Sea A una R-álgebra y sean M y N dos A-módulos a izquierda o derecha. Denotaremos el conjunto de los homomorfismos de A-módulos de M en N como $\mathrm{Hom}_A(M,N)$. El conjunto $\mathrm{Hom}_A(M,N)$ tiene estructura de R-módulo definiendo la suma y la multiplicación por escalares de la forma: $(\phi+\psi)(u) = \phi(u)+\psi(u)$, $(\psi a)(u) = \psi(u)a$. Si M coincide con N, entonces la composición de homomorfismos, $(\phi\psi)(u) = \phi(\psi(u))$, define un producto bilineal asociativo con el cual el conjunto $\mathrm{Hom}_A(M,M)$ adquiere estructura de R-álgebra con elemento unidad id_M.

Denotaremos este último $E_A(M)$ y la llamaremos álgebra de endomorfismos del módulo M.

La aplicación de $E_A(M)$ sobre M induce en M una estructura de $E_A(M)$-módulo a izquierda. De esta forma, un A-módulo a derecha M adquiere una estructura de $E_A(M)$-A-bimódulo. Dados $\phi \in E_A(M)$, $u \in M$, $x \in A$ y $a \in R$, se cumple la identidad $\phi(ux) = (\phi u)x$ gracias a que ψ es un homomorfismo de A-módulos y $au = (\mathrm{id}_M a)(u) = (\mathrm{id}_M u)(a)$ por la definición de multiplicación por escalares en $E_A(M)$.

Aprovecharemos esta estructura para definir el concepto de representación de un álgebra.

Sean A y B dos R-álgebras y M un A-B-bimódulo. Para $x \in A$, definimos $\lambda_x : M \to M$ por $\lambda_x u = xu$. Es claro que $\lambda_x \in E_B(M)$, la aditividad es inmediata y por las propiedades de R-álgebra tenemos que $\lambda_x(uy) = x(uy) = (xu)y = \lambda_x(u)y$. De forma análoga, para $y \in B$ definimos $\rho_y : M \to M$ por $\rho_y u = uy$. Así, $\rho_y \in$

$E_A(M)$.

Es claro que la aplicación $x \mapsto \lambda_x$ es un homomorfismo de anillos, y con las propiedades que hemos visto es de hecho un homomorfismo de R-álgebras: $\lambda_{xa}u = x(au) = x(ua) = (xu)a = (\lambda_x u)a = (\lambda_x a)u$ con $x \in A$, $a \in R$, $u \in M$, de forma que actúa sobre R.

Por su parte, la aplicación producto por escalares a derecha no es un homomorfismo de anillos, sino un antihomomorfismo. Tenemos que $\rho_{xy}u = uxy = \rho_y(ux) = \rho_y\rho_x u$. Se puede ver como un homomorfismo del opuesto de B, B^*, en $E_A(M)$, siendo B^* el opuesto habitual en categorías que se obtiene de B invirtiendo el orden de los factores en los productos.

Denotaremos el homomorfismo $x \mapsto \lambda_x$ y el antihomomorfismo $y \mapsto \rho_y$ por λ y ρ respectivamente.

Si M es un A-módulo a izquierda, entonces se puede ver M como un A-R-bimódulo, ya que R es conmutativo. En este caso, se dice que λ es una representación de A, esto es, un homomorfismo de álgebras de A en $E_R(M)$. Análogamente, si $\phi : A \to E_R(M)$ es una representación, entonces M es un A-módulo a derecha con $xu = \phi(x)u$, donde $u \in M$, $x \in A$. De esta forma, se tiene una correspondencia unívoca entre representaciones de un álgebra A y A-módulos a izquierda. De forma análoga tenemos una relación entre los A-módulos a derecha y las representaciones de su dual A^*.

Es inmediato obtener que si ϕ y ψ son dos homomorfismos de A en $E_R(M)$, es decir, representaciones sobre el mismo R-módulo, entonces ϕ y ψ inducen estructuras de A-módulo isomorfas en M si y solo si existe un elemento inversible θ en $E_R(M)$ tal que $\psi(x) = \theta^{-1}\phi(x)\theta$ para todo $x \in A$. Generalizando el resultado, existe un homomorfismo entre las estructuras de módulo definidas sobre M a través de ϕ y ψ si y solo si existe un endomorfismo de R-módulos $\theta \in E_R(M)$ tal que $\phi(x)\theta = \theta\psi(x)$ para todo $x \in A$. En ese caso se dice que θ entrelaza las representaciones ϕ y ψ.

Debido a las propiedades de asociatividad y a la existencia de elemento identidad, toda R-álgebra A adquiere una estructura de A-bimódulo, por lo que podemos construir representaciones usando A como módulo de representación. Los homomorfismos correspondientes λ y ρ de A en $E_A(A)$ se llaman respectivamente representación regular a izquierda y a derecha de A.

Podemos obtener una propiedad muy interesante de estas representaciones regulares por métodos elementales:

Proposición 2.8. Sea A una R-álgebra y sean λ y ρ sus representaciones regulares a izquierda y derecha respectivamente. Entonces λ y ρ son aplicaciones biyectivas. En particular, $A \cong E_A(A)$ como R-álgebras, considerando A como un A-módulo a derecha.

Demostración Hemos visto anteriormente que $\lambda : A \to E_A(A)$ es un homomorfismo de R-álgebras con núcleo $\{x \in A : xA = 0\}$, que ha de ser un ideal de A, pero este ideal es 0 ya que A tiene elemento unidad. Entonces $\phi(x) = \phi(1 \cdot x) = \phi(1)x = \lambda_y x$ donde $y = \phi(1)$. Así, λ es suprayectiva. De forma análoga vemos que ρ es también biyectiva.

2.1.2. Álgebras de grupos

El estudio de la teoría de representación de álgebras asociativas está íntimamente ligado con el estudio de la representación de grupos, y a nivel histórico tuvo en él uno de sus principales objetivos. Para realizar ese estudio se debe definir el concepto de álgebra de grupo. Fundamentalmente, un álgebra de grupo sobre R es una R-álgebra que se construye como un R-módulo libre con una base que consiste en los elementos de un grupo G, con la multiplicación inducida por la operación interna de G.

En particular es de amplio uso la construcción de álgebras de grupo sobre cuerpos, en cuyo caso se construye un espacio vectorial tomando cada elemento de G como un vector de la base. De esta forma, la estructura como espacio vectorial está unívocamente determinada por la cardinalidad del grupo G mientras que la estructura interna está determinada por su estructura de grupo. De esta forma el estudio de álgebras de grupo de determinada dimensión se reduce al estudio de los grupos de la misma cardinalidad.

Podemos generalizar la definición a la de álgebra de convolución, que se construye a partir de un monoide (un conjunto con multiplicación asociativa con elemento unidad) sobre un anillo:

Definición 2.9. Sea G un monoide y R un anillo conmutativo con elemento

unidad. Denotamos:

$$RG = \{\xi \in R^G : \xi(x) = 0 \quad \text{para casi todo} \quad x \in G\}. \tag{2.4}$$

Definimos la suma y la multiplicación por escalares de elementos de RG componente a componente:

$$(\xi a + \eta b)(x) = \xi(x)a + \eta(x)b \quad \forall a, b \in R, \quad \forall \xi, \eta \in RG, \quad \forall x \in G \tag{2.5}$$

Y definimos la multiplicación interna por convolución:

$$(\xi\eta)(x) = \sum \xi(y)\eta(z), \tag{2.6}$$

sumado sobre el conjunto finito de pares $(y,z) \in G \times G$ tales que $yz = x$ y $\xi(y)\eta(z) \neq 0$.

Definimos para cada $x \in G$ la función $\chi_x \in R^G$ dada por $\chi_x(z) = 0$ si $z \neq x$, y $\chi_x(x) = 1$. Es claro que dado $\xi \in RG$ se tiene que $\xi = \sum \chi_x \xi(x)$, sumado sobre todos los $x \in G$ tales que $\xi(x) \neq 0$. Se sigue que RG es un R-módulo libre con base $\{\chi_x : x \in G\}$.

Además, $\chi_x(u)\chi_y(v) = 0$ si $u \neq x$ o $v \neq y$, y $\chi_x(x)\chi_y(y) = 1$. Así, $(\chi_x\chi_y)(z) = 0$ si $z \neq xy$, y $(\chi_x\chi_y)(xy) = 1$. Por tanto, es claro que $\chi_x\chi_y = \chi_{xy}$. Se puede demostrar por procedimientos elementales que χ_1 es el elemento unidad de RG y que RG cumple las propiedades de R-álgebra.

Por lo anterior, se tiene que la aplicación $x \mapsto \chi_x$ es un homomorfismo de monoides inyectivo. Por tanto, se puede identificar x con su correspondiente función χ_x. Utilizando esta convención podemos simplificar la notación y denotar los elementos de RG como las combinaciones lineales $\sum x a_x$ con $x \in G$, $a_x \in R$ y la suma extendida a un subconjunto finito de G. Salvo el orden de los sumandos, esta representación es única.

Finalmente, es fácil observar que si G es un monoide, A una R-álgebra y $\phi : G \to A$ un homomorfismo de G en el monoide multiplicativo de A, entonces ϕ se extiende de forma única a un homomorfismo de R-álgebras de RG en A.

Efectivamente, cualquier extensión de ϕ a homomorfismo de módulos sa-

tisfará la relación:

$$\phi(\sum xa_x) = \sum \phi(x)a_x \tag{2.7}$$

Dado que G es una base de RG, esta relación define una extensión de ϕ a un homomorfismo de módulos. Usando la distributividad y las propiedades de ϕ se puede comprobar con facilidad que esta extensión es también un homomorfismo de anillos.

Notemos, por otra parte, que si bien la presentada es la definición formal de álgebra de grupo, es mucho más intuitivo pensar en ella como el R-módulo libre construido tomando como base los elementos de G. Es decir, podemos pensar en el álgebra de grupo como las combinaciones lineales finitas formales de elementos del grupo con coeficientes en R dotadas con las operaciones inducidas por las de R y G,

$$\left(\sum_{g\in G} a_g g\right) + \left(\sum_{g\in G} b_g g\right) = \sum_{g\in G} (a_g + b_g)g, \quad a_g, b_g \in R \quad \forall g \in G \tag{2.8}$$

$$\left(\sum_{g\in G} a_g g\right)\left(\sum_{g\in G} b_g g\right) = \sum_{g,h\in G} (a_g b_h)(gh), \quad a_g, b_g \in R \quad \forall g \in G \tag{2.9}$$

$$\left(\sum_{g\in G} a_g g\right) b = \sum_{g\in G} (a_g b)g, \quad a_g, b \in R \quad \forall g \in G \tag{2.10}$$

En el caso de álgebras de grupos construidas sobre cuerpos, los elementos de G conformarían los vectores de la base del álgebra como espacio vectorial, que sería por tanto de dimensión $|G|$.

2.1.3. Álgebras matriciales

Las álgebras matriciales son un tipo de álgebra de fácil manejo y construcción. Dada una R-álgebra A, denotaremos con $M_n(A)$ el conjunto de las matrices $n \times n$ con entradas en A. Es claro que $M_n(A)$ será también una R-álgebra con las operaciones comunes de suma y multiplicación de matrices y operaciones con escalares por elementos de R. Llamaremos a $M_n(A)$ el álgebra matricial $n \times n$ sobre A.

En general denotaremos las matrices con letras griegas minúsculas. En particular llamaremos ι o ι_n a la matriz identidad $n \times n$. Asimismo denotaremos ϵ_{ij} a las unidades matriciales para n y A fijados. Esto es, ϵ_{ij} denotará la matriz $n \times n$ con la unidad de A en la fila i, columna j, y el cero de A en las demás entradas. Se tiene que estas matrices cumplen:

$$\forall 1 \leq i, j, k, l \leq n, \quad \epsilon_{ij}\epsilon_{kl} = 0 \quad \text{si} j \neq k; \quad \epsilon_{ij}\epsilon_{jl} = \epsilon_{il} \tag{2.11}$$

Para describir una matriz en términos de sus entradas, usaremos la siguiente notación:

$$\alpha = [x_{ij}]; \quad \alpha = \begin{bmatrix} x_{11} & x_{12} & \dots & x_{1n} \\ x_{21} & x_{22} & \dots & x_{2n} \\ . & . & . & . \\ x_{m1} & x_{m2} & \dots & x_{mn} \end{bmatrix} \tag{2.12}$$

Es decir, denotaremos las entradas de la matriz con letras con dos subíndices que indicarán respectivamente la fila y la columna de la entrada.

Si A no es conmutativo como anillo entonces $M_n(A)$ no será una A-álgebra, pero será útil definir de todos modos la multiplicación por elementos de A. Si $\alpha = [x_{ij}] \in M_n(A)$ e $y \in A$, definiremos los productos $y\alpha = [yx_{ij}]$, $\alpha y = [x_{ij}y]$. Esta definición nos permite inducir una estructura de A-bimódulo en $M_n(A)$. Se puede observar que $M_n(A)$ tiene estructura de A-módulo libre con una base formada por las unidades matriciales:

$$[x_{ij}] = \sum_{ij} \epsilon_{ij} x_{ij} \tag{2.13}$$

y esta representación es única. Además, trivialmente cumple la propiedad:

$$(\alpha y)\beta = \alpha(y\beta) \quad \forall \alpha, \beta \in M_n(A), \quad \forall y \in A \tag{2.14}$$

Demostraremos en un apartado posterior que las álgebras matriciales son casos particulares de álgebras de endomorfismos, y de hecho se tiene que $M_n(A) \cong E_A(M)$ con M el A-módulo libre a derecha sobre n generadores. Por ello todos los resultados que obtengamos para álgebras de endomorfismos serán válidos para álgebras matriciales, aunque en muchos casos si se puede pa-

sar a un álgebra matricial los cálculos serán más sencillos.

Un ejemplo de resultado de álgebras matriciales será su construcción sobre álgebras de división, y en particular sobre álgebras sobre cuerpos, que tendrá importancia al estudiar su estructura.

Lema 2.10. Si D es un álgebra de división, entonces $M_n(D)$ es simple para todo $n \geq 1$.

Demostración Sea I un ideal no nulo de $M_n(D)$. Debemos probar que si $\alpha = [x_{ij}] \in M_n(D)$, entonces $\alpha \in I$. Dado que $I \neq 0$, existe un $\beta = [y_{ij}]$ no nulo en I. Supongamos $y_{rs} \neq 0$. Por (2.13) y (2.14) tenemos que $\alpha = \sum_{ij} \epsilon_{ij} x_{ij} = \sum_{ij} (\epsilon_{ir} \beta \epsilon_{sj}) y_{rs}^{-1} x_{ij} \in I$, ya que I es un ideal bilátero de $M_n(D)$.

2.1.4. Álgebras finito-dimensionales sobre un cuerpo

Haremos una breve consideración de la construcción de álgebras de dimensión finita sobre cuerpos. Como remarcamos con anterioridad, si A es una F-álgebra sobre un cuerpo F, en particular es un F-módulo y por tanto un espacio vectorial. Por tanto su estructura aditiva estará definida por su dimensión como espacio vectorial y tendrá una base $\{x_1, ..., x_n\}$. Por tanto se podrán inducir las estructuras de álgebra en A sin más que especificar los productos

$$x_i x_j = \sum_{k=1}^{n} x_k a_{ij}^k, \quad a_{ij}^k \in F, \quad 1 \leq i, j \leq n \tag{2.15}$$

Y esta relación se extiende con unicidad a un producto bilineal en A con la regla $(\sum_i x_i b_i)(\sum_j x_j c_j) = \sum_k x_k (\sum_{ij} b_i c_j a_{ij}^k)$. Los n^3 elementos a_{ij}^k se denominan constantes de estructura del producto.

Sin embargo en general la estructura de álgebra será no asociativa. Como vimos en la construcción de las álgebras de grupo, el producto será asociativo si y solo si $x_i(x_j x_k) = (x_i x_j)x_k$ para todo i, j, k entre 1 y n. Eso nos lleva a que las constantes de estructura habrán de satisfacer:

$$\sum_{r=1}^{n} a_{ij}^r a_{rk}^s = \sum_{r=1}^{n} a_{jk}^r a_{ir}^s \quad \forall 1 \leq i, j, k, s \leq n \tag{2.16}$$

A partir de esta relación se puede obtener una nueva condición para ga-

rantizar la asociatividad. Asociaremos a cada transformación lineal ϕ y cada F-base $\{x_1, ..., x_n\}$ de A la matriz $\alpha(\phi) = [a^k_{\phi j}]$ definida por $\phi(x_m) = \sum_{k=1}^{n} x_k a^k_{\phi j}$. Como se verá más adelante, la aplicación $\phi \mapsto \alpha(\phi)$ es un isomorfismo de $E(A)$ en $M_n(F)$. Es fácil ver que $[a^k_{ij}]$ es la matriz asociada de esta forma a λ_{x_i} al mismo tiempo que a ρ_{x_j}. Así, la identidad anterior equivale a las condiciones

$$\lambda_{x_i}\rho_{x_k}(x_j) = \rho_{x_k}\lambda_{x_i}(x_j) \quad \forall 1 \leq i, j, k \leq n \tag{2.17}$$

Así, (2.16) es una versión coordenada de la condición de conmutación de las representaciones regulares de A, lo cual equivale a la asociatividad.

Por otra parte, para tener un álgebra asociativa es necesario que tenga unidad. La manera más sencilla de comprobar que las ecuaciones (2.15) definen un álgebra con unidad es requerir que uno de los elementos de la base, *e. g.* x_1, actúe como la unidad. Es claro que esta condición es equivalente a

$$a^k_{1j} = a^k_{j1} = \delta_{jk} \quad \forall 1 \leq j, k \leq n \tag{2.18}$$

con δ_{jk} la delta de Kronecker. Dicho de otro modo, la condición equivale a $\lambda_{x_1} = \rho_{x_1} = \mathrm{id}_A$.

Es importante remarcar que con este requerimiento no hemos limitado las álgebras que podemos construir sobre F, ya que si $n > 0$ toda F-álgebra n-dimensional A es no trivial, por lo que podemos tomar el elemento unidad de A como un elemento de la base.

Por limitación en la profundidad del trabajo no nos pararemos a estudiar la unicidad de estas construcciones, pero es un resultado conocido que dado un cuerpo F y un número natural $n \geq 1$ la cardinalidad de los tipos de isomorfismos de F-álgebras n-dimensionales es a lo sumo $|F|^{n^3}$.

2.1.5. Álgebras de cuaternios

La importancia de las álgebras de cuaternios y su relevancia histórica subyacen en el hecho de que es una de las álgebras no asociativas no triviales más sencillas que se pueden construir y en su importante aplicación en distintos campos, especialmente en física.

Realizaremos la construcción sobre un cuerpo F cuya característica no sea 2, debido a las particularidades de estos últimos.

Definición 2.11. Sea F un cuerpo de característica distinta de 2 y sean a y b dos elementos de F. Decimos que A es un álgebra de cuaternios generalizada sobre F y lo denotamos $A = \left(\frac{a,b}{F}\right)$ si A es el F-espacio vectorial de dimensión 4 con base $1, \mathbf{i}, \mathbf{j}, \mathbf{k}$ y dotado de la multiplicación bilineal definida por la actuación de 1 como elemento unidad y por las relaciones

$$\mathbf{i}^2 = a, \quad \mathbf{j}^2 = b, \quad \mathbf{ij} = -\mathbf{ji} = \mathbf{k} \tag{2.19}$$

donde en las dos primeras relaciones se utiliza la identificación convencional de F con los múltiplos escalares del elemento unidad de A. Asumiendo la asociatividad, el resto de la tabla de multiplicar para la base de A se sigue de forma inmediata:

$$\mathbf{k}^2 = -ab, \quad \mathbf{ik} = -\mathbf{ki} = \mathbf{j}a, \quad \mathbf{jk} = -\mathbf{kj} = -\mathbf{i}b \tag{2.20}$$

El caso ampliamente utilizado de los cuaternios de Hamilton son el caso particular $\mathbb{H} = \left(\frac{-1,-1}{\mathbb{R}}\right)$.

Estudiemos algunas propiedades de este tipo de álgebras:

Lema 2.12. Para todo $a, b \in F$ no nulos, $A = \left(\frac{a,b}{F}\right)$ es un álgebra simple con centro F.

Demostración. Introduciremos el llamado corchete de Lie: $[x, y] = xy - yx$. Si tomamos en general $x = c_0 + \mathbf{i}c_1 + \mathbf{j}c_2 + \mathbf{k}c_3 \in A$, entonces utilizando (2.19) y (2.20) tenemos que $[\mathbf{i}, x] = \mathbf{j}(2ac_3) + \mathbf{k}(2c_2)$, $[\mathbf{j}, x] = \mathbf{i}(-2bc_3) + \mathbf{k}(-2c_1)$ y $[\mathbf{k}, x] = \mathbf{i}(2bc_2) + \mathbf{j}(-2ac_1)$. En particular, si $x \in Z(A)$ se cumple que $[\mathbf{i}, x] = [\mathbf{j}, x] = [\mathbf{k}, x] = 0$, de forma que necesariamente $c_1 = c_2 = c_3 = 0$, por lo que $Z(A) = F$.

Para ver que es simple, suponemos $0 \neq x \in I$ con $I \lhd A$. Dado que I es un ideal bilátero que contiene a x, también incluye los productos triples de Lie $[\mathbf{j}, [\mathbf{i}, x]] = \mathbf{i}(-4bc_2)$, $[\mathbf{k}, [\mathbf{j}, x]] = \mathbf{j}(4abc_3)$ y $[\mathbf{i}, [\mathbf{k}, x]] = \mathbf{k}(-4ac_1)$. Si c_1, c_2 y c_3 no son todos cero, entonces I contiene una unidad de A; si $c_1 = c_2 = c_3 = 0$ entonces $0 \neq x = c_0$ es una unidad que pertenece a I. En cualquiera de los casos, $I = A$ por lo que A es simple.

Decimos que una F-álgebra A es central si $Z(A) = F$. Por tanto, las álgebras de cuaternios son centrales y simples. De hecho, se puede demostrar que toda álgebra central, simple y de dimensión cuatro es un álgebra de cuaternios. También se demuestra que un álgebra de cuaternios sobre F o bien es un álgebra de división o bien es isomorfa a $M_2(F)$.

2.2. Introducción al producto tensorial de módulos

2.2.1. Producto tensorial de dos módulos

Una importante construcción en el campo de las álgebras es el producto tensorial de álgebras, que trataremos con más detalle más adelante. En la presente sección realizaremos un breve repaso al más general producto tensorial de módulos, en el que profundizaremos más en la sección dedicada a módulos.

Sea R un anillo, M un R-módulo a derecha y N un R-módulo a izquierda. Consideraremos el llamado problema de la aplicación universal, con Σ la clase de estructuras de $\mathbb{Z}$-módulos (siendo los morfismos las aplicaciones $\mathbb{Z}$-lineales, es decir, los homomorfismos de grupos aditivos) y llamaremos α-aplicaciones a las aplicaciones f de $M \times N$ en un $\mathbb{Z}$-módulo G que sean $\mathbb{Z}$-bilineales y que además satisfagan para todo $x \in M$, $y \in N$ y $\lambda \in R$ la condición de aplicación equilibrada,

$$f(x\lambda, y) = f(x, \lambda y) \tag{2.21}$$

Es un resultado conocido que este problema admite solución. Por tanto, consideramos el $\mathbb{Z}$-módulo $C = \mathbb{Z}^{(M\times N)}$ de combinaciones lineales formales de los elementos de $M \times N$ con coeficientes en $\mathbb{Z}$. Una base de este módulo es el conjunto de pares ordenados (x, y) con $x \in M$, $y \in N$. Sea D el $\mathbb{Z}$-submódulo de C generado por elementos de los siguientes tipos:

$$\begin{cases} (x_1 + x_2, y) - (x_1, y) - (x_2, y) \\ (x, y_1 + y_2) - (x, y_1) - (x, y_2) \\ (x\lambda, y) - (x, \lambda y) \end{cases} \tag{2.22}$$

con $x, x_1, x_2 \in M$, $y, y_1, y_2 \in N$ y $\lambda \in R$.

Definición 2.13. El producto tensorial del R-módulo a derecha M y el R-módulo

a izquierda N, denotado $M \otimes_R N$ (o simplemente $M \otimes N$ si no se presta a confusión) es el $\mathbb{Z}$-módulo cociente C/D con C y D los definidos anteriormente. Dados $x \in M$ e $y \in N$, denotamos al elemento de $M \otimes N$ que es imagen canónica del elemento (x, y) de C como $x \otimes y$ y lo llamamos producto tensorial de x e y.

La aplicación $(x, y) \mapsto x \otimes y$ de $M \times N$ en $M \otimes N$ se denomina aplicación canónica, y es una aplicación $\mathbb{Z}$-bilineal que satisface (2.21).

Probemos que el producto tensorial junto con la aplicación canónica es una solución del problema de la aplicación universal anterior:

Proposición 2.14. (a) Sea g una aplicación $\mathbb{Z}$-lineal de $M \otimes N$ en un $\mathbb{Z}$-módulo G. La aplicación $(x, y) \mapsto f(x, y) = g(x \otimes y)$ de $M \times N$ en G en $\mathbb{Z}$-bilineal y satisface la condición (2.21).

(b) Recíprocamente, sea f una aplicación $\mathbb{Z}$-bilineal de $M \times N$ en un $\mathbb{Z}$-módulo G que satisface la condición (2.21). Entonces existe una única aplicación $\mathbb{Z}$-lineal g de $M \otimes N$ en G tal que $f(x, y) = g(x \otimes y)$ para todo $x \in M$, $y \in N$.

Demostración. Si ϕ denota la aplicación canónica de $M \times N$ en $M \otimes N$, entonces $f = g \circ \phi$, lo que demuestra (a).

Para probar (b), notemos que, en la notación usada, f se extiende a una aplicación $\mathbb{Z}$-lineal $\overline{f}$ de C en G. Por la relación (2.21), f vale cero para todos los elementos de C de uno de los tipos de (2.22) y por tanto sobre D. Por tanto existe una aplicación $\mathbb{Z}$-lineal g de $C/D = M \otimes N$ en G tal que $\overline{f} = g \circ \psi$, donde $\psi : C \to C/D$ es el homomorfismo canónico. La unicidad de g es inmediata ya que $M \otimes N$ está generado como $\mathbb{Z}$-módulo por los elementos $x \otimes y$.

Definimos así un isomorfismo canónico del $\mathbb{Z}$-módulo de aplicaciones $\mathbb{Z}$-bilineales f de $M \times N$ en G que satisfacen la condición (2.21) en el $\mathbb{Z}$-módulo $\mathrm{Hom}_{\mathbb{Z}}(M \otimes N, G)$.

Corolario 2.15. Sea H un $\mathbb{Z}$-módulo y $h : M \times N \to H$ una aplicación $\mathbb{Z}$-bilineal que satisface (2.21) y tal que H está generada por $h(M \times N)$. Supongamos que para todo $\mathbb{Z}$-módulo G y toda aplicación $\mathbb{Z}$-bilineal f de $M \times N$ en G que satisface (2.21) existe una aplicación $\mathbb{Z}$-lineal $g : H \to G$ tal que $f = g \circ h$. Entonces,

si ϕ denota la aplicación canónica de $M \times N$ en $M \otimes N$, existe un único isomorfismo θ de $M \otimes N$ en H tal que $h = \theta \circ \phi$.

Corolario 2.16. Sea M^* (resp. N^*) el módulo M (resp. N) considerado como módulo a izquierda (resp. a derecha) sobre el anillo inverso R^*. Entonces existe un único isomorfismo de $\mathbb{Z}$-módulos $\sigma : M \otimes_R N \to N^* \otimes_{R^*} M^*$ tal que $\sigma(x \otimes y) = y \otimes x$ para todo $x \in M$, $y \in N$ (propiedad de conmutatividad de productos tensoriales).

Las demostraciones de ambos corolarios son inmediatas usando la proposición probada y las propiedades del problema de la aplicación universal.

2.2.2. Producto tensorial de dos aplicaciones lineales

Sea R un anillo, M, M' dos R-módulos a derecha, N, N' dos R-módulos a izquierda y $u : M \to M'$ y $v : N \to N'$ dos aplicaciones R-lineales. Se comprueba fácilmente que la aplicación

$$(x, y) \mapsto u(x) \otimes v(y) \tag{2.23}$$

de $M \times N$ en $M' \otimes N'$ es $\mathbb{Z}$-bilineal y satisface la condición (2.21). Por la proposición 2.14 existe por tanto una única aplicación $\mathbb{Z}$-lineal $w : M \otimes N \to M' \otimes N'$ tal que

$$w(x \otimes y) = u(x) \otimes v(y) \tag{2.24}$$

para todo $x \in M$, $y \in N$. Esta aplicación se denota $u \otimes v$ y se denomina producto tensorial de las aplicaciones lineales u y v.

Se sigue de forma inmediata de (2.24) que la aplicación $(u, v) \mapsto u \otimes v$ es una aplicación $\mathbb{Z}$-bilineal que llamaremos canónica:

$$\mathrm{Hom}_R(M, M') \times \mathrm{Hom}_R(N, N') \to \mathrm{Hom}_{\mathbb{Z}}(M \otimes N, M' \otimes N')$$

Le corresponde por tanto una aplicación $\mathbb{Z}$-lineal que llamaremos canónica:

$$\mathrm{Hom}_R(M, M') \otimes_{\mathbb{Z}} \mathrm{Hom}_R(N, N') \to \mathrm{Hom}_{\mathbb{Z}}(M \otimes N, M' \otimes N') \tag{2.25}$$

que asocia a cada elemento $u \otimes v$ del producto tensorial la aplicación canónica $u \otimes v : M \otimes N \to M' \otimes N'$. Esta aplicación canónica no es necesariamente inyectiva ni suprayectiva, por lo que la notación $u \otimes v$ en ciertos casos puede llevar a confusión y será necesario indicar si denota un elemento del producto tensorial o una aplicación lineal.

Finalmente, sea M'' un R-módulo a derecha y N'' un R-módulo a izquierda y $u' : M' \to M''$ y $v' : N' \to N''$ aplicaciones R-lineales. Entonces es inmediato obtener que

$$(u' \circ u) \otimes (v' \circ v) = (u' \otimes v') \circ (u \otimes v) \tag{2.26}$$

3. Módulos

Como vimos con anterioridad, es sobre la teoría de módulos sobre la que se construye la teoría de representaciones, y es por ello que partiendo del estudio fundamental de módulos obtendremos resultados generales que podremos aplicar al estudio de las álgebras.

En particular, estudiaremos las estructuras de módulos simples y semisimples, ya que nos llevarán al concepto de álgebra semisimple y finalmente al radical, que estudiaremos con más detalle en una sección posterior.

A partir de este punto, A denotará una R-álgebra no trivial. El anillo R sobre el que la construyamos no será especialmente relevante ya que los resultados serán generales en lo que se refiere a álgebras, por lo que hablaremos simplemente de «álgebras» refiriéndonos a álgebras sobre un cierto anillo.

Por otra parte, dado que no exigimos que A sea conmutativa no existe una identificación natural entre A-módulos a derecha e izquierda. No obstante, las teorías de módulos a izquierda y derecha son idénticas, por lo que salvo que se indique otra cosa tomaremos simplemente A-módulos a derecha y los resultados serán completamente extrapolables a A-módulos a izquierda.

3.1. Cambio de escalares

Cualquier álgebra A es en particular un A-módulo a derecha y a izquierda con la operación escalar definida por el producto interno del álgebra. Usare-

mos por tanto la notación A_A y ${}_AA$ para indicar A como A-módulo a derecha e izquierda respectivamente.

En estas condiciones, los submódulos de A_A son precisamente los ideales a derecha de A. Por tanto, todos los conceptos y resultados para submódulos de A pueden aplicarse de forma directa a sus ideales a derecha e izquierda.

Para el estudio de la teoría de submódulos necesitaremos hacer uso de algunos conceptos básicos de teoría de categoría, aunque en la medida de lo posible intentaremos prescindir de ellos para buscar un enfoque más clásico.

Una técnica útil en el estudio de las álgebras es la comparación de los módulos sobre A con los módulos sobre un álgebra relacionada, B. El concepto subyacente a esta comparación será un funtor que relacione ambas categorías, aunque podremos expresar los resultados mediante técnicas elementales.

Sean A y B dos álgebras, y sea $\theta : A \to B$ un homomorfismo de álgebras. Sea M un B-módulo a derecha, definiremos las operaciones escalares en M por elementos de A como $ux = u\theta(x)$ con $u \in M, x \in A$. Trivialmente esta operación dota a M de una estructura de A-módulo a derecha. Denotaremos por M_A (o, de ser necesario, M_θ) a M con esta estructura escalar.

Esta aplicación de M en M_A constituye un funtor de la categoría de módulos de B en la de módulos de A. Existen dos casos particulares importantes que someteremos a estudio. El primero de ellos es el caso en que A es una subálgebra de B y θ es el homomorfismo de inclusión. En ese caso denominamos funtor de olvido al funtor asociado.

El segundo caso de estudio será en el que $B = A/I$ con I un ideal de A, y θ el homomorfismo de proyección. En este caso definimos la operación sobre M como

$$ux = u(x + I) \tag{3.1}$$

Enunciemos un resultado elemental que nos servirá más adelante

Lema 3.1. Sean A, B dos álgebras y $\theta : A \to B$ un homomorfismo de álgebras, y sean M y N dos B-módulos a derecha. Entonces

(I). $(M \otimes N)_A = M_A \otimes N_A$.

(II). Si $\phi \in \mathrm{Hom}_B(M, N)$, entonces $\phi \in \mathrm{Hom}_A(M_A, N_A)$. Si θ es un epimorfismo

entonces $\mathrm{Hom}_B(M,N) = \mathrm{Hom}_A(M_A, N_A)$.

(III). Si N es un submódulo de M, entonces N_A es un submódulo de M_A. Si θ es un epimorfismo entonces los conjuntos $S(M)$ y $S(M_A)$ de submódulos de M y M_A coinciden.

La demostración del lema es elemental. Si $\theta : A \to B$ es un epimorfismo de álgebras, definiremos una caracterización de los A módulos con la forma M_A con M un B-módulo.

Definición 3.2. Sea M un A-módulo a derecha y X un subconjunto de M. Definimos el anulador de X en A, $\mathrm{ann}X$, como

$$\mathrm{ann}X = \{x \in A : ux = 0 \quad \forall u \in X\} \tag{3.2}$$

La definición del anulador para A-módulos a izquierda es análoga.

Enunciaremos algunos resultados simples e importantes de anuladores que serán útiles posteriormente.

Lema 3.3. Sean M, M' y $\{M_i : i \in J\}$ A-módulos a derecha, $X \subseteq M$ y $Y \subseteq M$. Entonces,

(I). $\mathrm{ann}X$ es un ideal a derecha de A. Si X es un submódulo de M, entonces $X \lhd A$.

(II). Si $X \subseteq Y$, entonces $\mathrm{ann}X \supseteq \mathrm{ann}Y$.

(III). Si $M \cong M'$, entonces $\mathrm{ann}M = \mathrm{ann}M'$.

(IV). Si $M = \sum_{i\in J} M_i$, entonces $\mathrm{ann}M = \bigcap_{i\in J} \mathrm{ann}M_i$.

(V). Si M es un ideal a derecha de A, entonces $\mathrm{ann}(A/M)$ es el mayor ideal K de A que cumple $K \subseteq M$.

Las cuatro primeras propiedades son inmediatas por la definición de anulador. Para la última, basta observar que por la primera propiedad, $\mathrm{ann}(A/M)$ es un ideal de A, que es claramente un subconjunto de M. Por otra parte, si $K \lhd A$ y $K \subseteq M$, entonces $(x+M)K \subseteq M$ para todo $x \in A$, de forma que $K \subseteq \mathrm{ann}(A/M)$.

Proposición 3.4. Sean A y B dos R-álgebras, y $\theta : A \to B$ un epimorfismo. Si N es un A-módulo a derecha entonces existe un B-módulo a derecha M tal que $N = M_A$ si y solo si $\mathrm{Ker}\theta \subseteq \mathrm{ann}N$.

Demostración. Claramente $\mathrm{Ker}\theta \subseteq \mathrm{ann}M_A$. Análogamente, si $\mathrm{Ker}\theta \subseteq \mathrm{ann}N$ entonces la ecuación $u\theta(x) = ux$ define una operación escalar válida en N por los elementos de $\mathrm{Im}\theta = B$. Con esta operación, N se convierte en un B-módulo M, y $N = M_A$ por definición.

Esta proposición adquiere gran importancia cuando $B = A/I$ con I un ideal de A. En ese caso, un A-módulo N proviene de un A/I-módulo si y solo si $I \subseteq \mathrm{ann}N$. De esta forma, no haremos distinción entre los A/I-módulos y los A-módulos tales que $I \subseteq \mathrm{ann}N$.

Diremos que un A-módulo M es fiel si $\mathrm{ann}M = 0$.

Corolario 3.5. Si I es un ideal del álgebra A, y N es un A/I-módulo a derecha, entonces N es fiel como A/I-módulo si y solo si $\mathrm{ann}N_A = I$.

Demostración. Claramente, $\mathrm{ann}N_{A/I} = (\mathrm{ann}N_A)/I$.

3.2. El retículo de submódulos

Dado cualquier A-módulo M, la colección $S(M)$ de todos los submódulos de M está dotada de un orden parcial por la relación de inclusión. Además, si $\{N_i : i \in J\}$ es un conjunto de submódulos de M, entonces $\bigcap_{i\in J} N_i$ es un submódulo de M (si $J = \emptyset$ tomamos la intersección como M). Claramente, la intersección es el mayor submódulo de M incluido en todos los N_i, esto es, $\bigcap_{i\in J} N_i$ es la mayor cota inferior de $\{N_i : i \in J\}$ con respecto a la relación de orden de inclusión.

El conjunto $\{N_i : i \in J\}$ tiene también una menor cota superior entre los submódulos de M. En general esta cota no es la unión de los conjuntos sino el submódulo generado por la unión, $\sum_{i\in J} N_i = \{\sum_{k=1}^{m} u_k : u_k \in N_{i_k}\}$. En particular, la menor cota superior de dos submódulos N y P de M es $N + P = \{u + v : u \in N, v \in P\}$.

Un conjunto parcialmente ordenado en el que todos los subconjuntos tienen una cota inferior máxima y una cota superior mínima se denomina retícu-

lo completo. Trabajaremos por tanto sobre el hecho de que $S(M)$ es un retículo completo.

Se pueden ver muchas propiedades fundamentales de módulos como hechos sobre retículos de módulos. Veremos algunas propiedades teóricas de retículos que se cumplen en todos los retículos de la forma $S(M)$. El siguiente resultado es el más importante de ellos.

Teorema 3.6. Ley modular. Sean N, P y Q submódulos de M tales que $N \subseteq Q$. Entonces $N + (P \cap Q) = (N + P) \cap Q$.

Demostración. Trivialmente, $N + (P \cap Q) \subseteq N + P$, y $N + (P \cap Q) \subseteq Q$ por la hipótesis de que $N \subseteq Q$. Así, $N + (P \cap Q) \subseteq (N + P) \cap Q$. Por otra parte, si $u \in (N + P) \cap Q$, entonces $u = v + w$ con $v \in N$ y $w \in P$. Así, $w = u - v \in P \cap (Q + N) = P \cap Q$, y $u = v + w \in N + (P \cap Q)$.

La ley modular (también llamada modularidad) es una condición bastante débil sobre un retículo. Algunos de los retículos de submódulos que estudiaremos tienen la propiedad mucho más fuerte de la distributividad.

Lema 3.7. Sea M un A-módulo. Las siguientes identidades (i.e., ecuaciones válidas para cualquier N, P y Q) son equivalentes para $S(M)$:

(I). $N \cap (P + Q) = (N \cap P) + (N \cap Q)$.

(II). $N + (P \cap Q) = (N + P) \cap (N + Q)$.

(III). $(N \cap P) + (P \cap Q) + (Q \cap N) = (N + P) \cap (P + Q) \cap (Q + N)$.

La demostración es directa sin más que aplicar repetidamente las identidades y aplicar la ley modular.

Proposición 3.8. Sea M un A-módulo tal que $S(M)$ es no distributivo. Entonces existen submódulos distintos P y Q de M tales que $P/(P \cap Q) \cong Q/(P \cap Q)$ como A-módulos.

Demostración. Dado que $S(M)$ es no distributivo, existen submódulos M_0, M_1, M_2, M_3 y M_4 de M tales que

$$M_0 = (M_1 \cap M_2) + (M_2 \cap M_3) + (M_3 \cap M_1) \subset (M_1 + M_2) \cap (M_2 + M_3) \cap (M_3 + M_1) = M_4 \tag{3.3}$$

Definimos

$$N = (M_1 \cap M_2) + (M_3 \cap (M_1 + M_2)), \tag{3.4}$$

$$P = (M_2 \cap M_3) + (M_1 \cap (M_2 + M_3)), \tag{3.5}$$

$$Q = (M_1 \cap M_3) + (M_2 \cap (M_1 + M_3)). \tag{3.6}$$

Aplicando la ley modular, tenemos que

$$P \cap Q = M_0 \tag{3.7}$$

y

$$P + Q = M_4 \tag{3.8}$$

En particular, $P \neq Q$ ya que $M_0 \subset M_4$. Además, es fácil obtener que $N \cap P = N \cap Q = M_0$, y $N + P = N + Q = M_4$. Por el isomorfismo de Noether, $P/(P \cap Q) = P/(P \cap N) \cong (P + N)/N = M_4/N$. Análogamente, $Q/(P \cap Q) \cong M_4/N$. Así, $P/(P \cap Q) \cong Q/(P \cap Q)$.

Dada una R-álgebra A, denotamos por $I(A)$ el conjunto de los ideales de A. Es sabido que los A-bimódulos se pueden ver como módulos a derecha sobre el álgebra envolvente A^e de A,y los subbimódulos de A son los ideales biláteros.

Es por tanto consecuencia inmediata que $I(A)$ es un retículo completo y modular. Además, si $I(A)$ no es distributivo, existen ideales distintos I y J en A tales que $I/(I \cap J) \cong J/(I \cap J)$ como A-bimódulos. La demostración es completamente análoga a la realizada para $S(A)$.

3.3. Módulos simples

Definición 3.9. Un módulo a derecha o izquierda N es simple si no es el módulo cero y los únicos submódulos de N son 0 y N. Un módulo M es semisimple si M es suma directa de módulos simples

Una denominación alternativa habitual en teoría de anillos es la de módulo irreducible para módulo simple y módulo completamente reducible para módulo semisimple. Usaremos sin embargo el convenio dado en la definición.

Trivialmente, un ideal a derecha M de un álgebra A es un A-módulo simple si y solo si M es un ideal minimal a derecha, esto es, M es minimal en el conjunto de ideales a derecha no nulos de A. Por supuesto, A no tiene por qué tener ideales minimales a derecha. No existe ninguno en el anillo $\mathbb{Z}$ de enteros, por ejemplo.

Por otra parte, la hipótesis de que A posea un elemento unidad distinto de cero implica, utilizando el lema de Zorn, que A incluye al menos un ideal maximal a derecha, esto es, un ideal que es maximal en el conjunto de ideales a derecha propios de A. Además, si M es un ideal maximal a derecha de A, entonces por el teorema de correspondencia, A_A/M es un módulo simple. Análogamente, si A_A/M es simple, entonces M es un ideal maximal a derecha.

Proposición 3.10. Para un A-módulo a derecha no nulo N, las siguientes condiciones son equivalentes:

(I). N es simple.

(II). $uA = N$ para todo $u \in N$ distinto de cero.

(III). $N \cong A_A/M$ para algún ideal maximal a derecha M de A.

Demostración. (I) implica claramente (II), ya que $0 \neq u \in uA < N$ implica que $uA = N$ por la simplicidad de N. Análogamente, dado que $N \neq 0$, (II) implica que N es el único submódulo distinto de cero de N, esto es, que N es simple. Como se afirmó más arriba, el que (III) implique (I) es consecuencia del teorema de correspondencia.

Para probar que (II) implica (III), sea u un elemento distinto de cero de N. Por (II), la aplicación $x \mapsto ux$ es un epimorfismo de módulos de A_A en N cuyo núcleo M es un ideal a derecha de A. Dado que (II) implica (I), se sigue que $A_A/M \cong N$ es simple. Por tanto, M es un ideal maximal a derecha de A.

Proposición 3.11. Lema de Schur. Sean M y N A-módulos a derecha, y sea $\phi : M \to N$ un homomorfismo no nulo. Entonces

(I). Si M es simple, entonces ϕ es inyectiva.

(II). Si N es simple, entonces ϕ es suprayectiva.

Demostración. Como $\phi \neq 0$, se sigue que $\mathrm{Ker}\phi \neq M$ y que $\mathrm{Im}\phi \neq 0$. Así, M simple implica que $\mathrm{Ker}\phi = 0$, y N simple implica $\mathrm{Im}\phi = N$.

Corolario 3.12. Si M y N son A-módulos a derecha simples, entonces o bien $M \cong N$ o bien $\mathrm{Hom}_A(M,N) = 0$.

El corolario es consecuencia inmediata del lema de Schur, ya que cualquier homomorfismo no nulo sería un isomorfismo.

Un A-módulo a derecha N es indescomponible si $N \neq 0$, y N no puede escribirse como suma directa de submódulos no nulos. Esto es, si $N = P \otimes Q$ entonces $P = 0$ o $Q = 0$. Los módulos indescomponibles tienen gran importancia en la teoría de álgebras.

Corolario 3.13. Dado un módulo semisimple N, las siguientes condiciones son equivalentes:

(I). N es simple.

(II). $E_A(N)$ es un álgebra de división.

(III). N es indescomponible.

Demostración. Si N es simple, entonces todo endomorfismo no nulo de N tiene inversa por el lema de Schur, por lo que $E_A(N)$ es un álgebra de división. Si $E_A(N)$ es un álgebra de división, entonces $\mathrm{id}_N \neq 0$, por lo que $N \neq 0$. Además, para cualquier descomposición en suma directa $N = P \otimes Q$, existe un elemento $\pi \in E_A(N)$ tal que $\pi(N) = P$, $(1-\pi)(N) = Q$ y $\pi^2 = \pi$; así, π es la proyección de N en P asociada con la descomposición. Por tanto, $\pi(\mathrm{id}_N - \pi) = 0$. La hipótesis de que $E_A(N)$ sea un álgebra de división implica que $\pi = 0$ o $\mathrm{id}_N - \pi = 0$. En esos casos, respectivamente, $P = 0$ o $Q = 0$. Finalmente, las hipótesis de N indescomponible y semisimple solo son compatibles si N es simple.

En adelante nos referiremos al propio lema y a sus dos corolarios como «lema de Schur» siempre y cuando no cause confusión.

3.4. Módulos semisimples

Si N y P son submódulos de un A-módulo M, llamamos a P un complemento de N en $S(M)$ si $N+P=M$ y $N\cap P=0$. Dicho de otra forma, M es la suma directa interna de N y P. Claramente, esta relación es simétrica. En general, los complementos no son únicos ni tienen por qué existir. De hecho, probaremos que la existencia universal de complementos caracteriza a los módulos semisimples.

Lema 3.14. Sea M un módulo tal que $M=\sum_{i\in J}N_i$, con los N_i submódulos simples de M. Si $P\in S(M)$, entonces existe un subconjunto I de J tal que $M=\left(\bigoplus_{i\in I}N_i\right)\oplus P$.

Demostración. Por el lema de Zorn, existe un subconjunto I de J tal que la colección $\{N_i : i\in I\}$ es maximal respecto a la independencia: $\left(\sum_{i\in I}N_i\right)+P=\left(\bigoplus_{i\in I}N_i\right)\oplus P$. Sea $M_1=\left(\sum_{i\in I}N_i\right)+P$. La maximalidad de I implica que $M_1\cap N_j\neq 0$ para todo $j\in J$. Por tanto, dado que cada N_j es simple, $N_j\subseteq M_1$ para todo $j\in J$. Así, $M=\sum_{j\in J}N_j\subseteq M_1\subseteq M$, y por tanto $M=\left(\bigoplus_{i\in I}N_i\right)\oplus P$.

Proposición 3.15. Dado un A-módulo a derecha M, las siguientes condiciones son equivalentes:

(I). M es semisimple.

(II). $M=\sum\{N\in S(M) : N \text{ es simple}\}$.

(III). $S(M)$ es un retículo complementado, esto es, todo submódulo de M tiene un complemento en $S(M)$.

(IV). Si $P\in S(M)$, entonces $S(P)$ es un retículo complementado.

Demostración. Es claro que (I) implica (II) sin más que utilizar la definición de módulo semisimple. Además, utilizando el lema anterior es inmediato que (II) implica (III), y además que (II) implica (I) tomando $P=0$.

Si tomamos ahora $M_1\in S(P)$, utilizando (III) tenemos que existe $M_2\in S(M)$ tal que $M=M_1\oplus M_2$. Por tanto, $P=P\cap(M_1\oplus M_2)=M_1\oplus(P\cap M_2)$ con $P\cap M_2\in S(P)$, con lo que probamos (IV).

Finalmente, deducimos de (IV) que si Q es un submódulo propio de M, entonces existe un submódulo simple N de M tal que $N \cap Q = 0$. Esto implica (II) y por tanto queda probada la proposición.

Podemos observar en la demostración que, aplicando el lema de Zorn y tomando $0 \neq u \in M - Q$, podemos suponer que Q es maximal con la propiedad $u \notin Q$. Aplicando (IV) con $P = M$ obtenemos un $N \in S(M)$ tal que $M = Q \oplus N$. Así, podemos escribir $u = w + v$ con $w \in Q$, $v \in N$. Dado que $u \notin Q$, se sigue que $v \neq 0$. En particular, $N \neq 0$. Si N_1 es un submódulo no nulo de N, entonces la maximalidad de Q implica que $w + v = u \in Q + N_1 = Q \oplus N_1$. Por tanto, $v \in N_1$. En particular, dos submódulos no nulos de N tienen intersección no vacía. Por otro lado, $S(N)$ es complementado por (IV). La única manera de no caer en contradicción es que $S(N) = \{0, N\}$, y por tanto N es simple.

Corolario 3.16. Si M es semisimple y $P < M$, entonces P y M/P son semisimples.

Demostración. Por (III) de la proposición, $M \cong P \oplus M/P$. Por tanto, utilizando nuevamente la proposición P y M/P son semisimples.

Corolario 3.17. La suma directa de módulos semisimples es semisimple.

La demostración de este corolario es inmediata de la definición de módulos semisimples.

Finalmente, nos interesará saber cuándo $S(M)$ es un retículo distributivo, para lo cual tenemos el siguiente corolario:

Corolario 3.18. Sea M un A-módulo a derecha semisimple. Suponemos que $M = \bigoplus_{i \in J} N_i$ con cada N_i simple. Entonces $S(M)$ es un retículo distributivo si y solo si $N_i \ncong N_j$ para todo $i \neq j$ en J.

Demostración. Si N es un A-módulo a derecha no nulo y $Q = N \oplus N$, entonces $S(Q)$ no es distributivo. De hecho, si $N_1 = \{(u, 0) \in Q : u \in N\}$, $N_2 = \{(0, u) \in Q : u \in N\}$ y $N_3 = \{(u, u) \in Q : u \in N\}$, entonces $N_1 + N_2 = Q$, $N_3 \cap N_1 = N_3 \cap N_2 = 0$, y $N_3 \cong N \neq 0$. Así, $N_3 \cap (N_1 + N_2) = N_3 \supset 0 = (N_3 \cap N_1) + (N_3 \cap N_2)$. En el contexto del corolario, esta observación muestra que si $S(M)$ es distributivo, entonces $N_i \ncong N_j$ para todo $i \neq j$.

Para probar la otra implicación, definimos $N(I) = \sum_{j\in I} N_j$ para cada subconjunto I de J. Dado que la suma $M = \bigoplus_{i\in J} N_i$ es directa, es claro que $N(I_1 \cup I_2) = N(I_1) \cap N(I_2)$ para cualesquiera dos subconjuntos I_1 e I_2 de J. Así, $\{N(I) : I \subseteq J\}$ es un subretículo distributivo de $S(M)$. Por tanto, solo nos queda probar que $S(M) = \{N(I) : I \subseteq J\}$. Dado $P < M$, definimos $I = \{i \in J : P \cap N_i \neq 0\}$. Probemos que $P = N(I)$. Como los N_i son simples, $P \cap N_i \neq 0$ implica que $N_i = P \cap N_i \subseteq P$. Así, $N(I) \subseteq P$. Bastará probar que $P \cap N(J-I) = 0$, ya que por la ley modular tendríamos que $P = P \cap (N(J-I) + N(I)) = P \cap N(J-I) + N(I) = N(I)$. Suponemos $P \cap N(J-I) \neq 0$ y tomamos un conjunto $K \subseteq J - I$ de la menor cardinalidad tal que $P \cap N(K) \neq 0$. Claramente, K es finito, y $|K| \geq 2$ ya que $P \cap N_i = 0$ para todo $i \in J - I$. Dado $i \in K$, tomamos $\pi_i : N(K) \to N_i$ el homomorfismo de proyección asociado a la descomposición directa $N(K) = \bigoplus_{j\in K} N_j$. Como $\mathrm{Ker}(\pi_i|_{P\cap N(K)}) \subseteq P \cap N(K - \{i\})$, la minimalidad de $|K|$ implica que $\mathrm{Ker}(\pi_i|_{P\cap N(K)}) = 0$. Por tanto, dado que los N_i son simples y $P \cap N(K) \neq 0$, se sigue que π_i es un isomorfismo de $P \cap N(K)$ en N_i. El hecho de que $|K| > 1$ nos lleva a contradicción con la hipótesis $N_i \ncong N_j$ para todo $i \neq j$ en J.

3.5. Estructura de módulos semisimples

Por definición, un A-módulo a derecha semisimple tiene una estructura «buena», es una suma directa de módulos simples. Estudiaremos ahora la unicidad de estas representaciones en suma directa. Para ello, necesitaremos obtener ciertos resultados previos.

Lema 3.19. Sea $M = \bigoplus_{i\in J} N_i$ con los N_i A-módulos a derecha simples. Supongamos que N es un A-módulo a derecha simple para el que existe un homomorfismo no nulo $\phi : N \to M$. Entonces, existe $j \in J$ tal que $M = \phi(N) \oplus (\bigoplus_{i\neq j} N_i)$ y $N \cong N_j$.

Demostración. Por el lema 3.14, existe $J' \subseteq J$ tal que $M = \phi(N) \oplus (\bigoplus_{i\in J'} N_i)$. Por tanto, $\bigoplus_{i\in J-J'} N_i \cong M/(\bigoplus_{i\in J'} N_i) \cong \phi(N) \cong N$ (usando el lema de Schur y la hipótesis $\phi \neq 0$). Así, $|J - J'| = 1$, con lo que el lema queda demostrado.

En adelante, consideraremos $\{N_i : i \in J\}$ un conjunto de representantes de las clases de isomorfismos de A-módulos a derecha simples. Así, J es un con-

junto índice no vacío, los N_i son A-módulos a derecha simples y todo A-módulo a derecha simple es isomorfo a un único N_i.

Además, dado un A-módulo a derecha M, denotaremos $M(i)$ el submódulo $\sum\{N < M : N \cong N_i\}$.

Lema 3.20. Si M es un A-módulo a derecha semisimple, entonces $M = \bigoplus_{i\in J} M(i)$.

Demostración. Como M es semisimple, $M = \bigoplus_{i\in J} M_i$, donde $M_i = \bigoplus_{j\in K} N_{ij}$, con $N_{ij} \cong N_i$. Es claro que $M_i \subseteq M(i)$. Bastará probar que $M(i) \subseteq M_i$. Sea $N_i \cong N < M$. Expresamos $M = M_i \oplus M_i'$, $M_i' = \bigoplus_{j\neq i} M_j$, y sea $\pi : M \to M_i'$ la proyección asociada a esta descomposición. Se sigue que $\pi(N) = 0$, esto es, $N \subseteq M_i$. Como N es un submódulo cualquiera de M isomorfo a N_i, queda probado que $M(i) \subseteq M_i$.

Lema 3.21. Sean M y M' A-módulos a derecha semisimples. Si $\phi : M \to M'$ es un homomorfismo, entonces $\phi(M(i)) \subseteq M'(i)$ para todo $i \in J$.

Demostración. Si $N_i \cong N < M$, entonces utilizando el lema de Schur o $\phi(N) = 0$ o $\phi(N) \cong N_i$. En ambos casos, $\phi(N) \subseteq M'(i)$. Se sigue que $\phi(M(i)) \subseteq M'(i)$.

Proposición 3.22. Sean M y M' A-módulos a derecha semisimples. Supongamos que $M = \bigoplus_{i\in J} M(i)$ con $M(i) \cong \bigoplus \alpha_i N_i$ y $M' = \bigoplus_{i\in J} M'(i)$ con $M'(i) \cong \bigoplus \beta_i N_i$. Entonces M es isomorfo a M' si y solo si los números cardinales α_i y β_i son iguales para todo $i \in J$.

Demostración. Supongamos que $\phi : M \to M'$ es un isomorfismo. Por el lema 3.21, $\phi(M(i)) = M'(i)$ para todo i. Fijamos $i \in J$. Para probar que $\alpha_i = \beta_i$, consideraremos primero el caso α_i finito y usaremos inducción. Si $\alpha_i = 0$, entonces $M'(i) = \phi(M(i)) = \phi(0) = 0$, luego $\beta_i = 0$. Supongamos $\alpha_i = m \geq 1$. Tenemos $M(i) = N_{i1} \oplus ... \oplus N_{i\,m-1} \oplus N_{im}$, $M'(i) = \bigoplus_{k\in I} N'_{ik}$ con $N_{ij} \cong N'_{ik} \cong N_i$ para todo j y k, y $|I| = \beta_i$. Por el lema 3.19, existe $l \in I$ tal que $\phi(N_{im}) \oplus (\bigoplus_{k\neq l} N'_{ik}) = M'(i) = \phi(N_{im}) = \phi(N_{im}) \oplus \phi(N_{i1} \oplus ... \oplus N_{i\,m-1})$. En consecuencia, $N_{i1} \oplus ... \oplus N_{i\,m-1} \cong \phi(N_{i1} \oplus ... \oplus N_{i\,m-1}) \cong M'(i)/\phi(N_{im}) \cong \bigoplus_{k\neq l} N'_{ik}$. Por la hipótesis de inducción, $m-l = |I-\{l\}|$, de forma que $\alpha_i = m = |I| = \beta_i$. Esto completa la inducción. Si β_i es finito, podemos utilizar la misma demostración utilizando ϕ^{-1}. Por tanto, supongamos ahora que α_i y β_i son ambos infinitos. Por la proposición 3.10 tenemos que existen descomposiciones $M(i) = \bigoplus_{k\in K} u_k A$, $M'(i) = \bigoplus_{l\in L} u'_l A$, con $|K| = \alpha_i$ y $|L| = \beta_i$. El isomorfismo ϕ induce una aplicación λ

de K en el conjunto de subconjuntos finitos de L tal que $\phi(u_k) \in \sum_{l\in\lambda(k)} u'_l A$, y $\bigcap_{k\in K} \lambda(k) = L$ ya que ϕ es suprayectiva. Por tanto, como L y K son infinitos, $\beta_i = |L| \leq \sum_{k\in K} |\lambda(k)| \leq \aleph_0 \cdot |K| = \alpha_i$. Por simetría, $\alpha_i \leq \beta_i$. Esto completa la demostración de que $M \cong M'$ implica $\alpha_i = \beta_i$ para todo $i \in J$. La otra implicación es inmediata.

3.6. Condiciones de cadena

La mayoría de módulos semisimples que utilizaremos serán sumas directas finitas de módulos simples. Es por ello que en este apartado estudiaremos diferentes condiciones de finitud para los módulos semisimples.

Decimos que un A-módulo M es artiniano (resp. noetheriano) si $S(M)$ satisface la condición de cadena descendiente (resp. ascendente). Esto es, no existen sucesiones infinitas y estrictamente decrecientes (resp. crecientes) de submódulos de M. De forma equivalente, M es artiniano (resp. noetheriano) si todo subconjunto no vacío de $S(M)$ incluye un elemento minimal (resp. maximal).

En general las propiedades artiniana y noetheriana son independientes entre sí. Por ejemplo, $\mathbb{Z}_{\mathbb{Z}}$ es noetheriano pero no artiniano, mientras que el $\mathbb{Z}$-módulo $\mathbb{Z}(p^\infty) = \{a/p^n : a \in \mathbb{Z}, n \in \mathbb{N}\}/\mathbb{Z}$ es artiniano pero no noetheriano. Sin embargo, veremos que en el caso de módulos semisimples son condiciones equivalentes.

Lema 3.23. Sean M, M'' y N submódulos del A-módulo M, con $M' \subseteq M''$. Entonces existe una sucesión exacta

$$0 \to \frac{M'' \cap N}{M' \cap N} \to \frac{M''}{M'} \to \frac{M'' + N}{M' + N} \to 0 \tag{3.9}$$

Demostración. Usando los teoremas de isomorfía de Noether y la ley modular tenemos que

$$\begin{aligned} \frac{M'' + N}{M' + N} &= \frac{M'' + (M' + N)}{M' + N} \cong \frac{M''}{M'' \cap (M' + N)} \\ &= \frac{M''}{M' + (M'' \cap N)} \cong \frac{(M''/M')}{(M' + (M'' \cap N))/M'} \end{aligned} \tag{3.10}$$

y $(M' + (M'' \cap N))/M' \cong (M'' \cap N)/M' \cap (M'' \cap N) = (M'' \cap N)/(M' \cap N)$.

Lema 3.24. Sea $0 \to N \to M \to P \to 0$ una sucesión exacta de A-módulos. El módulo M es artiniano (resp. noetheriano) si y solo si tanto N como P son artinianos (resp. noetherianos).

Demostración. Sin pérdida de generalidad, podemos suponer que $N \in S(M)$ y $P = M/N$. En este caso, $S(N)$ es un subretículo de $S(M)$, y por el teorema de correspondencia $S(P)$ es isomorfo a un subretículo de $S(M)$. Por tanto, si M es artiniano (noetheriano), también lo son N y P. Análogamente, si $M_0 \supset M_1 \supset M_2 \supset ...$ es una cadena descendiente infinita en $S(M)$, entonces tenemos $M_0 \cap N \supseteq M_1 \cap N \supseteq M_2 \cap N \supseteq ...$ en $S(N)$, y $(M_0 + N)/N \supseteq (M_1 + N)/N \supseteq (M_2 + N)/N \supseteq ...$ en $S(P)$, y por el lema 3.23, al menos una de estas cadenas es infinita. Así, si N y P son artinianos, también lo es M. La demostración para el caso noetheriano es análoga.

Lema 3.25. Supongamos que el A-módulo M es artiniano y noetheriano. Entonces existe una sucesión $0 = M_0 \subset M_1 \subset ... \subset M_{n-1} \subset M_n = M$ tal que todos los módulos cociente M_{i+1}/M_i, $i < n$, son simples.

Demostración. Si $M = 0$, entonces $0 = M_0 = M$. Supongamos $M \neq 0$. Usando la hipótesis de que M es artiniano, es posible construir (por inducción) una sucesión creciente $0 = M_0 \subset M_1 \subset M_2 \subset ...$ de submódulos de M tales que los factores M_{i+1}/M_i son simples. De hecho, si tenemos M_0, M_1, ..., M_i, y si $M_i \neq M$, entonces existe un submódulo M_{i+1} de M que contiene a M_i tal que M_{i+1}/M_i es un submódulo minimal no vacío de M/M_i, ya que M/M_i es artiniano por el lema 3.24. Como M es noetheriano, este proceso inductivo ha de terminar en un número finito de pasos, esto es, para algún $n < \infty$ tendremos $M_n = M$.

Se dice que una cadena $0 = M_0 \subset M_1 \subset ... \subset M_{n-1} \subset M_n = M$ de submódulos de M es una serie de composición de M si M_{i+1}/M_i es simple para todo $i < n$. Los módulos cociente M_{i+1}/M_i se llaman factores de composición de la serie, y son únicos

Teorema 3.26. Teorema de Jordan-Hölder. Si $0 = M_0 \subset M_1 \subset ... \subset M_{n-1} \subset M_n = M$ y $0 = M'_0 \subset M'_1 \subset ...M'_{k-1} \subset M'_k = M$ son series de composición del módulo M, entonces $n = k$, y existe una permutación π de $\{0,1,2,...,n-1\}$ tal que $M'_{j+1}/M'_j \cong M_{\pi(j)+1}/M_{\pi(j)}$ para todo $j < n$.

Demostración. Lo demostraremos por inducción en n. Si $n = 0$, entonces $M = 0$ y $k = 0$. Supondremos $n > 0$. Consideramos la cadena de submódulos $0 = M'_0 \cap M_{n-1} \subseteq M'_1 \cap M_{n-1} \subseteq ... \subseteq M'_k \cap M_{n-1} = M_{n-1} = M'_0 + M_{n-1} \subseteq M'_1 + M_{n-1} \subseteq ... \subseteq M'_k + M_{n-1} = M_n$. Por el lema 3.23, dado $j < k$ existe una sucesión exacta

$$0 \to \frac{M'_{j+1} \cap M_{n-1}}{M'_j \cap M_{n-1}} \to \frac{M'_{j+1}}{M'_j} \to \frac{M'_{j+1} + M_{n-1}}{M'_j + M_{n-1}} \to 0 \tag{3.11}$$

Como M'_{j+1}/M'_j es simple, entonces exactamente uno de

$$\frac{M'_{j+1} \cap M_{n-1}}{M'_j \cap M_{n-1}}, \quad \frac{M'_{j+1} + M_{n-1}}{M'_j + M_{n-1}} \tag{3.12}$$

es isomorfo a M'_{j+1}/M'_j y el otro cociente es 0. Además, como M_n/M_{n-1} es simple, existe exactamente un $i < k$ tal que $M_{n-1} = M'_l + M_{n-1} \subset M'_{i+1} + M_{n-1} = M_n$. Así, $M_n/M_{n-1} \cong M'_{i+1}/M'_i$, y $0 = M'_0 \cap M_{n-1} \subset M'_1 \cap M_{n-1} \subset ... \subset M'_{i-1} \cap M_{n-1} \subset M'_i \cap M_{n-1} = M'_{i+1} \cap M_{n-1} \subset ... \subset M'_k \cap M_{n-1} = M_{n-1}$ es una serie de composición de M_{n-1}. Por la hipótesis de inducción, $k-1 = n-1$, y existe una biyección $\pi : \{0, 1, ..., i-1, i+1, ..., k-1\} \to \{0, 1, ..., n-2\}$ tal que $M'_{j+1}/M'_j \cong M_{\pi(j)+1}/M_{\pi(j)}$ para todo $j \neq i$. Basta definir $\pi(i) = n-1$ para completar la demostración.

Si un módulo M se puede escribir como suma directa finita de módulos simples de dos formas, por ejemplo, $M = N_1 \oplus ... \oplus N_n$ y $M = N'_1 \oplus ... \oplus N'_k$, el teorema de Jordan-Hölder se puede aplicar a las series de composición $0 \subset N_1 \subset N_1 + N_2 \subset ... \subset N_1 + N_2 + ... + N_n = M$ y $0 \subset N'_1 \subset N'_1 + N'_2 \subset ... \subset N'_1 + N'_2 + ... + N'_k = M$ para obtener que $n = k$ y $N'_j \cong N_{\pi(j)}$ para alguna permutación π. En otras palabras, el teorema de Jordan-Hölder nos permite probar trivialmente el teorema 3.22 en el caso de que la suma directa sea finita.

Definición 3.27. Sea M un A-módulo a derecha artiniano y noetheriano. Por el lema 3.25, M tiene una serie de composición, y la longitud de la serie es única por el teorema de Jordan-Hölder. El número de factores de composición en la serie de composición de M se denomina longitud de composición de M, y lo denotaremos $l(M)$. Es claro que $l(M) = 0$ si y solo si $M = 0$ y $l(M) = 1$ si y solo si M es simple.

Corolario 3.28. Sean M, N y P módulos artinianos y noetherianos. Si $0 \to N \to M \to P \to 0$ es una sucesión exacta de homomorfismos de módulos, entonces $l(M) = l(N) + l(P)$

Demostración. Sin pérdida de generalidad, suponemos que N es un submódulo de M y $P = M/N$. Si $0 = N_0 \subset N_1 \subset ... \subset N_r = N$ es una serie de composición de N, y $0 = Q_0/N \subset Q_1/N \subset ... \subset Q_s/N = P$ es una serie de composición de P, entonces $0 = N_0 \subset N_1 \subset ... \subset N_r \subset Q_1 \subset ... \subset Q_s = M$ es una serie de composición de M. Así, $l(M) = r + s = l(N) + l(P)$.

Proposición 3.29. Dado un A-módulo a derecha semisimple M, las siguientes condiciones son equivalentes

(I). M es finitamente generado como A-módulo.

(II). $M = N_1 \oplus N_2 \oplus ... \oplus N_m$ con los N_j simples y $0 \leq m \leq \infty$.

(III). M es artiniano.

(IV). M es noetheriano.

(V). Existe $m < \infty$ tal que si $M_0 \subset M_1 \subset ... \subset M_k$ es una sucesión finita estrictamente creciente de submódulos de M, entonces $k \leq m$.

Demostración. Las condiciones (I) y (II) son claramente equivalentes. De hecho, (II) implica (I) por la proposición 3.10, y (II) es consecuencia de (I), (III) y (IV) ya que M es semisimple (es decir, suma directa de módulos simples), y una suma directa infinita no puede ser finitamente generada, artiniana ni noetheriana. Como los módulos simples son claramente artinianos y noetherianos, las condiciones (III) y (IV) son consecuencia inmediata utilizando el lema 3.24 e inducción sobre m. Claramente, (V) implica que M es artiniano y noetheriano. Análogamente, si M es artiniano y noetheriano, entonces una sucesión estrictamente creciente de submódulos de M incluye a lo sumo $l(M) + 1$ términos (por el corolario 3.28 y usando inducción).

Algunas de las implicaciones de la proposición son ciertas para módulos arbitrarios. En particular, la condición (V) es equivalente a la conjunción de (III)

y (IV). Además, todo A-módulo noetheriano M es finitamente generado; en caso contrario, el axioma de elección nos permitiría elegir una sucesión infinita u_1, u_2, ... de elementos de M tales que $u_1A \subset u_1A + u_2A \subset ...$, violando así la condición de cadena ascendente.

3.7. El radical de un módulo

Todo lo obtenido hasta ahora nos permite por fin definir el importante concepto de radical de un módulo, que tendrá gran importancia en la teoría de representación, y obtener varias propiedades suyas.

Definición 3.30. Sea M un A-módulo. El radical de M es $\mathrm{rad}M = \bigcap\{N \in S(M) : M/N \text{ es simple}\}$.

En general, puede darse el caso de que no exista ningún submódulo N de M tal que M/N sea simple. En tal caso $\mathrm{rad}M$ sería la intersección del subconjunto vacío de $S(M)$ que como ya definiéramos tomaremos por convenio como M.

Lema 3.31. Sea M un A-módulo. Entonces

(I). $\mathrm{rad}M$ es un submódulo de M.

(II). Si $N \in S(M)$, entonces $\mathrm{rad}M/N = 0$ implica $N \supseteq \mathrm{rad}M$.

(III). $\mathrm{rad}(M/\mathrm{rad}M) = 0$.

Todas estas observaciones son consecuencia inmediata del teorema de correspondencia.

Lema 3.32. Si M es un A-módulo semisimple, entonces $\mathrm{rad}M = 0$.

Demostración. Sea $M = \bigoplus_{i\in J} P_i$ con los P_i simples. Denotamos $N_j = \sum_{i\neq j} P_i \in S(M)$. Entonces $M/N_j \cong P_j$ es simple, luego $\mathrm{rad}M \subseteq \bigcap_{j\in J} N_j = 0$.

Proposición 3.33. Un A-módulo M es finitamente generado y semisimple si y solo si M es artiniano y $\mathrm{rad}M = 0$.

Demostración. Si M es finitamente generado y semisimple entonces M es artiniano por la proposición 3.29, y $\mathrm{rad}M = 0$ por el lema 3.32. Podemos suponer $M \neq 0$. Como $\mathrm{rad}M = 0$, existe un conjunto no vacío $\{N_i : i \in J\} \subseteq S(M)$

tal que M/N_i es simple para todo $i \in J$, y $\bigcap_{i\in J} N_i =$. La propiedad artiniana en M garantiza la existencia de un módulo $N_1 \cap ... \cap N_m$ minimal en la familia $\{N_{i_1} \cap ... N_{i_k} : i_1, ..., i_k \in J\}$. Necesariamente $N_1 \cap ... \cap N_m = 0$, ya que en otro caso $N_1 \cap N_m \nsubseteq N_i$ para algún $i \in J$, lo que lleva a contradicción $N_1 \cap ... \cap N_m \cap N_i \subset N_1 \cap ... \cap N_m$ con la minimalidad de $N_1 \cap ... \cap N_m$. Definimos $\phi : M \to (M/N_1) \oplus ... \oplus (M/N_m)$ como $\phi(u) = (u + N_1, ..., u + N_m)$. Claramente, ϕ es un homomorfismo de módulos con núcleo $N_1 \cap ... \cap N_m = 0$. Por tanto, M es isomorfo a un submódulo del módulo semisimple $M/N_1 \oplus ... \oplus M/N_m$, por lo que M es semisimple usando el corolario 3.16. Utilizando la proposición 3.29 también es finitamente generado.

3.8. Producto tensorial de módulos

Ahora que tenemos conceptos más avanzados de teoría de módulos podremos ampliar la introducción al producto tensorial que empezamos en el capítulo 2. No obstante, los resultados que obtendremos necesitarán únicamente cálculo en el formalismo tensorial, solo los colocamos en este punto para tener un mayor bagaje en el concepto de módulos.

Proposición 3.34. Sean M, M_1, M_2, N, N_1, N_2 y P R-módulos. Entonces

(I). $M \otimes (N_1 \oplus N_2) \cong (M \otimes N_1) \oplus (M \otimes N_2)$ por un isomorfismo que lleva $u \otimes (v_1, v_2)$ en $(u \otimes v_1, u \otimes v_2)$.

(II). $M \otimes (N \otimes P) \cong (M \otimes N) \otimes P$ por un isomorfismo que lleva $u \otimes (v \otimes w)$ en $(u \otimes v) \otimes w$.

(III). $M \otimes N \cong N \otimes M$ por un isomorfismo que lleva $u \otimes v$ en $v \otimes u$.

(IV). $M \otimes R \cong M$ y $R \otimes M \cong M$ por isomorfismos que llevan $u \otimes a$ y $a \otimes u$ en ua.

Las demostraciones son inmediatas sin más que usar las definiciones de producto tensorial, la condición de universalidad y los resultados de la sección 2.2.

Esto nos lleva a estar en situación de demostrar la propiedad fundamental de exactitud del producto tensorial.

Proposición 3.35. Si $M_1 \xrightarrow{\phi} M_2 \xrightarrow{\psi} M_3 \to 0$ es una sucesión exacta de R-módulos, entonces para todo R-módulo N la sucesión $M_1 \otimes N \xrightarrow{\chi} M_2 \otimes N \xrightarrow{\theta} M_3 \otimes N \to 0$ es exacta, donde $\chi = \phi \otimes \mathrm{id}_N$ y $\theta = \psi \otimes \mathrm{id}_N$.

Demostración. Claramente, Imθ incluye a todos los tensores de rango uno, de forma que θ es suprayectiva. Además, $\psi\phi = 0$ implica $\theta\chi = 0$, por lo que Im$\chi \subseteq$ Kerθ. Sea π la proyección natural de $M_2 \otimes N$ en $M_2 \otimes N/\mathrm{Im}\chi$. Como $\psi^{-1}(0) \otimes N = \mathrm{Im}\phi \otimes N \subseteq \mathrm{Im}\chi = \mathrm{Ker}\pi$, la fórmula $\Phi(u_3, v) = \pi(\psi^{-1}u_3 \otimes v)$ es una aplicación bilineal bien definida de $M_3 \times N$ en P. Así, existe un homomorfismo $\lambda : M_3 \otimes N \to P$ tal que $\lambda(u_3 \otimes v) = \pi(\psi^{-1}u_3 \otimes v)$. En particular, $\lambda(\psi(u_2) \otimes v) = \pi(u_2 \otimes v)$, de forma que $\lambda\theta = \pi$. Por tanto, Ker$\theta \subseteq$ Ker$\pi =$ Imχ.

Si $0 \to M_1 \to M_2 \to M_3 \to 0$ es una sucesión exacta corta, entonces en general $0 \to M_1 \otimes N \to M_2 \otimes N$ no es exacta. No obstante, existe un caso importante en el que la exactitud se preserva a través del producto tensorial.

Corolario 3.36. Si $0 \to M_1 \xrightarrow{\phi} M_2 \xrightarrow{\psi} M_3 \to 0$ es una sucesión exacta corta escindida, entonces $0 \to M_1 \otimes N \xrightarrow{\chi} M_2 \otimes N \xrightarrow{\theta} M_3 \otimes N \to 0$ es exacta.

De hecho, si $\tau : M_2 \to M_1$ es tal que $\tau\phi = \mathrm{id}_M$, entonces $(\tau \otimes \mathrm{id}_N)(\phi \otimes \mathrm{id}_N) = \mathrm{id}_{M_1 \otimes N}$, de manera que χ es inyectiva.

Un caso especial de este corolario es el caso del producto de espacios vectoriales (o, dicho de otra forma, F-módulos), que por tanto preserva la exactitud. De hecho, toda sucesión exacta corta de espacios vectoriales se escinde.

Proposición 3.37. Si M y N son F-espacios con bases $\{u_i : i \in I\}$ y $\{v_j : j \in J\}$, entonces $\{u_1 \otimes v_j : (i, j) \in I \times J\}$ es una base de $M \otimes N$. En particular, $\dim M \otimes N = (\dim M)(\dim N)$.

Demostración. Si $M_1 < M$ y $N_1 < N$, por el corolario anterior, las aplicaciones inclusión inducen un homomorfismo inyectivo $M_1 \otimes N_1 \to M \otimes N$. Por tanto, como los tensores de rango uno generan $M \otimes N$ y la independencia lineal está definida en términos de conjuntos finitos, podemos asumir que $I = \{1, ..., m\}$ y $J = \{1, ..., n\}$ son finitos. En consecuencia,

$$M \otimes N = \left(\bigoplus_{i=1}^{m} u_i F\right) \otimes \left(\bigoplus_{j=1}^{n} v_j F\right) \cong \bigoplus_{i,j} \left(u_i F \otimes v_j F\right) \cong \bigoplus_{i,j} \left(u_i \otimes v_j\right) F \qquad (3.13)$$

por la proposición 3.34.

La demostración anterior nos da otro ejemplo de la ambigüedad en la notación estándar de productos tensoriales, ya que la expresión $u_i \otimes v_j$ no solo depende de los elementos $u_i \otimes v_j$ sino de los módulos N y M en los que se incluyan. En general, en R-módulos el hecho de que los elementos $u_i \otimes v_j$ sean distintos, no nulos y linealmente independientes en $M_1 \otimes N_1$ no garantiza que los elementos correspondientes denotados de la misma forma en $M \otimes N$ mantengan dichas propiedades.

En el caso de módulos sobre un cuerpo, no tendremos este problema gracias a la exactitud del producto tensorial, de forma que $M_1 \otimes N_1 \to M \otimes N$ es inyectivo.

4. Álgebras semisimples

Tras nuestro trabajo en módulos en la sección anterior estamos en situación de introducir un concepto clave en el campo de las álgebras asociativas, el concepto de álgebra semisimple.

Nuestro principal objetivo en esta sección será llegar a demostrar el teorema de estructura de Wedderburn, de vital importancia en la teoría de álgebras.

4.1. Definición y propiedades

Definición 4.1. Una R-álgebra A es semisimple si A es semisimple como A-módulo a derecha.

Dicho de otro modo, A es semisimple si $A = \bigoplus_{i \in J} N_i$ con los N_i A-módulos simples a derecha. Como los N_i son submódulos de A_A, se tiene que que son ideales minimales a derecha. Además, el conjunto índice J ha de ser finito, ya que hemos visto que A_A está finitamente generado por 1_A.

Es relevante señalar que hemos definido las álgebras semisimples según módulos a derecha. Podríamos elaborar una definición similar con módulos a izquierda, y con lo visto hasta ahora no tendríamos motivo para suponer

que las estructuras de álgebra semisimple a derecha y a izquierda tuvieran que coincidir.

Más adelante, el teorema de estructura de Wedderburn nos permitirá ver que ambas estructuras son la misma, hasta entonces simplemente consideraremos que las estructuras a ambos lados son análogas sin más que cambiar «derecha» por «izquierda» en los resultados e invertir el orden de los factores.

De forma más rigurosa, solo tenemos que considerar que las álgebras semisimples a izquierda no son más que álgebras semisimples a derecha sobre el álgebra opuesta de A.

Pasaremos a nuestro estudio de álgebras semisimples reformulando la teoría de módulos semisimples.

Definición 4.2. Se dice que un álgebra A es artiniana (noetheriana) a derecha si A_A es artiniano (noetheriano), es decir, si el retículo de ideales de A satisface la condición de cadena descendente (ascendente).

Esta propiedad no será simétrica a izquierda como hemos adelantado que será la semisimplicidad, sin embargo. Obtengamos ahora algunas propiedades interesantes de las álgebras semisimples.

Proposición 4.3. Un álgebra A es semisimple si y solo si A es artiniana a derecha y $\mathrm{rad}A_A = 0$.

Dado que toda álgebra es finitamente generada como módulo a derecha o izquierda por la unidad de A, este resultado es un corolario inmediato de la proposición 3.33.

Un álgebra de dimensión finita A sobre un cuerpo F es automáticamente artiniana, ya que $S(A_A)$ es un subretículo de $S(A_F)$, y la dimensión finita de A_F implica que $S(A_F)$ satisface la condición de cadena descendente. En este caso, la proposición implica que A es semisimple si y solo si $\mathrm{rad}A = 0$. Más adelante probaremos que $\mathrm{rad}A_A = \mathrm{rad}_A A$, de forma que este subconjunto de A es un ideal, que llamaremos radical de Jacobson.

Demostraremos ahora un resultado que nos definirá la teoría de módulos sobre álgebras semisimples al mero estudio de las álgebras.

Proposición 4.4. Si A es un álgebra semisimple, entonces todo A-módulo es semisimple. Además, los A-módulos simples son isomorfos a ideales minimales a derecha de A, y todos los ideales minimales a derecha de A son A-módulos simples.

Demostración. Todo A-módulo libre a derecha es isomorfo a una suma directa de copias de A_A. Por tanto, los A-módulos libres son semisimples utilizando el corolario 3.17. Por la proposición 3.10, todo A-módulo a derecha simple es isomorfo a A_A/M con M un ideal maximal a derecha. La semisimplicidad de A_A garantiza que M tiene un complemento N en $S(A_A)$ por la proposición 3.15. Como M es un ideal maximal a derecha, N es un ideal minimal a derecha, y $N \cong A_A/M$. Así, los ideales minimales a derecha de A representan a todas las clases de isomorfismo de módulos simples.

Corolario 4.5. Si A es un álgebra semisimple, toda imagen por homomorfismos de A es semisimple.

Demostración. Sea $\theta : A \to B$ un homomorfismo de álgebras suprayectivo. Por los resultados obtenidos en el punto 2.1, se puede ver B como un A-módulo a derecha. Claramente, $\text{ann}B_A \supseteq \text{Ker}\theta$. Por la proposición anterior, B_A es semisimple, $B_A = \bigoplus_{i\in J} N_i$, con los N_i A-módulos simples. Como $\text{ann}N_i \supseteq \text{ann}B_A \supseteq \text{Ker}\theta$, se sigue que N_i es un B-módulo simple. Por tanto, B es semisimple.

A continuación veremos que las álgebras semisimples son también cerradas bajo productos finitos.

4.2. Ideales minimales a derecha

Para demostrar el teorema de estructura de Wedderburn precisaremos del lema de Schur, que ya hemos probado en la sección 2, y de algunos resultados sobre ideales minimales, que obtendremos a continuación.

Lema 4.6. Sea $A = A_1 \dot{+} A_2$ el producto interno de las álgebras A_1 y A_2, y sea M un ideal a derecha de A_1. Entonces,

(I). M es un ideal a derecha de A.

(II). $E_A(M) = E_{A_1}(M)$.

(III). $\mathrm{Hom}_A(M,A) = \mathrm{Hom}_A(M,A_1) = \mathrm{Hom}_{A_1}(M,A_1)$.

(IV). $S(M_{A_1}) = S(M_A)$.

(V). M es un ideal minimal a derecha de A si y solo si M es un ideal minimal a derecha de A_1.

(VI). Todo ideal minimal a derecha de A es un ideal minimal a derecha de A_1 o un ideal minimal a derecha de A_2.

Demostración. Los resultados (I) a (V) son consecuencia inmediata del hecho de que $MA_2 \subseteq A_1A_2 = 0$. Para el resultado (VI), supongamos que N es un ideal minimal a derecha de A. Para $i = 1,2$, tenemos que $NA_i \subseteq N \cap A_i < N$, de forma que o bien $N = N \cap A_i \subseteq A_i$ o bien $NA_i = N \cap A_i = 0$. No puede darse el caso de que $NA_1 = NA_2 = 0$ ya que entonces $N = NA_1 + NA_2 = 0$.

Corolario 4.7. Si A_1 y A_2 son álgebras semisimples, entonces $A_1 \dot{+} A_2$ es semisimple

Con ello obtenemos que la clase de álgebras semisimples es cerrada bajo productos finitos.

Lema 4.8. Si N es un ideal minimal a derecha del álgebra A, y $x \in A$, entonces o bien $xN = 0$ o bien xN es un ideal minimal a derecha de A tal que $xN \cong N$ como A-módulos.

Demostración. La aplicación $y \mapsto xy$ es un homomorfismo de A-módulos suprayectivo de N en xN, por lo que es una consecuencia directa del lema de Schur.

Lema 4.9. Sea N un ideal a derecha del álgebra A que satisface $N^k = 0$. Si P es un A-módulo simple, entonces $PN = 0$. Además, $N \subseteq \mathrm{rad}A_A$.

Demostración. Dado que P es simple y $PN < P$, o bien $PN = 0$ o bien $PN = N$. La segunda opción es imposible ya que lleva a contradicción: $P = PN = PN^2 = ... = PN^k = 0$. En particular, si M es un ideal maximal a derecha de A, entonces $(A_A/M)N = 0$, esto es, $N \subseteq M$. Por tanto, $N \subseteq \mathrm{rad}A_A$, la intersección de todos los ideales maximales a derecha de A.

Proposición 4.10. Las siguientes condiciones son equivalentes para ideales minimales a derecha N_1 y N_2 del álgebra semisimple A:

(I). $N_1 \cong N_2$ como A-módulos.

(II). $N_1 N_2 \neq 0$.

(III). Existe un elemento $x \in A$ tal que $N_1 = xN_2$.

Demostración. Si $\phi : N_1 \to N_2$ es un isomorfismo de A-módulos, entonces $\phi(N_1 N_2) = \phi(N_1)N_2 = N_2^2 \neq 0$ por el lema anterior. Así, $N_1 N_2 \neq 0$. Supongamos que $x \in N_1$ es tal que $xN_2 \neq 0$. Como N_1 es simple y xN_2 es un submódulo no nulo de N_1, se sigue que $N_1 = xN_2$. Finalmente, (III) implica (I) de forma inmediata por el lema 4.8.

Lema 4.11. Sea A un álgebra semisimple con $A_A = N_1 \oplus ... \oplus N_m$ con cada N_i un ideal minimal a derecha de A. Si N es un ideal minimal a derecha de A, entonces $N \cong N_i$ para algún i con $1 \leq i \leq m$.

Demostración. Dado que A_A es semisimple, por la proposición 3.15 tenemos que $A_A = N \oplus M$ para un cierto ideal a derecha M. Por el corolario 3.16, M es también un A-módulo semisimple. La conclusión de que $N \cong N_i$ es inmediata bien por la proposición 3.22 o bien por el teorema de Jordan-Hölder.

Corolario 4.12. Si A es un álgebra semisimple, entonces el número de clases de isomorfismos de A-módulos simples es finito.

Este corolario es consecuencia directa del lema anterior y de la proposición 4.4

4.3. Álgebras simples

Pasaremos ahora a trabajar el concepto de álgebra simple. Al contrario de lo que ocurre con módulos, no todas las álgebras simples son semisimples, como podría parecer por el nombre. Así, pasaremos a caracterizar cuándo un álgebra simple es semisimple y viceversa.

Definición 4.13. Un álgebra A es simple si $A \neq 0$ y $I(A) = \{0, A\}$.

Proposición 4.14. Dada un álgebra simple A, las siguientes condiciones son equivalentes:

(I). A es semisimple.

(II). A es artiniana a derecha.

(III). A tiene un ideal minimal a derecha.

Demostración. (I) implica (II) por la proposición 3.33, y es evidente que (II) implica (III). Supongamos que N es un ideal minimal a derecha de A. Entonces $AN = \sum_{x\in A} xN$ es un ideal no nulo de A, de forma que $A = \sum_{x\in A} xN$ ya que A es simple. Por el lema 4.8, todo xN no nulo es un A-módulo simple a derecha. Por tanto, A es semisimple usando la proposición 3.15.

Proposición 4.15. Dada un álgebra semisimple A, las siguientes condiciones son equivalentes:

(I). A es simple.

(II). Todos los ideales minimales a derecha de A son isomorfos.

(III). Todos los A-módulos simples a derecha son isomorfos.

Demostración. Por la proposición 4.4, todo A-módulo simple a derecha es isomorfo a un ideal minimal a derecha e A, por lo que (II) y (III) son equivalentes. Supongamos que A es simple que y que N_1 y N_2 son ideales minimales a derecha de A. Entonces $AN_1 = AN_2 = A$, como en la demostración anterior. Por tanto, $A(N_1N_2) = (AN_1)N_2 = AN_2 = A$. En particular, $N_1N_2 \neq 0$, de forma que $N_1 \cong N_2$ por la proposición 4.10. Análogamente, supongamos que todos los ideales minimales a derecha de A son isomorfos. Sea J un ideal no nulo de A. Como A es semisimple, existe un ideal minimal a derecha N de A tal que $N \subseteq J$. La suposición de que todos los ideales minimales a derecha de A son isomorfos, junto con las proposiciones 4.10 y 3.15, lleva a que $A = \sum\{xN : x \in A\} \subseteq J$. Por tanto, A es simple.

Corolario 4.16. Sea A un álgebra simple y sea N un ideal minimal a derecha suyo. Si M es un A-módulo a derecha, entonces existe un único número cardinal α tal que $M \cong \bigoplus_\alpha N$.

Esto se sigue de forma directa de las dos proposiciones que acabamos de demostrar junto con la proposición 3.22.

Corolario 4.17. Sea A una F-álgebra simple y de dimensión finita con F un cuerpo, y sean M_1 y M_2 A-módulos a derecha. Entonces $M_1 \cong M_2$ si y solo si $\dim_F M_1 = \dim_F M_2$.

Demostración. Dado que A es de dimensión finita, es artiniana, y existe un ideal minimal a derecha N de A con $\dim_F N$ finita. Por el corolario anterior, $M_1 \cong \bigoplus_\alpha N$ y $M_2 \cong \bigoplus_\beta N$ para ciertos números cardinales α y β. Claramente, $M_1 \cong M_2$ si y solo si $\alpha = \beta$, y dado que $\dim_F N < \infty$, $\alpha = \beta$ es equivalente a $\dim_F M_1 = \alpha \dim_F N = \beta \dim_F N = \dim_F M_2$.

A modo de ejemplo, apliquemos estos resultados a un álgebra matricial.

Proposición 4.18. Sea $A = M_n(D)$ el álgebra de matrices $n \times n$ con entradas en un álgebra de división D. Para $1 \leq i \leq n$, definimos $N_i = \epsilon_{ii} A$. Entonces

(I). N_i es un ideal minimal a derecha de A.

(II). $A_A = \bigoplus_{i=1}^n N_i$.

(III). $N_i \cong N_j$ para todo i, j.

(IV). A_A es simple y semisimple.

(V). $E_A(N_i) \cong D$.

Demostración. Claramente, N es un ideal a derecha de A. Si $\alpha = \sum_{j,k} \epsilon_{jk} z_{jk}$ con $z_{jk} \in D$, entonces $\epsilon_{ii}\alpha = \sum_k \epsilon_{ik} z_{ik}$. Así, $N_i = \sum_k \epsilon_{ik} D = \bigoplus_k \epsilon_{ik} D$ y $A = \bigoplus i, k \epsilon_{ik} D = \bigoplus_i N_i$ como D-módulos. Si $\beta = \sum_k \epsilon_{ik} z_k \in N_i$ con algún $z_j \neq 0$, entonces $\beta(\sum_i \epsilon_{ji} z_j^{-1} w_i) = \sum_i \epsilon_{il} w_i$ para $w_i \in D$ arbitrarios. Esto es, si $0 \neq \beta \in N_i$, entonces $\beta A = N_i$, de forma que N_i es simple por la proposición 3.10. Además, $N_j = \epsilon_{jj} A = \epsilon_{ji}\epsilon_{ij} A = \epsilon_{ji} N_i$, y por tanto $N_j \cong N_i$ por la proposición 4.10. Se sigue de (I), (II), (III) y el lema 4.11 que A_A es semisimple y sus ideales minimales a derecha son isomorfos. Por tanto, A es simple por la proposición 4.15. Dado $z \in D$, la aplicación multiplicación a izquierda $\lambda_z \alpha = z\alpha$ es un endomorfismo de A-módulos de N_i, y $z \mapsto \lambda_z$ es un homomorfismo inyectivo de D

en $E_A(N_i)$. Si $\phi \in E_A(N_i)$, supongamos $\phi(\epsilon_{ii}) = \epsilon_{ii}\beta$, entonces $\phi(\epsilon_{ii}) = \phi(\epsilon_{ii}^2) = \phi(\epsilon_{ii})\epsilon_{ii} = \epsilon_{ii}\beta\epsilon_{ii} = z\epsilon_{ii}$ para cierto $z \in D$. En consecuencia, si $\alpha \in N_i$, entonces $\phi(\alpha) = \phi(\epsilon_{ii}\alpha) = \phi(\epsilon_{ii})\alpha = z\epsilon_{ii}\alpha = z\alpha = \lambda_z\alpha$, esto es, $\phi = \lambda_z$. Por tanto, $D \cong E_A(N_i)$.

4.4. Matrices de homomorfismos

Para abordar la demostración del teorema de Wedderburn, introduciremos una notación matricial generalizada que resultará útil.

Sea A una R-álgebra, y supongamos que $(M_1, M_2, ...M_n)$ es una sucesión de A-módulos a derecha. Denotamos por

$$[\mathrm{Hom}_A(M_j, M_i)] = \begin{bmatrix} \mathrm{Hom}_A(M_1, M_1) & \mathrm{Hom}_A(M_2, M_1) & ... & \mathrm{Hom}_A(M_n, M_1) \\ \mathrm{Hom}_A(M_1, M_2) & \mathrm{Hom}_A(M_2, M_2) & ... & \mathrm{Hom}_A(M_n, M_2) \\ . & . & . & . \\ \mathrm{Hom}_A(M_1, M_n) & \mathrm{Hom}_A(M_2, M_n) & ... & \mathrm{Hom}_A(M_n, M_n) \end{bmatrix} \tag{4.1}$$

al conjunto de todas las matrices $n \times n$

$$\begin{bmatrix} \phi_{11} & \phi_{12} & ... & \phi_{1n} \\ \phi_{21} & \phi_{22} & ... & \phi_{2n} \\ . & . & . & . \\ \phi_{n1} & \phi_{n2} & ... & \phi_{nn} \end{bmatrix} \tag{4.2}$$

con $\phi_{ij} \in \mathrm{Hom}_A(M_j, M_i)$.

Definimos la suma y la multiplicación por escalares componente a componente, y definimos la multiplicación interna con la regla usual de la multiplicación, $[\phi_{ij}][\psi_{jk}] = [\chi_{ik}]$, con $\chi_{ik} = \sum_{j=1}^{n} \phi_{ij}\psi_{jk} \in \mathrm{Hom}_A(M_k, M_i)$.

Proposición 4.19. $[\mathrm{Hom}_A(M_j, M_i)]$ es una R-álgebra isomorfa a

$$E_A(M_1 \oplus M_2 \oplus ... \oplus M_n).$$

Demostración. Denotamos la suma directa $M_1 \oplus M_2 \oplus ... \oplus M_n$ por M. Sea $\pi_j : M \to M_j$ y $\kappa_j : M_j \to M$ los homomorfismos proyección e inyección asociados

a la suma directa. Entonces se cumple

$$\sum_{j=1}^{n} \kappa_j \pi_j = \mathrm{id}_M \tag{4.3}$$

$$\pi_i \kappa_j = 0 \quad \text{si} \quad i \neq j; \quad \pi_j \kappa_j = \mathrm{id}_{M_j} \tag{4.4}$$

Definimos las aplicaciones $\alpha : E_A(M) \to [\mathrm{Hom}_A(M_j, M_i)]$ y $\beta : [\mathrm{Hom}_A(M_j, M_i)] \to E_A(M)$ por $\alpha(\phi) = [\pi_i \phi \kappa_j]$ y $\beta([\phi_{ij}]) = \sum_{i,j=1}^{n} \kappa_i \phi_{ij} \pi_j$. Trivialmente, $\beta\alpha$ es la aplicación identidad en $E_A(M)$ y $\alpha\beta$ es la identidad en $[\mathrm{Hom}_A(M_j, M_i)]$. Además, α es un homomorfismo de R-álgebras. Por ejemplo, $\alpha(\phi\psi) = [\pi_i \phi \psi \kappa_k] = [\pi_i \phi (\sum_{j=1}^{n} \kappa_j \pi_j) \psi \kappa_k] = [\sum_{j=1}^{n} (\pi_i \phi \kappa_j)(\pi_j \psi \kappa_k)] = \alpha(\phi)\alpha(\psi)$. Así, α es un isomorfismo.

Corolario 4.20. Si A es una R-álgebra y M es un A-módulo a derecha, entonces

$$E_A(\bigoplus_n M) \cong M_n(E_A(M)).$$

Corolario 4.21. Si A es una R-álgebra y M es el A-módulo libre a derecha con n generadores, entonces $E_A(M) \cong M_n(A)$.

Demostración. Dado que $M \cong \bigoplus_n A_A$, el corolario anterior lleva a que $E_A(M) \cong M_n(E_A(A_A))$, y por tanto $E_A(A_A) \cong A$ por la proposición 2.8.

Corolario 4.22. Si A es una R-álgebra y M_1, M_2, ..., M_n son A-módulos a derecha tales que $\mathrm{Hom}_A(M_i, M_j) = 0$ si $i \neq j$, entonces

$$E_A\left(\bigoplus_{i=1}^{n} M_i\right) \cong E_A(M_1) \dot{+} E_A(M_2) \dot{+} \ldots \dot{+} E_A(M_n)$$

Demostración. Usando la proposición, $E_A\left(\bigoplus_{i=1}^n M_i\right)$ es isomorfo a

$$\begin{bmatrix} \mathrm{Hom}_A(M_1,M_1) & \mathrm{Hom}_A(M_2,M_1) & ... & \mathrm{Hom}_A(M_n,M_1) \\ \mathrm{Hom}_A(M_1,M_2) & \mathrm{Hom}_A(M_2,M_2) & ... & \mathrm{Hom}_A(M_n,M_2) \\ . & . & . & . \\ \mathrm{Hom}_A(M_1,M_n) & \mathrm{Hom}_A(M_2,M_n) & ... & \mathrm{Hom}_A(M_n,M_n) \end{bmatrix} =$$

$$\begin{bmatrix} E_A(M_1) & & & \\ & E_A(M_2) & & \\ & & \ddots & \\ & & & E_A(M_n) \end{bmatrix} \cong E_A(M_1) \dotplus E_A(M_2) \dotplus ... \dotplus E_A(M_n)$$

4.5. Teorema de estructura de Wedderburn

Con los resultados anteriores ya estamos en posición de enunciar y demostrar el teorema de estructura de Wedderburn, que resultará fundamental en la teoría de álgebras asociativas.

Teorema 4.23. Teorema de estructura de Wedderburn. Sea A una R-álgebra semisimple a derecha o a izquierda. Entonces

(I). Existen números naturales $n_1,...,n_r$ y R-álgebras de división $D_1,...,D_r$ tales que

$$A \cong M_{n_1}(D_1) \dotplus ... \dotplus M_{n_r}(D_r) \tag{4.5}$$

(II). Los pares $(n_1,D_1),...,(n_r,D_r)$ para los que se satisface (4.5) están unívocamente determinados (salvo isomorfismos) por A.

(III). Análogamente, si $n_1,...,n_r \in \mathbb{N}$ y $D_1,...,D_r$ son álgebras de división sobre R, entonces $M_{n_1}(D_1) \dotplus ... \dotplus M_{n_r}(D_r)$ es una R-álgebra semisimple a izquierda y derecha.

Demostración. (I): Si A es semisimple a derecha, entonces $A_A \cong M_1 \oplus ... \oplus M_r$, con los M_i sumas directas de n_i copias de un ideal minimal a derecha N_i de A, elegido de forma que N_i no sea isomorfo a N_j si $i \neq j$. Por el lema 3.21, $\mathrm{Hom}_A(M_i,M_j) = 0$ si $i \neq j$. El isomorfismo (4.5) se sigue de la proposición 2.8 y de los corolarios 4.22 y 4.20: $A \cong E_A(A_A) \cong E_A(M_1) \dotplus ... \dotplus E_A(M_r) \cong M_{n_1}(D_1) \dotplus ... \dotplus$

$M_{n_r}(D_r)$ con $D_i = E_A(N_i)$ un álgebra de división sobre R por el lema de Schur. El resultado para álgebras semisimples a izquierda es análogo empleando ideales minimales a izquierda y endomorfismos a derecha.

(II): Supongamos que $A = A_1 \dotplus ... \dotplus A_s$, con $A_i \cong M_{k_i}(C_i)$ donde C_i son álgebras de división sobre R. Por la proposición 4.18 y el lema 4.6, A_i es isomorfo como A-módulo a una suma directa de k_i copias de un ideal minimal a derecha P_i de A, con $P_i \subseteq A_i$, y $C_i \cong E_{A_i}(P_i) = E_A(P_i)$. Dado que cada A_i es un ideal de A que contiene a P_i, la proposición 4.10 implica que $P_i \ncong P_j$ si $i \neq j$. La unicidad de las descomposiciones en suma directa de módulos simples da el resultado que buscamos, $s = r$ y (en un orden adecuado) $k_i = n_i$, $P_i \cong N_i$ como A-módulos y $C_i \cong E_A(P_i) \cong E_A(N_i) = D_i$.

(III): Por la proposición 4.18 y su análogo a izquierda, cada una de las R-álgebras $M_n(D_i)$ es semisimple a derecha y a izquierda. Por tanto, $M_{n_1}(D_1) \dotplus ... \dotplus M_{n_r}(D_r)$ es semisimple a derecha e izquierda por el corolario 4.7.

Las partes (I) y (III) del teorema nos muestran el resultado que habíamos adelantado de que las clases de álgebras semisimples a derecha e izquierda coinciden. Además, para álgebras simples, las condiciones de cadena descendentes a izquierda y derecha son equivalentes.

Corolario 4.24. Un álgebra artiniana a derecha o izquierda A es simple si y solo si $A \cong M_n(D)$ para cierto número natural n y cierta álgebra de división D. En este caso, A determina n unívocamente y D salvo isomorfismo.

Para algunos cuerpos F, las únicas álgebras de división de dimensión finita sobre F son conmutativas. En este caso, el teorema de estructura arroja conclusiones más fuertes sobre las álgebras semisimples de dimensión finita: los D_i son necesariamente cuerpos. El resultado óptimo se obtiene cuando F es algebraicamente cerrado.

Lema 4.25. Sea F un cuerpo algebraicamente cerrado. Si D es un álgebra de división de dimensión finita sobre F, entonces $D = F$.

Demostración. Sea $\dim_F D = m$. Si $x \in D$, entonces la sucesión $1, x, ..., x^m$ es linealmente dependiente, de forma que existe un polinomio mónico $\Phi \in F[X]$ de grado mínimo tal que $\Phi(x) = 0$. Dado que D es un álgebra de división, el

hecho de que el grado de Φ sea mínimo implica que Φ es irreducible sobre F. En consecuencia, $\Phi = X - a$ para algún $a \in F$, ya que F es algebraicamente cerrado. Esto es, $x = a \in F$.

Corolario 4.26. Sea F un cuerpo algebraicamente cerrado. Una F-álgebra de dimensión finita A es semisimple si y solo si $A \cong M_{n_1}(F) \dotplus ... \dotplus M_{n_r}(F)$ donde $1 \leq n_1 \leq ... \leq n_r$ están unívocamente determinados por el tipo de isomorfismo de A. Además, A es simple si y solo si $A \cong M_n(F)$, donde $\dim_F A = n^2$.

Este último corolario es consecuencia inmediata del lema anterior y del teorema de estructura.

4.6. Teorema de Maschke

El teorema de estructura de Wedderburn que acabamos de probar es una caracterización interna del concepto de álgebra semisimple. En la siguiente sección del trabajo, dedicada a la teoría del radical, encontraremos lo importantes que son estas álgebras en la teoría general. Antes de pasar a ello, nos pararemos en un resultado de interesante aplicación en la teoría clásica de representaciones de grupos.

Teorema 4.27. Teorema de Maschke. Sea G un grupo finito y F un cuerpo. El álgebra de grupo FG es semisimple si y solo si la característica de F no divide al orden de G.

Demostración. Supongamos que F no divide a $n = |G|$. Esto implica que n (identificado con $n \cdot 1 \in FG$) es una unidad. Por la proposición 3.15 es suficiente probar que si M es un ideal a derecha de FG, entonces $FG = M \oplus N$ para algún ideal a derecha N de FG. Podemos llegar a esta conclusión probando que existe un homomorfismo de FG-módulos $\rho : FG \to M$ tal que $\rho u = u$ para todo $u \in M$. De hecho, dado un ρ que cumpla esto, $N = \text{Ker}\rho = (1 - \rho)M$ es un ideal a derecha tal que $M \cap N = 0$ y $M + N = FG$. Como primera aproximación a ρ usaremos el hecho de que M es un subespacio de FG (con FG considerado como espacio vectorial sobre el cuerpo F) para encontrar un homomorfismo de F-espacios $\pi : FG \to M$ que satisfaga $\pi u = u$ para todo $u \in M$. Definiremos ρ promediando π sobre G.

De forma rigurosa, dado $u \in FG$, sea $\rho u = \left(\sum_{x\in G} \pi(ux)x^{-1}\right) n^{-1}$. Claramente, ρ es un homomorfismo de F-espacios. Sin embargo, podemos observar que para todo $y \in G$, $\rho(uy) = \left(\sum_{x\in G} \pi(uyx)x^{-1}\right) n^{-1} = \left(\left(\sum_{x\in G} \pi(u(yx))(yx)^{-1}\right) y\right) n^{-1} = \left(\left(\sum_{yx\in yG=G} \pi(u(yx))(yx)^{-1}\right) n^{-1}\right) y = \rho(u)y$.

Por tanto, ρ es un homomorfismo de FG-módulos. Finalmente, sea $u \in M$. Entonces $ux \in M$ para todo $x \in G$ ya que M es un ideal a derecha. Por tanto, dado que $\pi|_M = \mathrm{id}_M$, tenemos que $\rho u = \left(\sum_{x\in G} \pi(ux)x^{-1}\right) n^{-1} = \left(\sum_{x\in G} (ux)x^{-1}\right) n^{-1} = \left(\sum_{x\in G} u\right) n^{-1} = (un)n^{-1} = u$. Consideramos ahora el caso en el que la característica de F (que es necesariamente un primo) divide al orden n de G. Esto implica que la suma de n copias de un elemento de FG es cero. Sea $e = \sum_{x\in G} x \in FG - \{0\}$. Entonces $ey = \sum_{x\in G} xy = \sum_{xy\in Gy=g} xy = e$ para todo $y \in G$. En consecuencia, $e^2 = \sum_{y\in G} ey = \sum_{y\in G} e = en = 0$. Además, el ideal a derecha N de FG generado por e coincide con eF. Por tanto, $N^2 = 0$. Se sigue del lema 4.9 que $0 \neq N \subseteq \mathrm{rad}FG$. Por tanto, por el corolario 4.5, FG no es semisimple.

La mayoría de resultados de representación de grupos utilizan el álgebra de grupo compleja $\mathbb{C}G$, que cumple las condiciones del teorema. Sin embargo, la mayoría de resultados son aplicables a cualquier cuerpo F algebraicamente cerrado cuya característica no divida al orden de G. En estas condiciones, los n_i del corolario 4.26 son los grados de las representaciones irreducibles de G, esto es, las dimensiones de los FG-módulos simples. Además, el número r de factores simples es una propiedad numérica estándar de G, como veremos en el siguiente corolario.

Corolario 4.28. Sea G un grupo finito cuyo orden no es divisible por la característica del cuerpo algebraicamente cerrado F. El álgebra de grupo FG es isomorfa a un producto $M_{n_1}(F) \dotplus \ldots \dotplus M_{n_r}(F)$ de álgebras matriciales completas sobre F, donde r es el número de clases de conjugación de G.

Por el teorema de Maschke la única parte sin probar sería que r es el número de clases de conjugación. Esto se sigue de dos observaciones básicas: como F-espacio, el centro $Z(M_{n_1}(F) \dotplus \ldots \dotplus M_{n_r}(F))$ es de dimensión r; y $\dim_F Z(FG)$ es el número de clases de conjugación de G. Ambas afirmaciones son relativamente directas y fáciles de demostrar, por lo que no profundizaremos más en ello.

5. El radical de un álgebra

Con el teorema de Wedderburn hemos podido caracterizar las álgebras semisimples y hemos visto que es una clase bastante pequeña. Por otro lado, hemos visto que el concepto del radical de un álgebra tiene gran importancia a la hora de estudiar su semisimplicidad. Es por ello que profundizaremos más en sus propiedades.

5.1. Propiedades básicas

El primer resultado que buscaremos probar es que el radical de un álgebra es un ideal. Para ello, necesitaremos un resultado previo aplicable a radicales de módulos.

Lema 5.1. Sean M_1 y M_2 A-módulos a derecha. Si $\phi \in \mathrm{Hom}_A(M_1, M_2)$, entonces $\phi(\mathrm{rad}M_1) \subseteq \mathrm{rad}M_2$, y ϕ induce un homomorfismo de $M_1/\mathrm{rad}M_1$ en $M_2/\mathrm{rad}M_2$.

Demostración. Si $N < M_2$, entonces ϕ induce una aplicación inyectiva de $M_1/\phi^{-1}(N)$ en M_2/N. En particular, si M_2/N es simple, entonces o bien $\phi^{-1}(N) = M_1$ o bien $M_1/\phi^{-1}(N) \cong M_2/N$ es simple. En ambos casos, $\phi^{-1}(N) \supseteq \mathrm{rad}M_1$. Así, $\phi^{-1}(\mathrm{rad}M_2) \supseteq \mathrm{rad}M_1$, esto es, $\phi(\mathrm{rad}M_1) \subseteq \mathrm{rad}M_2$. La última afirmación, por tanto, es trivial.

Proposición 5.2. Si A es una R-álgebra no trivial, entonces $\mathrm{rad}A_A$ es un ideal propio bilátero de A.

Demostración. La aplicación $y \mapsto xy$ es un endomorfismo de A-módulos de A para todo $x \in A$. Por el lema anterior, $x(\mathrm{rad}A_A) \subseteq \mathrm{rad}A_A$, esto es, $\mathrm{rad}A_A \lhd A$. Como A tiene elemento unidad, se sigue por el lema de Zorn que existe un ideal maximal a derecha M de A. En consecuencia, A_A/M es simple. Por tanto, $\mathrm{rad}A_A \subseteq M \subset A$, por lo que $\mathrm{rad}A_A$ es un ideal propio de A.

Corolario 5.3. Si A es una R-álgebra artiniana a derecha, entonces $A/\mathrm{rad}A_A$ es una R-álgebra semisimple.

Demostración. Se sigue del corolario 3.16 que $A/\mathrm{rad}A_A$ es un A-módulo semisimple, y por tanto también es semisimple como $(A/\mathrm{rad}A_A)$-módulo por la proposición 3.4. Usando el lema 3.31 tenemos que $\mathrm{rad}(A/\mathrm{rad}A_A) = 0$. Así, $A/\mathrm{rad}A_A$ es un álgebra semisimple por la proposición 4.3.

Notemos que lo que afirma el corolario tiene sentido ya que al ser $\mathrm{rad}A_A$ un ideal, $A/\mathrm{rad}A_A$ es un álgebra.

Corolario 5.4. Si M es un A-módulo a derecha, entonces $M(\mathrm{rad}A_A) \subseteq \mathrm{rad}M$.

Demostración. Para todo $u \in M$, la aplicación $x \mapsto ux$ es un homomorfismo de A-módulos de A_A en M, por lo que usando el lema, $u(\mathrm{rad}A_A) \subseteq \mathrm{rad}M$.

5.2. Lema de Nakayama

Existen diferentes resultados equivalentes que se conocen como «lema de Nakayama». A continuación, presentaremos dos de las versiones más habituales del lema, que resulta de capital importancia en la teoría de anillos.

Tiene también importantes aplicaciones a la teoría de grupos, ya que el radical de un módulo es análogo al subgrupo de Frattini de un grupo, y el lema de Nakayama es una variante de la caracterización estándar del subgrupo de Frattini.

Lema 5.5. Dado un elemento u de un A-módulo M, las siguientes condiciones son equivalentes.

(I). $u \in \mathrm{rad}M$.

(II). Si $N < M$ es tal que $uA + N = M$, entonces $N = M$.

Demostración. Si $u \notin \mathrm{rad}M$, entonces existe un submódulo N de M tal que M/N es simple y $u \notin N$. En ese caso, $uA + N = M \neq N$. Por tanto, (I) es consecuencia de (II). Análogamente, supongamos que existe $N < M$ con la propiedad $uA + N = M \neq N$. Es claro que $u \notin N$. Por el lema de Zorn, existe un submódulo P de M que contiene a N tal que es maximal con la propiedad $u \notin P$. Si $P \subset Q < M$, entonces $u \in Q$, de forma que $M = uA + N \subseteq Q$. Por tanto, M/P es simple, $\mathrm{rad}M \subseteq P$ y por tanto $u \notin \mathrm{rad}M$.

Proposición 5.6. Lema de Nakayama para módulos. Sea P un submódulo del A-módulo M que satisface la propiedad de que para todo submódulo N de M, si $P + N = M$ entonces $N = M$. Entonces $P \subseteq \mathrm{rad}M$. Análogamente, si $P < M$, $P \subseteq \mathrm{rad}M$, y o P o M es finitamente generado como A-módulo, entonces P satiface la propiedad anterior.

Demostración. Supongamos que existe $u \in P - \text{rad}M$. Usando el lema anterior, existe un submódulo N de M tal que $N \neq M = uA + N \subseteq P + N$. Para probar la otra implicación, supongamos que $P < \text{rad}M$ y $N < M$ es tal que $P + N = M$. Si M es finitamente generado, entonces existe un submódulo finitamente generado Q de P tal que $Q + N = M$. Así, en todos los casos se puede asumir que P es finitamente generado. Tomemos $P = u_1A + u_2A + ... + u_nA$. Usando el lema de nuevo iterativamente llegamos al resultado, $M = u_1A + u_2A + ...u_nA + N = u_2A + ... + u_nA + N = ... = u_nA + N = N$.

Proposición 5.7. Lema de Nakayama para álgebras. Sea P un ideal a derecha de la R-álgebra A. Las siguientes condiciones son equivalentes.

(I). $P \subseteq \text{rad}A_A$.

(II). Si M es un A-módulo a derecha finitamente generado, y $N < M$ satisface $N + MP = M$, entonces $N = M$.

(III). $G = \{1 + x : x \in P\}$ es un subconjunto de A^o.

Demostración. La propiedad (II) se sigue de la (I) como consecuencia del lema de Nakayama para módulos y el corolario 5.3. Para probar (III) desde (II), sea $x \in P$. Denotamos $y = 1 + x$. Se sigue que $1 = y - x \in yA + P$ de forma que $yA + P = A_A$. Como A_A está finitamente generado por 1, se sigue de (II) que $yA = A$. En particular, $1 = yz = z + xz$ para algún $z \in A$. Por tanto, $z = 1 - xz \in G$, ya que $P < A_A$ y $x \in P$. Con esto probamos que todo elemento de G tiene inverso por la derecha en G. Por tanto, G es un grupo y $G \subseteq A^o$. Para deducir (I) desde (III), sea $x \in P$. Por el lema, basta probar que si un ideal a derecha N de A satisface $xA + N = A$, entonces $N = A$. La hipótesis $xA + N = A$ implica que $1 = xz + y$ para ciertos $z \in A$, $y \in N$. Así, $y = 1 + x(-z)$ con $x(-z) \in P$. Por (III), $y \in A^o$. Así, $N = A$, como buscábamos.

Tomando $N = 0$ y $P = \text{rad}A_A$ en esta segunda versión obtenemos un corolario que también se suele llamar lema de Nakayama.

Corolario 5.8. Si M es un A-módulo a derecha finitamente generado tal que $M(\text{rad}A_A) = M$, entonces $M = 0$.

5.3. El radical de Jacobson

Con lo que hemos demostrado hasta ahora estamos en situación de demostrar lo que ya afirmamos en el párrafo 4.1.

Lema 5.9. Si A es una R-álgebra, entonces $\mathrm{rad}\, A_A = \mathrm{rad}_A A$.

Demostración. Usando los análogos a izquierda de los párrafos anteriores, ${}_A A < A_A$ y $\{1 + x : x \in \mathrm{rad}_A A\} \subseteq A^o$. Por el lema de Nakayama, $\mathrm{rad}_A A \subseteq \mathrm{rad}\, A_A$. Usando un argumento simétrico, $\mathrm{rad}\, A_A \subseteq \mathrm{rad}_A A$.

Una vez probado esto, podemos fijar nuestra notación para este radical.

Definición 5.10. Dada una R-álgebra A, el radical de Jacobson de A es $J(A) = \mathrm{rad}\, A_A$.

Proposición 5.11. El radical de Jacobson de un álgebra A es un ideal bilátero $J(A)$ que satisface

(I). $J(A) = \bigcap\{M : M \text{ es un ideal maximal a derecha de } A\}$.

(II). $J(A) = \{x \in A : 1 + xy \in A^o \ \forall\, y \in A\}$.

(III). $J(A) = \{x \in A : 1 + yx \in A^o \ \forall\, y \in A\}$.

Esta proposición es consecuencia inmediata del lema anterior y del lema de Nakayama. En adelante cuando hablemos del «radical de A» nos referiremos al radical de Jacobson de A.

Una versión alternativa de la proposición nos será también útil más adelante.

Corolario 5.12. Si M es un ideal a derecha o izquierda del álgebra A tal que $1+x \in A^o$ para todo $x \in M$, entonces $M \subseteq J(A)$. Si además $\mathrm{rad}\, A/M = 0$, entonces $M = J(A)$.

Demostración. La hipótesis de que M es un ideal a izquierda o derecha y que $1+x \in A^o$ para todo $x \in M$ implica que $M \subseteq J(A)$ por la proposición anterior. Por otra parte, si $\mathrm{rad}\, A/M = 0$, entonces $J(A) \subseteq M$ por el lema 3.31.

Diremos que un elemento x de un álgebra A es nilpotente si existe un número natural n tal que $x^n = 0$. Eso nos lleva al siguiente corolario.

Corolario 5.13. Si M es un ideal a derecha o izquierda del álgebra A tal que todo elemento de M es nilpotente, entonces $M \subseteq J(A)$.

Demostración. Si $x^n = 0$, entonces $(1+x)\left(\sum_{0\leq i\leq n}(-x)^i\right) = \left(\sum_{0\leq i\leq n}(-x)^i\right)(1+x) = 1$, por lo que es un caso particular del corolario anterior.

Obtendremos ahora algunas propiedades útiles del radical de Jacobson.

Lema 5.14. Sean A y B R-álgebras.

(I). Si $\theta : A \to B$ es un homomorfismo de álgebras suprayectivo, entonces $\theta(J(A)) \subseteq J(B)$.

(II). $J(A \dotplus B) = J(A) \dotplus J(B)$.

Demostración. (I) es consecuencia de los lemas 5.1 y 3.1, $\theta(J(A)) = \theta(\mathrm{rad}A_A) \subseteq \mathrm{rad}B_A = \mathrm{rad}B_B = J(B)$. Aplicando este resultado a las proyecciones de $A \dotplus B$ en A y B tenemos que $J(A \dotplus B) \subseteq J(A) \dotplus J(B)$. Por otro lado, si $x \in J(A)$, $y \in J(B)$, entonces $1_A + x \in A^o$ y $1_B + y \in B^o$ por la proposición. Por tanto, $(1_A, 1_B) + (x, y)$ es una unidad de $A \dotplus B$. Como $J(A) \dotplus J(B)$ es un ideal de $A \dotplus B$, se sigue del corolario 5.12 que $J(A) \dotplus J(B) \subseteq J(A \dotplus B)$.

Veamos ahora un ejemplo de una clase de álgebras con radical cero.

Proposición 5.15. Si M es un A-módulo semisimple, entonces $J(E_A(M)) = 0$.

Demostración. Cuando M es también finitamente generado, $E_A(M)$ es siempre semisimple y el radical es 0 de forma trivial. Para probar el resultado en general, sea $0 \neq \phi \in E_A(M)$. Por la proposición 3.15 es claro que existe un submódulo simple N de M tal que $\phi(N) \neq 0$. Por el lema de Schur, ϕ lleva N de forma isomorfa a $\phi(N)$. Aplicando de nuevo la proposición 3.15 tenemos la existencia de $\pi \in E_A(M)$ tal que $\pi^2 = \pi$ y $\pi(M) = \phi(N)$. Sea $\psi = (\phi|_N)^{-1}\pi$. Claramente, $\psi \in E_A(M)$ y $\phi\psi = \pi$. Como $\pi \neq 0$ y $\pi(1 - \phi\psi) = 0$, se sigue que $1 - \phi\psi$ no es una unidad de $E_A(M)$. Por tanto, $\phi \notin J(E_A(M))$ por la proposición.

5.4. El radical de un álgebra artiniana

En la mayoría de los casos, el problema de encontrar el radical es harto complicado. Sin embargo, es mucho más sencillo calcular el radical de un álgebra

de dimensión finita sobre un cuerpo (o de forma más general, el radical de un álgebra artiniana).

Proposición 5.16. Si A es un álgebra artiniana a derecha o izquierda, entonces existe un número natural k tal que $J(A)^k = 0$.

Demostración. $J(A) \supseteq J(A)^2 \supseteq J(A)^3 \supseteq ...$ es una sucesión descendente de ideales biláteros, de forma que por la propiedad artiniana a derecha o a izquierda, existe un número natural k tal que $J(A)^k = J(A)^{k+1}$. Si podemos suponer que $J(A)^k$ es finitamente generado como A-módulo, entonces por el corolario 5.8 tenemos que $J(A)^k = 0$. Así, si A es noetheriano además de artiniano, la proposición es una aplicación sencilla del lema de Nakayama. Más adelante probaremos que A ha de ser necesariamente noetheriano, pero como para demostrarlo necesaremos esta proposición seguiremos adelante sin ello. Supongamos que $J(A)^k \neq 0$. En particular, el conjunto de ideales a derecha no nulos M de A tales que $MJ(A) = M$ incluye a $J(A)^k$. Por tanto, existe un M minimal con estas propiedades. Como $M = MJ(A)^2 = ... = MJ(A)^k$, existe algún $x \in M$ tal que $xJ(A)^k \neq 0$. Claramente, $xJ(A)^k$ es un ideal a derecha de A contenido en M, y $(xJ(A)^k)J(A) = xJ(A)^{k+1} = xJ(A)^k$. Del hecho de que M es minimal se sigue que $M = xJ(A)^k \subseteq xA = M$. Por tanto, M es finitamente generado, lo que contradice el lema de Nakayama, ya que $0 \neq M = MJ(A)$.

Corolario 5.17. Sea A un álgebra artiniana a derecha o a izquierda. Dado un ideal a derecha o a izquierda M de A, las siguientes condiciones son equivalentes.

(I). $M \subseteq J(A)$.

(II). Existe un número natural k tal que $M^k = 0$.

(III). Todos los elementos de M son nilpotentes.

Demostración. El hecho de que (I) implica (II) es consecuencia directa de la proposición anterior, (II) implica (III) trivialmente. Finalmente, (I) se sigue de (III) para cualquier álgebra por el corolario 5.13

5.5. Álgebras artinianas y noetherianas

Como ya adelantamos en la proposición del párrafo anterior, podremos demostrar que toda álgebra artiniana es noetheriana, lo cual será el principal resultado de esta sección. De hecho, podremos probar un resultado un poco más general.

Proposición 5.18. Sea A un álgebra artiniana a derecha o a izquierda. Si M es un A-módulo artiniano, entonces M es noetheriano.

Demostración. Denotemos $J = J(A)$. Como A es artiniana, existe un número natural k tal que $J^k = 0$ por la proposición 5.16. En particular, existe un $n \in \mathbb{N}$ mínimo tal que $MJ^n = 0$ (consideraremos el caso de módulos a derecha, el caso a izquierda es completamente análogo). Procederemos por inducción en n. Si $n = 0$, entonces $0 = MJ^0 = MA = M$, y el módulo cero es claramente noetheriano. Sea $n = 1$. La condición $MJ = 0$ implica que M se puede considerar como un módulo sobre el álgebra A/J. Como A/J es semisimple por el corolario 5.3, todo A/J-módulo es semisimple por la proposición 4.4 (usando el hecho de que coincide la semisimplicidad a derecha y a izquierda). Por tanto, $M_{A/J}$ es noetheriano por la proposición 3.29. Como $S(M_A) = S(M_{A/J})$ por el lema 3.1, M_A también es noetheriano. Supongamos que $n > 1$. El paso de inducción está basado en el lema 3.24. Denotamos $N = MJ^{n-1} < M$. N es artiniano y $NJ = 0$, por lo que en el caso $n = 1$, N es noetheriano. El módulo cociente M/N es también artiniano y $(M/N)J^{n-1} = 0$. Por la hipótesis de inducción, M/N es noetheriano. En consecuencia, M es noetheriano.

Corolario 5.19. Si la R-álgebra A es artiniana por la derecha (izquierda), entonces A es noetheriana por la derecha (izquierda).

Corolario 5.20. Si A es una R-álgebra artiniana por la derecha, entonces las siguientes condiciones sobre un A-módulo M son equivalentes.

(I). M es artiniano.

(II). M es noetheriano.

(III). M es finitamente generado.

Demostración. Por la proposición, (I) implica (II), y (III) se sigue de (II) por la proposición 3.29. Para la implicación restante, supongamos que $N = u_1A + ... + u_nA$. Entonces existe un homomorfismo de A-módulos suprayectivo de $\bigoplus_n A_A$ en M definido por

$$(x_1, ..., x_n) \mapsto \sum_{i=1}^{n} u_i x_i \tag{5.1}$$

Dado que A_A es artiniano, se sigue del lema 3.24 que $\bigoplus_n A_A$ es artiniano, y por tanto M es artiniano.

5.6. Álgebras nilpotentes

Otra aplicación más de la proposición 5.16 da una caracterización de las álgebras nilpotentes de dimensión finita. El resultado que probaremos en relación a ello aparece en uno de los últimos artículos de Wedderburn, pero se basa en resultados anteriores de Engel y Lie sobre álgebras de Lie nilpotentes y resolubles.

Para probar nuestro resultado necesitaremos de la proposición 3.29, del teorema de estructura de Wedderburn y de un resultado elemental previo acerca de la aplicación traza de las matrices. Si $\alpha = [\alpha_{ij}]$ es una matriz $n \times n$ con entradas en un cuerpo F, definimos la traza de α como

$$\mathrm{tr}\alpha = \sum_{i=1}^{n} \alpha_{ii} \tag{5.2}$$

Es claro que la traza es F-lineal de $M_n(F)$ en F solo con usar la definición. Además, si α es nilpotente ($\alpha^m = 0$), entonces el polinomio mínimo de α es X^k con $1 \leq k \leq m$ (ya que este polinomio divide a X^k), y su polinomio característico es $X^n - (\mathrm{tr}\alpha)X^{n-1} + ... = X^n$ (ya que el polinomio mínimo y el polinomio característico tienen los mismos factores irreducibles). Por tanto, tenemos que si α es nilpotente, entonces $\mathrm{tr}\alpha = 0$.

Lema 5.21. No existe ningún conjunto de matrices nilpotentes que generen $M_n(F)$ como F-espacio vectorial.

Demostración. En caso contrario, existirían matrices nilpotentes $\alpha_1, ...\alpha_r \in M_n(F)$ y escalares $b_1, ..., b_r \in F$ tales que $\epsilon_{11} = \alpha_1 b_1 + ... + \alpha_r b_r$. Por las propiedades de la traza que vimos anteriormente, esta ecuación lleva a contradicción, $1 = \text{tr}\epsilon_{11} = (\text{tr}\alpha_1)b_1 + ... + (\text{tr}\alpha_r)b_r = 0$ #

Proposición 5.22. Sea A una F-álgebra de dimensión finita. Supongamos que B es un subespacio de A cerrado bajo la multiplicación, y que está generado por un conjunto de elementos nilpotentes. Entonces $B^k = 0$ para algún $k \in \mathbb{N}$.

Demostración. Hallaremos dos resultados previos para facilitar la demostración. Asumiremos en primer lugar que

$$F \text{ es algebraicamente cerrado} \tag{5.3}$$

Para ver esto, sea $x_1, ..., x_m$ una F-base de A, con $x_j x_k = \sum_{i=1}^m x_i c_{ijk}$, $c_{ijk} \in F$. Denotamos la clausura algebraica de F por K. Formamos la K-álgebra $A' = x_1 K \oplus ... \oplus x_m K$ con la multiplicación en A' definida por las constantes de estructura $\{c_{ijk}\}$. Claramente, A es una subálgebra de $(A')_F$. Por tanto, B es una subálgebra de $(B')_F$, con $B' = BK$. Por tanto, $(B')^k = 0$ implica que $B^k = 0$. Queda señalar que B' satisface la misma hipótesis que B: B' es un K-subespacio de A', B' es cerrada bajo multiplicación y B' está generada por elementos nilpotentes. La siguiente simplificación que haremos es suponer que

$$B \text{ es un ideal de } A \tag{5.4}$$

Para lograr esta condición, basta reemplazar A por $B + 1_A F$. Como B es cerrado bajo la multiplicación, es trivialmente un ideal de $B + 1_A F$. Para completar la demostración, basta probar que

$$\text{si } A \text{ es semisimple, entonces } B = 0 \tag{5.5}$$

De hecho, podemos reemplazar A por el álgebra semisimple $A/J(A)$, y el ideal B de A por el ideal $(B + J(A))/J(A)$ de $A/J(A)$. Como $(B + J(A))/J(A)$ es una imagen homomorfa de B, está generada por elementos nilpotentes. Por tanto, (5.5) nos lleva a la conclusión de que $B + J(A) = J(A)$, esto es, $B \subseteq J(A)$. Por la proposición 5.16, $B^k \subseteq J(A)^k = 0$ para cierto $k \in \mathbb{N}$.

Solo nos queda, por tanto, probar (5.5), usando las hipótesis añadidas (5.3) y (5.4). Por el corolario 4.26, $A = A_1 \dot{+} ... \dot{+} A_t$ donde cada $A_i \cong M_{n_i}(F)$ es simple. Sea $\pi_i : A \to A_i$ el homomorfismo de proyección. Para cada i, $\pi_i(B)$ es un ideal de A_i, luego o bien $\pi_i(B) = 0$ o bien $\pi_i(B) = A_i$ por ser A_i simple. La segunda opción no se puede dar, ya que implicaría que $A_i \cong M_{n_i}(F)$ estaría generado por elementos nilpotentes, en contradicción con el lema anterior. Por tanto, $B \subseteq \text{Ker}\pi_i$ para todo i. Por tanto, $B \subseteq \bigcap_{i=1}^{t} \text{Ker}\pi_i = 0$, lo que prueba (5.5).

5.7. El radical de un álgebra de grupo

Con las herramientas que hemos obtenido, nos dedicaremos brevemente al problema de describir el radical de un álgebra de grupo. En concreto estudiaremos $J(FG)$ cuando F es un cuerpo y G un grupo finito. El teorema de Maschke nos dice que si la característica de F no divide al orden de G, entonces $J(FG) = 0$. Por tanto, supondremos que la característica de F es un primo p que divide a $n = |G|$. Obtendremos un resultado enunciado por Wallace que se basará en el resultado sobre álgebras nilpotentes que acabamos de probar.

Proposición 5.23. Sea F un cuerpo de característica prima p. Supongamos que G es un grupo finito que tiene un subgrupo normal p-Sylow H. El radical de Jacobson del álgebra de grupo FG es $J(FG) = \sum_{x \in H-\{1\}} (x-1)FG$.

Demostración. Denotaremos $A = FG$. Sabemos que el homomorfismo de proyección $\phi : G \to G/H$ se extiende de forma lineal a un homomorfismo de F-álgebras suprayectivo $\phi : A = FG \to F(G/H)$. Si $y_1, ..., y_m$ es una colección de representantes de clases laterales de H, esto es, $G = Hy_1 \dot{\cup} ... \dot{\cup} Hy_m$, y si $y \in G$, entonces $\phi(y) = \phi(y_i)$ si y solo si $y \in Hy_i$. Por tanto, dado $z = \sum_{y \in G} ya_y \in A$, tenemos $\phi(z) = \sum_{y \in G} \phi(y)a_y = \sum_{i=1}^{m} \phi(y_i)\left(\sum_{x \in H} a_{xy_i}\right)$. En particular, si $\phi(z) = 0$, entonces $\sum_{x \in H} a_{xy_i} = 0$ para $1 \leq i \leq m$. Esto implica que $a_{y_i} = -\sum_{x \in H-\{1\}} a_{xy_i}$, de forma que $z = \sum_{i=1}^{m} \sum_{x \in H-\{1\}} (x-1)y_i a_{xy_i} = \sum_{x \in H-\{1\}} (x-1)\left(\sum_{i=1}^{m} y_i a_{xy_i}\right) \in \sum_{x \in H-\{1\}} (x-1)A$. Análogamente, si $z \in \sum_{x \in H-\{1\}} (x-1)A$, entonces $\phi(z) \in \sum_{x \in H-\{1\}} (\phi(x) - \phi(1))\phi(A) = 0$. Por tanto, $\text{Ker}\phi = \sum_{x \in H-\{1\}} (x-1)A = J$. Con esto probamos que J es un ideal de A tal que $A/J \cong F(G/H)$. Como H es un p-subgrupo de Sylow de G, p no divide a $|G/H|$. Por tanto, $F(G/H)$ es semisimple por el teorema de Maschke. Esto implica que $J \supseteq J(A)$. Usaremos esto para

probar que $J^k = 0$ para cierto $k \in \mathbb{N}$. Denotamos $B = \sum_{x \in H-\{1\}}(x-1)F$. Claramente, B es un subespacio de A. Además, B es cerrado bajo la multiplicación, ya que $(x-1)(y-1) = (xy-1)-(x-1)-(y-1)$. Si $|H| = p^l$, entonces, dado que car$F = p$, $(x-1)^{p^l} = x^{p^l} - 1 = 0$ para todo $x \in H$. Por tanto, B está generado por elementos nilpotentes. Por la proposición 5.22 tenemos que $B^k = 0$ para cierto $k \in \mathbb{N}$. Con ello tenemos que $J^k = 0$ sin más que ver que $J = BA$ (trivial) y que $BA = AB$ (ya que $(x-1)y = y(y^{-1}xy-1)$ y $y^{-1}xy \in H$ para $x \in H$, $y \in G$ por la normalidad de H). Así, $J^k = (BA)^k = B^k A^k = 0A = 0$.

Corolario 5.24. Si H es un p-grupo finito y F es un cuerpo de característica p, entonces $J(FH) = \sum_{x \in H-\{1\}}(x-1)F$.

Demostración. Si $x, y \in H$, entonces $(x-1)y = (xy-1)-(y-1)$. Así, $\sum_{x \in H-\{1\}}(x-1)FH = \sum_{x \in H-\{1\}}(x-1)F$. Por tanto el corolario es consecuencia directa de la proposición.

5.8. Ideales en álgebras artinianas

Concluiremos la sección con algunos resultados sobre el retículo de ideales de un álgebra. En concreto, veremos que si A es semisimple, entonces $I(A)$ es distributivo, y con ello podremos determinar si $I(A)$ es distributivo sin más que estudiar el retículo de sub-bimódulos de $J(A)$, supuesto que $A/J(A)$ es semisimple.

Lema 5.25. Sea A un álgebra semisimple. Entonces,

(I). Si M es un ideal a derecha de A y N es un ideal a izquierda de A, entonces $MN = M \cap N$.

(II). $I(A)$ es un retículo distributivo.

Demostración. (I): $MN \subseteq M$ ya que $M < A_A$, y $MN \subseteq N$ ya que $N < {}_A A$. Por tanto, $MN \subseteq M \cap N$. Como A es semisimple, se sigue de la proposición 3.15 que $A_A = M \oplus P$ para cierto ideal a derecha P de A. Así, $N = AN = MN + PN \subseteq MN + P$. Por la ley modular, $N \cap M \subseteq (MN + P) \cap M = MN + (P \cap M) = MN$.

(II): Si I, J y K son ideales de A, entonces por (I) tenemos que $I \cap (J+K) = I(J+K) = IJ + IK = (I \cap J) + (I \cap K)$. Por tanto, $I(A)$ es distributivo.

Lema 5.26. Sea A un álgebra tal que $A/J(A)$ es semisimple. Entonces existen homomorfismos de retículos suprayectivos $\rho : I(A) \to I(A/J(A))$ y $\sigma : I(A) \to S({}_AJ(A)_A)$ (donde $S({}_AJ(A)_A)$ es el retículo de sub-bimódulos de $J(A)$), tal que si I y J son ideales de A que satisfacen $\rho(I) = \rho(J)$ y $\sigma(I) = \sigma(J)$ entonces $I = J$.

Demostración. Sea $\rho : A \to A/J(A)$ el homomorfismo de proyección. Por ser ρ suprayectiva, tenemos que $\rho(I) \lhd A/J(A)$ para todo $I \in I(A)$. Si I y J son ideales de A, entonces $\rho(I+J) = \rho(I) + \rho(J)$ y $\rho(I \cap J) \subseteq \rho(I) \cap \rho(J) = \rho(I)\rho(J) = \rho(IJ) \subseteq \rho(I \cap J)$ por el lema anterior. Por tanto, ρ es un homomorfismo de retículos. Por el teorema de correspondencia, todo ideal de $A/J(A)$ tiene la forma $I/J(A) = \rho(I)$ para cierto $I \in I(A)$, esto es, ρ es suprayectiva. Definimos $\sigma : I(A) \to S(J(A))$ por $\sigma(I) = I \cap J(A)$. Claramente, $\sigma(I \cap J) = \sigma(I) \cap \sigma(J)$ y $\sigma(I + J) \supseteq \sigma(I) + \sigma(J)$ para todo $I, J \in I(A)$. Si $x + y \in J(A)$, con $x \in I$, $y \in J$, entonces $\rho(x) - \rho(y) \in \rho(I) \cap \rho(J) = \rho(I \cap J)$. Esto es, $\rho(x) = -\rho(y) = \rho(z)$ para cierto $z \in I \cap J$. Por tanto, $x - z \in I \cap J(A) = \sigma(I)$ y $y + z \in J \cap J(A) = \sigma(J)$, de forma que $x + y = (x - z) + (y + z) \in \sigma(I) + \sigma(J)$. Con esto probamos que $\sigma(I+J) \subseteq \sigma(I) + \sigma(J)$, lo que demuestra que σ es un homomorfismo de retículos. Todo sub-bimódulo de $J(A)$ es un ideal de A, por lo que σ es suprayectivo. Finalmente, supongamos que $\rho(I) = \rho(J)$ y $\sigma(I) = \sigma(J)$. Si $x \in I$, existe $y \in J$ tal que $\rho(x) = \rho(y)$. Por tanto, $x - y \in (I + J) \cap J(A) = \sigma(I + J) = \sigma(I) + \sigma(J) = \sigma(J) \subseteq J$, y $x = (x - y) + y \in J$. Análogamente, si $x \in J$, entonces $x \in I$. Por tanto, $I = J$.

Proposición 5.27. Sea A un álgebra artiniana. El retículo de ideales de A es distributivo si y solo si el retículo $S(J(A))$ de sub-bimódulos de $J(A)$ es distributivo.

Demostración. Dado que $S(J(A))$ es un subretículo de $I(A)$, si $I(A)$ es distributivo $S(J(A))$ también lo será trivialmente. Análogamente, supongamos que $S(J(A))$ es distributivo. Si I, J y K son ideales de A, entonces $\sigma(I \cap (J + K)) = \sigma(I) \cap (\sigma(J) + \sigma(K)) = (\sigma(I) \cap \sigma(J)) + (\sigma(I) \cap \sigma(K)) = \sigma((I \cap J) + (I \cap K))$. De forma similar, se sigue del lema 5.25 que $\rho(I \cap (J + K)) = \rho((I \cap J) + (I \cap K))$. Por el lema 5.26, $I \cap (J + K) = (I \cap J) + (I \cap K)$.

En el formalismo de álgebra universal, el lema 5.26 afirmaría que $I(A)$ es un producto subdirecto de $I(A/J(A))$ y $S(J(A))$. En particular, $I(A)$ es isomorfo a un subretículo del producto de $I(A/J(A))$ y $S(J(A))$. Esta idea es la base detrás de la proposición.

6. Módulos indescomponibles

Tras estudiar una de las estructuras de álgebra más sencillas, las álgebras semisimples, en esta sección intentaremos ampliar nuestro estudio a álgebras más generales. Intentaremos encontrar un análogo general al teorema de estructura de Wedderburn, para lo cual nuestro análogo a los módulos simples serán lo que llamaremos módulos indescomponibles.

6.1. Descomposiciones directas

Durante toda la sección, supondremos que A es una R-álgebra con R un anillo, que no jugará un papel importante en la teoría.

Definición 6.1. Un A-módulo N es indescomponible si $N \neq 0$ y los únicos sumandos directos de N son 0 y N, esto es, si $N = P \oplus Q$, entonces o bien $P = 0$ o bien $Q = 0$. Un módulo M es descomponible si $M = M_1 \oplus M_2$ con M_1 y M_2 módulos distintos de cero. Así, el módulo cero no es ni descomponible ni indescomponible.

Proposición 6.2. Si M es un A-módulo artiniano o noetheriano, entonces se puede expresar M como suma directa finita de A-módulos indescomponibles.

Demostración. Si $M = 0$, entonces la proposición es cierta por la convención de que la suma vacía es 0. Supongamos que $M \neq 0$. Es fácil observar en primer lugar que existe un sumando directo indescomponible de M. Efectivamente, si N es minimal entre los sumandos no nulos de M, entonces N es trivialmente indescomponible. La existencia de un N minimal es evidente si M es artiniano. Si M es noetheriano, usamos que el complemento de cualquier sumando directo maximal es minimal. Iterando recursivamente este procedimiento, y usando el hecho de que las propiedades artiniana y noetheriana se heredan por submódulos, tenemos que

$$M = N_1 \oplus M_1 = N_1 \oplus N_2 \oplus M_2 = N_1 \oplus N_2 \oplus N_3 \oplus M_3 = \ldots \tag{6.1}$$

con cada N_i indescomponible y $M_1 \supset M_2 \supset M_3 \supset \ldots$. Esta sucesión de descomposiciones terminará en un paso k solo si $M_k = 0$, en cuyo caso $M = N_1 \oplus \ldots \oplus N_k$.

O bien la condición de cadena ascendente aplicada a $M_1 \supset M_2 \supset M_3 \supset \ldots$ o la descendente aplicada a $N_1 \subset N_1 + N_2 \subset N_1 + N_2 + N_3 \subset \ldots$ lleva a que el proceso ha de terminar en un número finito de pasos.

6.2. Álgebras locales

Es trivial que los módulos simples son indescomponibles. El recíproco es cierto para módulos sobre álgebras semisimples, pero no en general. Para las álgebras artinianas, existe una caracterización de los módulos indescomponibles y finitamente generados en términos de sus álgebras de endomorfismos de forma análoga a la caracterización de módulos simples a través del lema de Schur.

Definición 6.3. Se dice que un álgebra A es un álgebra local si $A/J(A)$ es un álgebra de división.

Como consecuencia directa, si A es local, entonces $1_A \neq 0$, por lo que A es no trivial.

Proposición 6.4. Dada un álgebra no trivial A, las siguientes condiciones son equivalentes.

(I). A es un álgebra local.

(II). $A - A^o \subseteq J(A)$.

(III). $A - A^o$ es cerrado bajo la suma.

Demostración. (I) $\Rightarrow$ (II). Si $x \in A - J(A)$, por (I) existe un $y \in A$ tal que $xy - 1 \in J(A)$ y $yx - 1 \in J(A)$. Por tanto, por la proposición 5.11, $xy = 1 + (xy - 1) \in A^o$. Análogamente, $yx \in A^o$. Se sigue por tanto que $x \in A^o$.

(II) $\Rightarrow$ (III). Dado que A es no trivial, es claro por la proposición 5.11 que ninguna unidad de A pertenece a $J(A)$. Así, $J(A) \cap A^o = \varnothing$. Por tanto, (II) es equivalente a que $A - A^o = J(A)$, y de esta forma (III) es consecuencia de que $J(A)$ es un ideal.

(III) $\Rightarrow$ (I). Supongamos que $x \in A - J(A)$. Por la proposición 5.11, existen elementos y y z en A tales que $1 + xy \in A - A^o$ y $1 + zx \in A - A^o$. Por tanto,

$xy \in A^o$ y $zx \in A^o$, ya que en otro caso $1 \in A - A^o$ por (III). Así, x tiene inversa tanto por la derecha como por la izquierda en A, de forma que $x \in A^o$. Con esto probamos que $A - J(A) \subseteq A^o$, con lo que es claro que $A/J(A)$ es un álgebra de división.

Corolario 6.5. Sea A un álgebra tal que todo elemento no unidad de A es nilpotente. Entonces A es un álgebra local.

Demostración. Sea $0 \neq x \in A - A^o$. Por la suposición, $x^k = 0$ para algún número natural mínimo $k > 1$. Entonces, $xy \in A - A^o$ para todo $y \in A$. De otra forma, $x^{k-1}(xy) = 0$ implicaría $x^{k-1} = 0$, lo que contradice la minimalidad de k. Así, por hipótesis, todo elemento de xA es nilpotente, de forma que $x \in xA \subseteq J(A)$ por el corolario 5.13. Con esto probamos que $A - A^o \subseteq J(A)$, por lo que A es local usando la proposición anterior.

Corolario 6.6. Si N es un A-módulo tal que $E_A(N)$ es un álgebra local, entonces N es indescomponible.

Demostración. La hipótesis de que $E_A(N)$ sea local incluye la condición de que $\mathrm{id}_N \neq 0$, por lo que $N \neq 0$. Si $N = P \oplus Q$ con las proyecciones asociadas $\pi : N \to P$ y $\rho : N \to Q$, entonces, como $\pi + \rho = \mathrm{id}_N$ y $E_A(N)$ es local, o π o ρ será una unidad por la proposición. Como $\pi^2 = \pi$ y $\rho^2 = \rho$, se sigue que $\pi = \mathrm{id}_N$ o $\rho = \mathrm{id}_N$, por lo que $Q = 0$ o $P = 0$.

6.3. Lema de Fitting

Buscaremos ahora probar el recíproco del corolario 6.6. El resultado correspondiente se conoce como lema de Fitting, y será de capital importancia en la teoría de álgebras. Probaremos antes un resultado previo que también será relevante.

Lema 6.7. Sea M un A-módulo, y supongamos que $\phi \in E_A(M)$. Si se cumple cualquiera de las siguientes hipótesis, entonces ϕ es un automorfismo.

(I). M es noetheriano y ϕ suprayectivo.

(II). M es artiniano y ϕ inyectivo.

Demostración. Supongamos que M es noetheriano y ϕ suprayectivo. Como $0 \subseteq \text{Ker}\phi \subseteq \text{Ker}\phi^2 \subseteq ...$, la condición de cadena ascendente implica que $\text{Ker}\phi^n = \text{Ker}\phi^{n+1}$ para cierto $n \in \mathbb{N}$. Esto es, $(\phi^n)^{-1}(\text{Ker}\phi) = (\phi^{n+1})^{-1}(0) = \text{Ker}\phi^{n+1} = \text{Ker}\phi^n = (\phi^n)^{-1}(0)$. Como ϕ es suprayectiva, también lo es ϕ^n. Por tanto, $\text{Ker}\phi = \phi^n(\phi^n)^{-1}(\text{Ker}\phi) = \phi^n(\phi^n)^{-1}(0) = 0$. La demostración con la condición (II) es análoga.

Teorema 6.8. Lema de Fitting. Sea M un A-módulo artiniano y noetheriano. Si $\phi \in E_A(M)$, entonces existe una descomposición $M = P \oplus Q$ tal que

(I). $\phi(P) \subseteq P$ y $\phi(Q) \subseteq Q$.

(II). $\phi|_P$ es un automorfismo.

(III). $\phi|_Q$ es nilpotente.

Demostración. La hipótesis de que M es artiniano y noetheriano aplicada a las cadenas $M \supseteq \phi(M) \supseteq \phi^2(M) \supseteq ...$ y $0 \subseteq \text{Ker}\phi \subseteq \text{Ker}\phi^2 \subseteq ...$ lleva a que existe un $m \in \mathbb{N}$ tal que $\phi^n(M) = \phi^m(M)$ y $\text{Ker}\phi^n = \text{Ker}\phi^m$ para todo $n \geq m$. Definimos $P = \phi^m(M)$ y $Q = \text{Ker}\phi^m$. Entonces, $\phi(P) = \phi^{m+1}(M) = \phi^m(M) = P$, y $\phi(Q) = \phi(\text{Ker}\phi^m) = \phi(\text{Ker}\phi^{m+1}) \subseteq \text{Ker}\phi^m = Q$. Usando el lema anterior, $\phi|_P$ es un automorfismo. Además, $\phi^m(Q) = \phi^m((\phi^m)^{-1}(0)) = 0$, de forma que $\phi|_Q$ es nilpotente. Tenemos también que $P \cap Q = 0$, ya que $\phi|_{P\cap Q}$ sería tanto inyectiva como nilpotente. Finalmente, $M = (\phi^m)^{-1}(\phi^m(M)) = (\phi^m)^{-1}(\phi^{2m}(M)) = (\phi^m)^{-1}(\phi^m(\phi^m(M))) = \phi^m(M) + \text{Ker}\phi^m = P + Q$.

Corolario 6.9. Si el A-módulo M es artiniano y noetheriano, entonces M es indescomponible si y solo si $E_A(M)$ es un álgebra local.

Demostración. Si $E_A(M)$ es local, entonces M es indescomponible por el corolario 6.6. Supongamos que M es indescomponible. Por el lema de Fitting, todo elemento de $E_A(M)$ es nilpotente o una unidad. Por tanto, $E_A(M)$ es un álgebra local por el corolario 6.5.

El caso que más nos influirá será en el que A es artiniano a derecha y M es un A-módulo a derecha finitamente generado. Por el corolario 5.20, esto garantizará que M será artiniano y noetheriano.

6.4. Teorema de Krull-Schmidt

Estudiaremos ahora la unicidad de las descomposiciones directas. Para ello, nuestro resultado principal será la generalización de Azumaya del teorema clásico de Krull y Schmidt. Para ello, necesitaremos dos resultados previos.

Lema 6.10. Dada una sucesión exacta $0 \to N \xrightarrow{\phi} M \xrightarrow{\psi} P \to 0$ de A-módulos, las siguientes condiciones son equivalentes.

(I). Existe $\chi \in \mathrm{Hom}_A(P,M)$ tal que $\psi\chi = \mathrm{id}_P$.

(II). Existe $\theta \in \mathrm{Hom}_A(M,N)$ tal que $\theta\phi = \mathrm{id}_N$.

En ese caso, $M = \mathrm{Im}\chi \oplus \mathrm{Ker}\psi = \mathrm{Im}\phi \oplus \mathrm{Ker}\theta$.

Demostración. Si se cumple (I), entonces $u = \chi\psi u + (u - \chi\psi u)$ y $\psi(u - \chi\psi u) = \psi u - \psi u = 0$ para todo $u \in M$. Por tanto, $M = \mathrm{Im}\chi + \mathrm{Ker}\psi$. Además, $\mathrm{Ker}\psi \cap \mathrm{Im}\chi = \mathrm{Ker}(\psi|_{\mathrm{Im}\chi}) = 0$ ya que $\psi\chi = \mathrm{id}_P$. Tenemos también que, como $\mathrm{Im}\phi = \mathrm{Ker}\psi$ y ϕ es inyectivo, que $\theta u = \phi^{-1}(u - \chi\psi u)$ define un homomorfismo de M en N tal que $\theta\phi v = \phi^{-1}\phi v = v$ para todo $v \in N$. La demostración de que (II) implica (I) y $M = \mathrm{Im}\phi \oplus \mathrm{Ker}\theta$ es análoga.

Si se cumplen las condiciones del lema, se dice que $0 \to N \to M \to P \to 0$ es una sucesión exacta escindida. Además, si se satisface (I), se dice que ψ es una suprayección de escisión, y si se cumple (II) se dice que ϕ es una inyección de escisión.

Lema 6.11. Sean $M = M_1 \oplus M_2 = N_1 \oplus N_2$ sumas directas de descomposiciones del A-módulo M. Supongamos que existe un automorfismo ϕ de M, con

$$\phi = \begin{bmatrix} \phi_{11} & \phi_{12} \\ \phi_{21} & \phi_{22} \end{bmatrix} \in \begin{bmatrix} \mathrm{Hom}_A(M_1,N_1) & \mathrm{Hom}_A(M_2,N_1) \\ \mathrm{Hom}_A(M_1,N_2) & \mathrm{Hom}_A(M_2,N_2) \end{bmatrix} \tag{6.2}$$

tal que ϕ_{11} es un isomorfismo. Entonces $M_2 \cong N_2$.

Demostración. Claramente,

$$\begin{bmatrix} \mathrm{id}_{N_1} & 0 \\ -\phi_{21}\phi_{11}^{-1} & \mathrm{id}_{N_2} \end{bmatrix}, \quad \begin{bmatrix} \mathrm{id}_{M_1} & -\phi_{11}^{-1}\phi_{12} \\ 0 & \mathrm{id}_{M_2} \end{bmatrix} \tag{6.3}$$

son automorfismos de M. Como ϕ es un automorfismo, también lo es

$$\begin{bmatrix} \mathrm{id}_{N_1} & 0 \\ -\phi_{21}\phi_{11}^{-1} & \mathrm{id}_{N_2} \end{bmatrix} \begin{bmatrix} \phi_{11} & \phi_{12} \\ \phi_{21} & \phi_{22} \end{bmatrix} \begin{bmatrix} \mathrm{id}_{M_1} & -\phi_{11}^{-1}\phi_{12} \\ 0 & \mathrm{id}_{M_2} \end{bmatrix} = \begin{bmatrix} \phi_{11} & -0 \\ 0 & \psi \end{bmatrix} \tag{6.4}$$

con $\psi = \phi_{22} - \phi_{21}\phi_{11}^{-1}\phi_{12} \in \mathrm{Hom}_A(M_2, N_2)$. Por tanto, ψ es también un isomorfismo.

Proposición 6.12. Sea A una R-álgebra. Supongamos que M y N son A-módulos a derecha con $M = M_1 \oplus ... \oplus M_r$, $N = N_1 \oplus ... \oplus N_s$, con $E_A(M_i)$ y $E_A(N_j)$ álgebras locales para todo i y j. Si $M \cong N$, entonces $r = s$ y existe una permutación σ tal que $M_i \cong N_{\sigma(i)}$ para $1 \leq i \leq r$.

Demostración. Usaremos inducción en r. Para $r = 0$, tenemos $M = 0$. Para el paso base de la inducción, $N \cong M = 0$, de forma que $s = 0$ (notemos que la definición de álgebra local implica la no trivialidad, por lo que el que $E_A(N_j)$ sea local implica que $N_j \neq 0$). Supongamos que $r > 0$ y que la proposición es válida para módulos que se pueden expresar como suma directa de menos de r factores que tienen álgebras de endomorfismos locales. Sin pérdida de generalidad, supongamos que $N = M$, sin más que transferir la descomposición de N a M utilizando el isomorfismo entre ambas. Así, tenemos

$$M = M_1 \oplus ... \oplus M_r = N_1 \oplus ... \oplus N_s \tag{6.5}$$

Sean $\pi_i : M \to M_i$, $\kappa_i : M_i \to M$, $\rho_j : M \to N_j$, $\lambda_j : N \to M$ las proyecciones e inyecciones canónicas asociadas a las descomposiciones de M. Entonces, $\mathrm{id}_M = \lambda_1\rho_1 + ... + \lambda_s\rho_s$ y $\mathrm{id}_{M_1} = \pi_1\kappa_1 = \sum_{j=1}^{s} \pi_1\lambda_j\rho_j\kappa_1$. Como $E_A(M_1)$ es un álgebra local, se sigue de la proposición 6.4 que $\phi = \pi_1\lambda_j\rho_j\kappa_1$ es una unidad de $E_A(M_1)$ para algún índice j. Para simplificar la notación, ordenaremos la descomposición $N_1 \oplus ... \oplus N_s$ de forma que $j = 1$. Sea $\psi = \phi^{-1}\pi_1\lambda_1 \in \mathrm{Hom}_A(N_1, M_1)$ y $\chi = \rho_1\kappa_1 \in \mathrm{Hom}_A(M_1, N_1)$ de forma que $\psi\chi = \mathrm{id}_{M_1}$. Se sigue del 6.10 que $N_1 = \mathrm{Ker}\psi \oplus \mathrm{Im}\chi$. Sin embargo, como $E_A(N_1)$ es local, N_1 es indescomponible por el corolario 6.6. Por tanto, $N_1 = \mathrm{Im}\chi$ y $\chi = \rho_1\kappa_1$ es un isomorfismo. Denotamos $M' = M_2 \oplus ... \oplus M_r$ y $N' = N_2 \oplus ... \oplus N_s$ de forma que $M = M_1 \oplus M' = N_1 \oplus N'$ con las correspondientes proyecciones e inyecciones canónicas $\pi_1 : M \to M_1$,

$\pi' : M \to M'$, $\kappa_1 : M_1 \to M$, $\kappa' : M' \to M$, $\rho_1 : M \to N_1$, $\rho' : M \to N'$, $\lambda_1 : N_1 \to M$, $\lambda' : N' \to M$. La matriz

$$\begin{bmatrix} \rho_1\kappa_1 & \rho_1\kappa' \\ \rho'\kappa_2 & \rho'\kappa' \end{bmatrix} \tag{6.6}$$

se corresponde con la descomposición de los isomorfismos $M_1 \oplus M' \to M$ y $M \to N_1 \oplus N'$ (definidos por $(u_1, u') \mapsto u_1 + u'$ y $v \mapsto (\rho_1 v, \rho' v)$), de forma que es un isomorfismo. Como $\rho_1\kappa_1$ es también un isomorfismo, usando el lema 6.11 tenemos que $M_2 \oplus ... \oplus M_r = M' \cong N' = N_2 \oplus ... \oplus N_s$. Aplicamos ahora la hipótesis de inducción a M' y N' y con ello completamos la demostración.

Corolario 6.13. Si M es un A-módulo a derecha artiniano y noetheriano, entonces $M = M_1 \oplus ... \oplus M_r$ con cada M_i un A-módulo indescomponible. Esta descomposición es única salvo isomorfismos.

Esto es consecuencia inmediata de la proposición anterior, la proposición 6.2 y el corolario 6.9. El teorema de Krull-Schmidt clásico es una generalización de este corolario a grupos con operadores.

Corolario 6.14. Si A es una R-álgebra artiniana a derecha, entonces todo A-módulo finitamente generado es unívocamente (salvo isomorfismos) una suma directa finita de A-módulos indescomponibles.

Y este último corolario es consecuencia inmediata del anterior y del corolario 5.20.

6.5. Representaciones de álgebras

Finalmente, con todos los conceptos y resultados que hemos ido recopilando, podemos pasar a definir y trabajar con las representaciones de álgebras. En este caso, nos limitaremos a las álgebras sobre un cuerpo F, ya que la mayoría de sus aplicaciones cumplen esta restricción.

Definición 6.15. Una representación matricial de una F-álgebra A es un homomorfismo de álgebras θ de A en la F-álgebra de matrices $n \times n$ con entradas en el cuerpo F.

El número natural n se llama grado de θ, y lo denotaremos como $\deg\theta$.

Una representación θ de A es fiel si $\mathrm{Ker}\theta = 0$. En ese caso, $\dim_F A \leq \dim_F M_n(F) = n^2$, con $n = \deg\theta$. En particular, A no puede tener una representación fiel si es de dimensión infinita.

Introduciremos ahora la noción de morfismo entre representaciones. Sean θ y ψ dos representaciones del álgebra A con grados n y m respectivamente. Una matriz α $n \times m$ entrelaza θ y ψ si $\theta(x)\alpha = \alpha\psi(x)$ para todo $x \in A$. Las matrices de entrelazamiento juegan el papel de morfismos. Por ello, utilizaremos la notación $\alpha : \theta \to \psi$ para referirnos a que α entrelaza θ y ψ. Si $\alpha : \theta \to \psi$ y $\beta : \psi \to \chi$ son matrices que entrelazan representaciones de A, entonces $\theta(x)\alpha\beta = \alpha\psi(x)\beta = \alpha\beta\chi(x)$ para todo $x \in A$. Así, el producto matricial $\alpha\beta$ entrelaza θ y χ. Esto muestra que la composición de morfismos se puede tomar como la multiplicación matricial en orden inverso, $\alpha\beta = \beta \circ \alpha$. La asociatividad de la composición se cumple de forma automática.

Finalmente, la matriz identidad ι_n claramente entrelaza una representación de grado n consigo misma, y tiene las propiedades usuales de un morfismo identidad. Se puede observar que las representaciónes de un álgebra A junto con las matrices de entrelazamiento forman una categoría. Sin embargo, es importante señalar que no es adecuado identificar los morfismos con matrices, sino con tripletas (θ, α, ψ) donde $\alpha : \theta \to \psi$, ya que una misma matriz puede entrelazar diferentes pares de representaciones y no entrelazar otras. No obtante, prescindiremos de esta precisión en nuestra notación.

Se dice que dos representaciones θ y ψ de A son equivalentes si son isomorfas en el sentido de que existen morfismos $\alpha : \theta \to \psi$ y $\beta : \psi \to \theta$ cuya composición en ambos órdenes es la identidad. Se puede probar fácilmente que θ y ψ son equivalentes si y solo si $\deg\theta = \deg\psi$ y existe una matriz cuadrada no singular α que entrelaza θ y ψ. Dicho de otro modo, $\psi(x) = \alpha^{-1}\theta(x)\alpha$ para todo $x \in A$. Lo denotaremos $\theta \cong \psi$. Es claro que $\cong$ es una relación de equivalencia.

Dado θ una representación A con $\deg\theta = n$, podemos utilizarlo para definir un A-módulo M_θ. Como F-espacio, $M_\theta = \bigoplus_n F$. La operación escalar de A en M_θ viene dada por

$$[a_1, ..., a_n]x = [a_1, ..., a_n]\theta(x) \tag{6.7}$$

es decir, el producto matricial por la derecha, para todo $x \in A$. Se puede calcular de forma directa que M_θ es efectivamente un A-módulo por la derecha. Es claro también que

$$\dim_F M_\theta = \deg\theta, \quad \operatorname{ann} M_\theta = \operatorname{Ker}\theta \tag{6.8}$$

La correspondencia $M : \theta \mapsto$ lleva por tanto las representaciones en A-módulos a derecha. Efectivamente, supongamos que $\alpha : \theta \to \psi$. Definimos $\mu_\alpha : M_\theta \to M_\psi$ por $\mu_\alpha([a_1,...,a_n]) = [a_1,...,a_n]\alpha$. Claramente, μ_α es una aplicación F-lineal de M_θ en M_ψ, y $\mu_\alpha([a_1,...,a_n]x) = \mu_\alpha([a_1,...,a_n]\theta(x)) = [a_1,...,a_n]\theta(x)\alpha = [a_1,...,a_n]\alpha\psi(x) = \mu_\alpha([a_1,...,a_n])x$. Esto es, $\mu_\alpha \in \operatorname{Hom}_A(M_\theta, M_\psi)$. Es claro que $\mu_\alpha\mu_\beta = \mu_{\beta\alpha} = \mu_{\alpha\circ\beta}$. Así, las aplicaciones $\theta \mapsto M_\theta$, $\alpha \mapsto \mu_\alpha$ constituyen un funtor entre las representaciones de A y los A-módulos a derecha.

Proposición 6.16. Sean θ y ψ representaciones de la F-álgebra A. Entonces,

(I). Si $\alpha : \theta \to \psi$ y $\beta : \theta \to \psi$ satisfacen $\mu_\alpha = \mu_\beta$, entonces $\alpha = \beta$.

(II). Si $\phi \in \operatorname{Hom}_A(M_\theta, M_\psi)$, entonces existe $\alpha : \theta \to \psi$ tal que $\phi = \mu_\alpha$.

(III). Si M es un A-módulo a derecha tal que $0 < \dim_F M = n \in \mathbb{N}$, entonces existe una representación χ de A tal que $M \cong M_\chi$.

Demostración. Si $\mu_\alpha = \mu_\beta$, entonces $[a_1,...,a_n]\alpha = [a_1,...,a_n]\beta$ para todo $a_1,...,a_n \in F$. Claramente, esto solo puede ocurrir si $\alpha = \beta$. Si $\phi \in \operatorname{Hom}_A(M_\theta, M_\psi)$, en particular ϕ es una aplicación lineal entre dos espacios vectoriales fila. Por tanto, existe una matriz α tal que $\phi([a_1,...,a_n]) = [a_1,...,a_n]\alpha$ para todo $a_1,...,a_n$ en F. Además, ϕ es un homomorfismo de A-módulos. Así, $[a_1,...,a_n]\theta(x)\alpha = \phi([a_1,...,a_n]x) = \phi([a_1,...,a_n])x = [a_1,...,a_n]\alpha\psi(x)$ para todo $a_1,...,a_n \in F$, de forma que α entrelaza θ y ψ. Por definición, $\mu_\alpha = \phi$.

Para probar (III), tomamos una base $u_1,...,u_n$ de M. Definimos $\chi : A \to M_n(F)$ por la condición

$$[u_1,...,u_n]x = [u_1,...,u_n]\chi(x)^t \tag{6.9}$$

donde el superíndice t denota la trasposición de matrices. Se puede calcular con facilida que $\chi(x+y) = \chi(x) + \chi(y)$, $\chi(xa) = \chi(x)a$ y $\chi(xy) = \chi(x)\chi(y)$ para

todo $x, y \in A$, $a \in F$. Por tanto, χ es una representación de A. Definimos $\phi : M \to \bigoplus_n F = M_\chi$ por $\phi(v) = [a_1, ..., a_n]$ donde $v = u_1 a_1 + ... + u_n a_n$. Trivialmente, ϕ es un isomorfismo de F-espacios caracterizado por $v = [u_1, ..., u_n]\phi(v)^t$. Si $v \in M$ y $x \in A$, entonces $[u_1, ..., u_n]\phi(vx)^t = vx = [u_1, ..., u_n]\phi(v)^t x = [u_1, ..., u_n]x\phi(v)^t = [u_1, ..., u_n]\chi(x)^t\phi(v)^t$ ya que $F \subseteq Z(A)$. Por tanto, $\phi(vx) = \phi(v)\chi(x) = \phi(v)x$, esto es, ϕ es un isomorfismo de A-módulos.

Corolario 6.17. Si θ y ψ son representaciones de A, entonces $\theta \cong \psi$ si y solo si $M_\theta \cong M_\psi$.

Demostración. Si $\alpha : \theta \to \psi$ es no singular, entonces $\mu_\alpha : M_\theta \to M_\psi$ es un homomorfismo de módulos tal que $\mu_{\alpha^{-1}} = (\mu_\alpha)^{-1}$. Recíprocamente, un isomorfismo de M_ψ en M_ψ viene dado por μ_α donde $\alpha : \theta \to \psi$ es no singular.

Corolario 6.18. Sea A una F-álgebra tal que $\dim_F A = n$. Entonces existe una representación fiel θ de A tal que $\deg\theta = n$.

Demostración. Por la proposición 6.16, existe una representación θ de A tal que $A_A \cong M_\theta$. Así, $\deg\theta = \dim_F M_\theta = \dim_F A = n$, y $\mathrm{Ker}\theta = \mathrm{ann}M_\theta = \mathrm{ann}A_A = 0$.

Las representaciones de álgebras tienen un importante paralelismo con las representaciones de grupos. Si G es un grupo y F un cuerpo, una F-representación de G es un homomorfismo de grupos θ de G en $GL_n(F)$, con $GL_n(F) = M_n(F)^o$ el grupo lineal general de matrices $n \times n$ no singulares con entradas en F. Al igual que en el caso de álgebras, las F-representaciones de G forman una categoría en la que los morfismos son las tripletas (θ, α, ψ) tales que α es una matriz que entrelaza θ y ψ, $\theta(x)\alpha = \alpha\psi(x)$ para todo $x \in G$.

La conexión más importante de las F-representaciones de G es que son isomorfas a las representaciones del álgebra de grupo FG. Además, si θ es un homomorfismo de grupos de G en $GL_n(F)$, entonces θ tiene una extensión única a un homomorfismo de álgebras de FG en $M_n(F)$. Recíprocamente, se puede restringir cualquier homomorfismo de álgebras de FG en $M_n(F)$ a un homomorfismo de grupos de G en $GL_n(F)$. Así, existe una correspondencia biyectiva natural entre las F-representaciones de G y las representaciones de FG, que además es un isomorfismo.

6.6. Representaciones indescomponibles e irreducibles

Si θ y ψ son representaciones del álgebra A con $\deg\theta = n$ y $\deg\psi = m$, entonces la suma directa de θ y ψ es la aplicación $\theta \oplus \psi : A \to M_{n+m}(F)$ definida por

$$(\theta \oplus \psi)(x) = \begin{bmatrix} \theta(x) & 0 \\ 0 & \psi(x) \end{bmatrix} \tag{6.10}$$

Claramente, $\theta \oplus \psi$ es una representación de grado $n+m$.

Se dice que una representación ψ de A es indescomponible si no se puede expresar como suma directa de dos representaciones (de grado positivo). Podremos encontrar un análogo del teorema de Krull-Schmidt para representaciones.

Lema 6.19. Si θ y ψ son representaciones de A, entonces $M_{\theta\oplus\psi} \cong M_\theta \oplus M_\psi$.

Demostración. La aplicación $([a_1,...,a_n],[b_1,...,b_m]) \mapsto [a_1,...,a_n,b_1,...,b_m]$ es trivialmente un isomorfismo de F-espacios de $M_\theta \oplus M_\psi$ en $M_{\theta\oplus\psi}$, y las operaciones escalares de estos módulos están definidas de forma que hacen de la aplicación un isomorfismo de módulos.

Proposición 6.20. (I). θ es una representación indescomponible de A si y solo si M_θ es un A-módulo indescomponible.

(II). Toda representación θ de A es equivalente a una suma directa finita de representaciones indescomponibles.

(III). Si $\psi_1 \oplus ... \oplus \psi_r \cong \chi_1 \oplus ... \oplus \chi_s$ con cada ψ_i y χ_j indescomponibles, entonces $r = s$ y existe una permutación σ tal que $\chi_i \cong \psi_{\sigma(i)}$ para todo i.

Demostración. Si $\theta = \psi \oplus \chi$, entonces $M_\theta \cong M_\psi \oplus M_\chi$ por el lema anterior. Así, M_θ no es indescomponible. Recíprocamente, si $M_\theta = N_1 \oplus N_2$ con $N_1, N_2 \neq 0$, entonces por la proposición 6.16 tenemos que $M_\theta \cong M_\psi \oplus M_\chi$ para ciertas representaciones ψ y χ. Por el lema anterior y el corolario 6.17, $\theta \cong \psi \oplus \chi$. Así, θ no es indescomponible. Para probar (II), observemos que M_θ es de dimensión finita, y por tanto artiniano y noetheriano. Por la proposición 6.2, $M_\theta = N_1 \oplus ... \oplus N_r$ con los N_i A-módulos indescomponibles de dimensión finita. Por la proposición 6.16, existen representaciones ψ_i de A tales que $N_i \cong M_\psi$.

Por tanto, $\theta \cong \psi_1 \oplus ... \oplus \psi_r$. Aplicando (I), cada ψ_i es indescomponible. La unicidad de (III) se obtiene de (I) y del corolario 6.13: $\psi_1 \oplus ... \oplus \psi_r \cong \chi_1 \oplus ... \oplus \chi_s$ implica que $M_{\psi_1} \oplus ... \oplus M_{\psi_r} \cong M_{\chi_1} \oplus ... \oplus M_{\chi_s}$ con cada sumando indescomponible. Así, $r = s$ y $M_{\chi_i} \cong M_{\psi_{\sigma(i)}}$ (y por tanto $\chi_i \cong \psi_{\sigma(i)}$ por el corolario 6.17) para una cierta permutación σ.

Dos representaciones cualesquiera de A están siempre entrelazadas por una matriz cero de dimensión adecuada. En algunos casos, es el único entrelazamiento posible.

Proposición 6.21. Dada una representación θ de la F-álgebra A, las siguientes condiciones son equivalentes.

(I). θ es equivalente a una representación ψ de A talq ue para todo $x \in A$, $\psi(x)$ tiene la forma

$$\begin{bmatrix} \psi_1(x) & * \\ 0 & \psi_2(x) \end{bmatrix} \tag{6.11}$$

donde ψ_1 y ψ_2 son representaciones de A.

(II). Existe una representación χ de A con $\deg\chi < \deg\theta$, y un entrelazamiento no nulo $\alpha : \theta \to \chi$.

(III). M_θ no es simple.

Demostración. Si se satisface (I), entonces (II) es cierta con $\chi = \psi_1$. Además, si $r = \deg\psi_1$, $\deg\theta = n$ y 0 es la matriz cero $(n-r) \times r$, entonces $\begin{bmatrix} \iota_r \\ 0 \end{bmatrix}$ entrelaza ψ y ψ_1. Como $\theta \cong \psi$, existe un entrelazamiento no nulo $\alpha = \theta \to \psi_1$.

Supongamos que se satisface (II). Por la proposición 6.16, $\mu_\alpha : M_\theta \to M_\chi$ es un homomorfismo no nulo. Si M_θ fuera simple, entonces μ_α sería inyectiva por el lema de Schur, por lo que $\deg\theta = \dim_F M_\theta \leq \dim_F M_\chi = \deg\chi$, lo que contradice la hipótesis. Por tanto, M_θ no es simple y (II) implica (III).

Si $M\theta$ no es simple, entonces existe un submódulo N de M_θ tal que $0 \neq N \subset M_\theta$. Elegimos una base como F-espacio $u_1, ..., u_r, u_{r+1}, ..., u_n$ de M_θ de forma que $u_{r+1}, ..., u_n$ sea una base de N. Así, $1 \leq r \leq n-1$. Definimos $\psi : A \to M_n(F)$ por $[u_1, ..., u_n]x = [u_1, ..., u_n]\psi(x)^t$. En la demostración de la proposición 6.16

observamos que ψ es una representación de A tal que $M_\psi \cong M_\theta$. Por tanto, $\psi \cong \theta$ por el corolario 6.17. Sea $\psi(x) = [a_{ij}]$, de forma que por la definición, $u_i x = \sum_{j=1}^{n} u_i a_{ij}$. Como $N < M_\theta$ y $u_{r+1}, ..., u_n \in N$, se sigue que $a_{ij} = 0$ si $1 \leq j \leq r < i \leq n$. Dicho de otra forma, $\psi(x)$ tiene la forma

$$\begin{bmatrix} \psi_1(x) & * \\ 0 & \psi_2(x) \end{bmatrix} \tag{6.12}$$

donde $\psi_1 : A \to M_r(F)$ y $\psi_2 : A \to M_{n-r}(F)$ son aplicaciones adecuadas. El hecho de que ψ es una representación de A implica que ψ_1 y ψ_2 son también representaciones.

Se dice que una representación θ de A es irreducible si θ no satisface las condiciones de la proposición anterior. En particular, θ es irreducible si y solo si M_θ es simple.

Utilizaremos ahora otra caracterización de módulos simples. El resultado será también válido para R-álgebras.

Lema 6.22. Sea N un A-módulo a derecha. Si N es simple, entonces $J(A) \subseteq \text{ann}N$ y N es indescomponible. El recíproco es cierto si A es artiniana a derecha o a izquierda: $J(A) \subseteq \text{ann}N$ y N indescomponible implican que N es simple.

Demostración. Si N es simple, por el corolario 5.3 tenemos que $NJ(A) \subseteq \text{rad}N = 0$. Esto es, $J(A) \subseteq \text{ann}N$. Claramente, N es indescomponible. Para el recíproco, observemos que por la proposición 3.4 podemos ver N como un $A/J(A)$-módulo. La hipótesis de que A es artiniano garantiza que $A/J(A)$ es semisimple. Así, N es semisimple por la proposición 4.4. Como N es también indescomponible, se sigue que N es simple.

Corolario 6.23. SI A es una F-álgebra semisimple, entonces una representación θ de A es indescomponible si y solo si θ es irreducible.

Corolario 6.24. Sea A una F-álgebra artiniana a derecha. El número de clases de equivalencia de representaciones irreducibles de A es el número de factores en una descomposición de $A/J(A)$ como producto de álgebras simples.

Demostración. Por el lema anterior, existe una correspondencia biunívoca entre las clases de isomorfismos de A-módulos simples y las clases de isomor-

fismos de $A/J(A)$-módulos. Si $A/J(A) = A_1 \dotplus ... \dotplus A_r$ con cada A_i simple, entonces por la proposición 4.4 y el lema 4.6 tenemos todo $A/J(A)$-módulo simple es isomorfo a un ideal minimal a derecha de algún A_i. Todos los ideales minimales a derecha de A_i son isomorfos por la proposición 4.15, mientras que si $i \neq j$ entonces un ideal minimal a derecha de A_i no es isomorfo a un ideal minimal a derecha de A_j. Por tanto, el corolario es consecuencia de la proposición anterior.

Corolario 6.25. Sea F un cuerpo algebraicamente cerrado, y supongamos que A es una F-álgebra de dimensión finita. Entonces el número de representaciones irreducibles de A es $\dim_F Z(A/J(A))$.

Demostración. Por el corolario 4.26, $A \cong M_{n_1}(F) \dotplus ... \dotplus M_{n_r}(F)$. El número natural r es igual a $\dim_F Z(A/J(A))$.

7. Producto tensorial de álgebras

Finalizaremos el presente trabajo cerrando el estudio del producto tensorial al analizar su comportamiento sobre álgebras. Acabaremos la sección viendo la importancia del producto tensorial en las representaciones a través del concepto de módulos inducidos.

7.1. El producto tensorial como R-álgebra

En primer lugar, observaremos que el producto tensorial de dos álgebras con una operación producto definida adecuadamente mantiene el estatus de R-álgebra. Asimismo, encontraremos una caracterización interna en términos de subálgebras.

Proposición 7.1. Si A y B son R-álgebras, entonces existe una operación producto sobre $A \otimes B$ que satisface

$$(x_1 \otimes y_1)(x_2 \otimes y_2) = x_1 x_2 \otimes y_1 y_2 \tag{7.1}$$

Este producto es asociativo y $1_A \otimes 1_B = 1_{A \otimes B}$.

Demostración. Para $x_1 \in A$ y $y_1 \in B$, sean λ_{x_1} y λ_{y_1} los endomorfismos de multiplicación a izquierda de A y B correspondientes a x_1 e y_1. Podemos ver fácilmente que $\lambda_{x_1} \otimes \lambda_{y_1} \in E_R(A \otimes B)$ satisface $(\lambda_{x_1} \otimes \lambda_{y_1})(x_2 \otimes y_2) = x_1x_2 \otimes y_1y_2$. Además, $(x_1, y_1) \mapsto \lambda_{x_1} \otimes \lambda_{y_1}$ es una aplicación bilineal de $A \times B$ en $E_R(A \otimes B)$. Así, existe un homomorfismo de R-módulos $\phi : A \otimes B \to E_R(A \otimes B)$ tal que $\phi(x_1 \otimes y_1) = \lambda_{x_1} \otimes \lambda_{y_1}$. Definimos $(A \otimes B) \times (A \otimes B) \to A \otimes B$ por $(z, w) \mapsto zw = \phi(z)(w)$. Dado que ϕ es un homomorfismo de R-módulos y $\phi(z) \in E_R(A \otimes B)$, la aplicación es bilineal y por tanto una operación producto sobre $A \otimes B$. Por construcción, $(x_1 \otimes y_1)(x_2 \otimes y_2) = \phi(x_1 \otimes y_1)(x_2 \otimes y_2) = (\lambda_{x_1} \otimes \lambda_{y_1})(x_2 \otimes y_2) = x_1x_2 \otimes y_1y_2$, y por tanto se satisface (7.1). Por tanto, el producto es asociativo. Además, $1_A \otimes 1_B$ es el elemento unidad de $A \otimes B$ trivialmente por (7.1).

Corolario 7.2. Sean A, B y C R-álgebras. Entonces,

(I). $(A \dotplus B) \otimes C \cong (A \otimes C) \dotplus (B \otimes C)$.

(II). $(A \otimes B) \otimes C \cong A \otimes (B \otimes C)$.

(III). $A \otimes B \cong B \otimes A$.

(IV). $A \otimes R \cong R \otimes A \cong A$.

En este último corolario, $\cong$ denota la relación de isomorfismo de R-álgebras, aunque se pueden encontrar los isomorfismos de R-módulos correspondientes fácilmente.

Lema 7.3. Las aplicaciones $\kappa_A : A \to A \otimes B$ y $\kappa_B : B \to A \otimes B$ definidas por $\kappa_A(x) = x \otimes 1_B$ y $\kappa_B(y) = 1_A \otimes y$ son homomorfismos de álgebras tales que

(I). $\kappa_A(A) \cup \kappa_B(B)$ genera $A \otimes B$ como R-álgebra.

(II). $\kappa_A(x)\kappa_B(y) = \kappa_B(y)\kappa_A(x)$ para todo $x \in A$, $y \in B$.

Si A y B son F-álgebras, entonces κ_A y κ_B son inyectivas. Además, si $\{x_i : i \in I\}$ es una base de A y $\{y_j : j \in J\}$ es una base de B, entonces $\{\kappa_A(x_i)\kappa_B(y_j) : (i, j) \in I \times J\}$ es una base de $A \otimes B$.

Demostración. La bilinealidad de $\otimes$ junto con (7.1) implica que κ_A y κ_B son homomorfismos de álgebras. Usando (7.1), $\kappa_A(x)\kappa_B(y) = x \otimes y = \kappa_B(y)\kappa_A(x)$, lo

que lleva trivialmente a (I) y (II). La última afirmación es consecuencia de la proposición 3.37.

Definición 7.4. Sea X un subconjunto de una R-álgebra A. Definimos el centralizador de X en A como

$$C_A(X) = \{y \in A : xy = yx \quad \forall x \in X\} \tag{7.2}$$

Este concepto ya es familiar de otras ramas del álgebra, aunque remarcaremos algunas consecuencias directas de la definición.

Lema 7.5. Sean X e Y subconjuntos del álgebra A, y sea B una subálgebra de A. Entonces,

(I). $C_A(X)$ es una subálgebra de A con $Z(A) \subseteq C_A(X)$.

(II). Si $X \subseteq Y$, entonces $C_A(Y) \subseteq C_A(X)$.

(III). $X \subseteq C_A(Y)$ si y solo si $Y \subseteq C_A(X)$. En particular, $X \subseteq C_A(C_A(X))$.

(IV). $B \cap C_A(B) = Z(B)$.

(V). $C_A(X) = A$ si y solo si $X \subseteq Z(A)$.

Utilizaremos esto para probar una propiedad universal del producto tensorial de álgebra, que nos llevará al teorema de caracterización.

Proposición 7.6. Sean A, B y C R-álgebras. Si $\phi : B \to A$ y $\psi : C \to A$ son homomorfismos de álgebras tales que $\psi(C) \subseteq C_A(\phi(B))$, entonces existe un único homomorfismo de álgebras $\theta : B \otimes C \to A$ que satisface

$$\theta(x \otimes y) = \phi(x)\psi(y) \tag{7.3}$$

para todo $x \in B$, $y \in C$. En particular, $\phi = \theta\kappa_B$ y $\psi = \theta\kappa_C$.

Demostración. Como ϕ y ψ son homomorfismos de R-módulos, la aplicación $(x, y) \mapsto \phi(x)\psi(y)$ es bilineal. Así, existe un homomorfismo de R-módulos que satisface (7.3). Por (7.1) y (7.3), tenemos que $\theta((x_1 \otimes y_1)(x_2 \otimes y_2)) = \phi(x_1x_2)\psi(y_1y_2) = \phi(x_1)\phi(x_2)\psi(y_1)\psi(y_2) = \phi(x_1)\psi(y_1)\phi(x_2)\psi(y_2) =$

$\theta(x_1 \otimes y_1)\theta(x_2 \otimes y_2)$, ya que $\psi(C) \subseteq C_A(\phi(B))$. Por tanto, θ es un homomorfismo de álgebras.

Corolario 7.7. Si $\phi : B \to B_1$ y $\psi : C \to C_1$ son homomorfismos de álgebras, entonces $\phi \otimes \psi : B \otimes C \to B_1 \otimes C_1$ es un homomorfismo de álgebras. Si B, B_1, C y C_1 son F-álgebras y ϕ y ψ son inyectivos, entonces $\phi \otimes \psi$ es inyectivo.

El corolario es consecuencia directa del lema 7.3 y la proposición 7.6.

Proposición 7.8. Si A, B y C son F-álgebras, entonces $B \otimes C \cong A$ si y solo si A contiene subálgebras B' y C' tales que

(I). $B' \cong B$ y $C' \cong C$ como F-álgebras.

(II). $C' \subseteq C_A(B')$.

(III). Existen bases $\{x_i : i \in I\}$ de B' y $\{y_j : j \in J\}$ de C' tales que $\{x_i y_j : (i, j) \in I \times J\}$ es una base de A.

Si A es de dimensión finita, se puede intercambiar esta última condición por

(IV). A está generada como F-álgebra por $B' \cup C'$ y $\dim A = (\dim B)(\dim C)$.

Demostración. Por el lema 7.3, es necesario que se cumplan todas las condiciones. Supongamos que existen subálgebras B' y C' de A que satisfacen (I) y (II). Sean $\phi : B \to B'$ y $\psi : C \to C'$ los isomorfismos correspondientes a (I). Por (II) y por la proposición 7.6, existe un homomorfismo de álgebras $\theta : B \otimes C \to A$ tal que $\theta(x \otimes y) = \phi(x)\psi(y)$ para todo $x \in B$, $y \in C$. Por el lema 7.3 y por (III), θ lleva una base de $B \otimes C$ biyectivamente a una base de A, de forma que θ es un isomorfismo. Si A es de dimensión finita y se satisface (IV), entonces θ es suprayectiva ya que $\theta(B \otimes C)$ es una subálgebra de A que incluye al conjunto generador $B' \cup C'$, y θ es inyectiva ya que $\dim A = (\dim B)(\dim C) = \dim B \otimes C$ por el lema 7.3.

Veamos una aplicación de estos resultados a álgebras de grupo.

Proposición 7.9. Sean G_1 y G_2 grupos finitos, y sea $G = G_1 \times G_2$ el producto de G_1 y G_2. Si F es un cuerpo, entonces $FG \cong FG_1 \otimes FG_2$.

Demostración. Denotamos por simplicidad $A = FG$. Consideraremos G_1 y G_2 como subgrupos de G, de forma que cada elemento de G tiene una representación único en la forma xy con $x \in G_1$, $y \in G_2$. Sea A_1 el subespacio generado por G_1 y A_2 el subespacio generado por G_2. Claramente, A_1 y A_2 son subálgebras de A tales que $A_1 \cong FG_1$ y $A_2 \cong FG_2$. Como $xy = yx$ para todo $x \in G_1$, $y \in G_2$, tenemos que $A_1 \subseteq C_A(A_2)$. Claramente, $A_1 \cup A_2$ genera A como F-álgebra. Finalmente, $\dim A = |G| = |G_1||G_2| = (\dim A_1)(\dim A_2)$. Así, por la proposición 7.8, tenemos que $FG = A \cong A_1 \otimes A_2 \cong FG_1 \otimes FG_2$.

7.2. Producto tensorial de módulos sobre álgebras

Veremos en este apartado cómo al producto tensorial de módulos sobre álgebras A y B se le puede dotar de estructura de $A \otimes B$-módulo.

Lema 7.10. Si M es un A-módulo a derecha y N es un B-módulo a derecha, entonces $M \otimes N$ es un $A \otimes B$-módulo a derecha con operaciones escalares que satisfacen

$$(u \otimes v)(x \otimes y) = ux \otimes vy \tag{7.4}$$

para todo $u \in M$, $v \in N$, $x \in A$, $y \in B$.

La demostración de este lema es una adaptación trivial de la demostración de la proposición 7.1.

Proposición 7.11. Sean M_1 y M_2 A-módulos a derecha, y sean N_1 y N_2 B-módulos a derecha. Entonces,

(I). Si $\phi \in \mathrm{Hom}_A(M_1, M_2)$ y $\psi \in \mathrm{Hom}_B(N_1, N_2)$, entonces $\phi \otimes \psi \in \mathrm{Hom}_{A\otimes B}(M_1 \otimes N_1, M_2 \otimes N_2)$.

(II). La aplicación $(\phi, \psi) \mapsto \phi \otimes \psi$ induce un homomorfismo de R-módulos $\theta : \mathrm{Hom}_A(M_1, M_2) \otimes \mathrm{Hom}_B(N_1, N_2) \to \mathrm{Hom}_{A\otimes B}(M_1 \otimes N_1, M_2 \otimes N_2)$.

(III). $\theta : E_A(M_1) \otimes E_B(N_1) \to E_{A\otimes B}(M_1 \otimes N_1)$ es un homomorfismo de álgebras.

Demostración. Dado que ϕ y ψ son homomorfismos de módulos, $(\phi \otimes \psi)((u \otimes v)(x \otimes y)) = \phi(ux) \otimes \psi(vy) = \phi(u)x \otimes \psi(v)y = ((\phi \otimes \psi)(u \otimes v))(x \otimes y)$. La afirmación

(I) se sigue por tanto de la proposición 2.14 sobre la unicidad de aplicaciones. Dado que $(\phi,\psi)\mapsto\phi\otimes\psi$ es bilineal, la existencia de θ es consecuencia de la propiedad de universalidad de productos tensoriales. Para evitar confusiones en la demostración de (III), denotaremos un tensor de rango uno en $E_A(M_1)\otimes E_B(N_1)$ por $\phi\otimes'\psi$. Así, por definición, $\theta(\phi\otimes'\psi)=\phi\otimes\psi$. Así, $\theta((\phi_1\otimes'\psi_1)(\phi_2\otimes'\psi_2))=\theta(\phi_1\phi_2\otimes'\psi_1\psi_2)=\phi_1\phi_2\otimes\psi_1\psi_2=(\phi_1\otimes\psi_1)(\phi_2\otimes\psi_2)=\theta(\phi_1\otimes'\psi_1)\theta(\phi_2\otimes'\psi_2)$. Se sigue por tanto que θ es un homomorfismo de álgebras.

En general, el homomorfismo θ no es ni inyectivo ni suprayectivo. Sin embargo, en los casos que trataremos θ será un isomorfismo.

Corolario 7.12. Sean M_1 y M_2 A-módulos a derecha y sean N_1 y N_2 B-módulos a derecha con M_1 y N_1 libres con bases finitas. El homomorfismo $\theta:\mathrm{Hom}_A(M_1,M_2)\otimes\mathrm{Hom}_B(N_1,N_2)\to\mathrm{Hom}_{A\otimes B}(M_1\otimes N_1,M_2\otimes N_2)$ es un isomorfismo. En particular, $E_A(M_1)\otimes E_B(N_1)\cong E_{A\otimes B}(M_1\otimes N_1)$.

Demostración. Dado que M_1 y N_1 son libres, existen $m,n\in\mathbb{N}$ tales que $M_1\cong\bigoplus_m A$ y $N_1=\bigoplus_n B$. Con lo visto anteriormente es claro que $\mathrm{Hom}_A(M_1,M_2)\otimes\mathrm{Hom}_B(N_1,N_2)\cong\mathrm{Hom}_A(\bigoplus_m A,M_2)\otimes\mathrm{Hom}_B(\bigoplus_n B,N_2)\cong(\bigoplus_m\mathrm{Hom}_A(A,M_2))\otimes(\bigoplus_n\mathrm{Hom}_b(B,N_2))\cong\bigoplus_{mn}(\mathrm{Hom}_A(A,M_2)\otimes\mathrm{Hom}_B(B,N_2))\cong\bigoplus_{mn}\mathrm{Hom}_{A\otimes B}(A\otimes B,M_2\otimes N_2)\cong\mathrm{Hom}_{A\otimes B}(\bigoplus_{mn}A\otimes B,M_2\otimes N_2)\cong\mathrm{Hom}_{A\otimes B}(M_1\otimes N_1,M_2\otimes N_2)$. La comprobación de que θ es un isomorfismo de composición es puramente rutinaria.

Corolario 7.13. $M_m(A)\otimes M_n(B)\cong M_{mn}(A\otimes B)$.

Este último es una reformulación de la última parte del corolario anterior utilizando el isomorfismo $E_A(\bigoplus_m A)\cong M_m(A)$ que probamos en el corolario 4.21.

7.3. Extensiones escalares

Los productos tensoriales son también útiles en el estudio de álgebras porque permiten extender el dominio de escalares de R a un anillo conmutativo que contiene a R como subanillo. De forma más general, permiten pasar de una R-álgebra a una S-álgebra con S una R-álgebra conmutativa.

Proposición 7.14. Sea A una R-álgebra. Si S es una R-álgebra conmutativa, entonces $A \otimes S$ es una S-álgebra cuyo producto satisface

$$(x \otimes c)(y \otimes d) = xy \otimes cd \tag{7.5}$$

para todo $x, y \in A$, $c, d \in S$. Se define la operación escalar sobre $A \otimes S$ por elementos de S como

$$zc = z(1_A \otimes c) \tag{7.6}$$

para todo $z \in A \otimes S$, $c \in S$.

Demostración. Por la proposición 7.1, $A \otimes S$ es una R-álgebra, y $\kappa_S : S \to A \otimes S$ (definido por $\kappa_S(c) = 1_A \otimes c$) es un homomorfismo de R-álgebras tal que $\kappa_A(A) \subseteq C_{A\otimes S}(\kappa_S(S))$. Además, $\kappa_S(S) \subseteq C_{A\otimes S}(\kappa_S(S))$ ya que S es conmutativo. Así, $A \otimes S = C_{A\otimes S}(\kappa_S(S))$ usando los lemas 7.3 y 7.5. Esto es, $\kappa_S(S) \subseteq Z(A \otimes S)$. Esta inclusión garantiza que la operación de S-módulo (7.6) induce una estructura de S-álgebra sobre $A \otimes S$.

Si A es una R-álgebra y S una R-álgebra conmutativa, denotaremos $A \otimes S$ por A^S con el producto tensorial visto como S-álgebra. Es relevante señalar que especialmente en la literatura más antigua sobre álgebras asociativas se suele denotar también por A_S.

Las leyes distributiva y asociativa tienen importantes consecuencias en las extensiones escalares.

Corolario 7.15. Sean A y B R-álgebras. Si S es una R-álgebra conmutativa y T es una S-álgebra conmutativa, entonces

(I). $(A \dot{+} B)^S \cong A^S \dot{+} B^S$.

(II). $(A \otimes_R B)^S \cong A^S \otimes_S B^S$.

(III). $(A^S)^T \cong A^T$.

Demostración. El primer isomorfismo es consecuencia directa del corolario 7.2(I). Las demostraciones de (II) y (III) son extensiones menores de la ley asociativa; si M es un R-módulo y N y P son S-módulos, entonces se pueden

ver N y $N \otimes_S P$ como R-módulos, y $M \otimes_R (N \otimes_S P) \cong (M \otimes_R N) \otimes_S P$. Usando este resultado, tenemos que $(A \otimes_R B)^S = (A \otimes_R B) \otimes_R S \cong (A \otimes_R S) \otimes_R B \cong (A \otimes_R (S \otimes_S S)) \otimes_R B \cong ((A \otimes_R S) \otimes_S S) \otimes_R B \cong A^S \otimes_S B^S$, y $(A^S)^T = (A \otimes_R S) \otimes_S T \cong A \otimes_R (S \otimes_S T) \cong A \otimes_R T = A^T$.

Lema 7.16. Sea A una F-álgebra con base $\{x_i : i \in I\}$. Si E es una extensión de cuerpos de F, entonces $\{x_i \otimes 1_e : i \in I\}$ es una E-base de A^E. En particular, $\dim_E A^E = \dim_F A$.

Demostración. Sea $\{c_j : j \in J\}$ una F-base de E. Entonces, $\{x_i \otimes c_j : (i,j) \in I \times J\}$ es una F-base de $A \otimes E$. Usando (7.6), $x_i \otimes c_j = (x_i \otimes 1)c_j$, de forma que $\{x_i \otimes 1 : i \in I\}$ genera A^E. Supongamos que $\sum_i (x_i \otimes 1)d_i = 0$ con $d_i \in E$. Denotamos $d_i = \sum_j c_j a_{ji}$ para ciertos $a_{ji} \in F$. Se sigue que

$$\sum_{i,j} (x_i \otimes c_j)a_{ji} = \sum_i (x_i \otimes 1)d_i = 0$$

de forma que $a_{ji} = 0$ para todo j, i. Por tanto, $d_i = 0$ para todo $i \in I$.

La formulación de este lema es más sencilla para álgebras de dimensión finita, como veremos en el siguiente corolario.

Corolario 7.17. Sea A una F-álgebra de dimensión n con base $x_1, x_2, ..., x_n$ y constantes de estructura correspondientes a_{ij}^k. Si E/F es una extensión de cuerpos, entonces A^E es isomorfo a la E-álgebra de dimensión n con base $x_1, x_2, ..., x_n$ y constantes de estructura correspondientes a_{ij}^k.

Este corolario es consecuencia directa del lema. El isomorfismo es el obvio que lleva $x_i \otimes 1$ en x_i.

Un caso útil de este corolario se da cuando A es un álgebra de cuaternios. En ese caso, si E/F es una extensión de cuerpos y $a, b \in F^o$, entonces $\left(\frac{a,b}{F}\right)^E = \left(\frac{a,b}{E}\right)$.

Proposición 7.18. Sea A una F-álgebra, y sea E/F una extensión de cuerpos. Una E-álgebra B es isomorfa a A^E si y solo si existe una F-subálgebra A' de B tal que

(I). $A' \cong A$ como F-álgebras.

(II). Existe una F-base de A' que es también E-base de B.

Si $\dim_F A < \infty$, entonces se puede sustituir (II) por

(III). $A'E = B$ y $\dim_E B = \dim_F A$.

Demostración. Si $B \cong A^E$, entonces se satisfacen (I) y (II) por la proposición 7.6 y el lema 7.16. Es evidente que las condiciones (II) y (III) son equivalentes si la dimensión es finita. Supongamos que se satisfacen (I) y (II). Sea $E' = \{1_B c : c \in E\}$. Claramente, E' es una F-subálgebra de B isomorfa a E, y $E' \subseteq Z(B) \subseteq C_B(A')$. Si $\{x_i : i \in I\}$ es una F-base de A', y $\{c_j : j \in J\}$ es una F-base de E', entonces $\{x_i c_j : (i,j) \in I \times J\}$ es una F-base de B. Efectivamente, por (II) tenemos que $\sum_{i,j} x_i c_j F = \sum_i x_i E = B$, y $\sum_{i,j} x_i c_j a_{ij} = 0$ con $a_{ij} \in F$ implica que $\sum_j c_j a_{ij} = 0$ para todo i, de forma que $a_{ij} = 0$ para todo $i \in I, j \in J$. Por la proposición 7.6, existe un isomorfismo de F-álgebras $\theta : A \otimes E \to B$ tal que $\theta(1_A \otimes c) = 1_B c$ para todo $c \in E$. Por tanto, si $z \in A \otimes E$ y $c \in E$, entonces $\theta(zc) = \theta(z(1 \otimes c)) = \theta(z)(1_B c) = \theta(z)c$, esto es, θ es un isomorfismo de E-álgebras.

Veremos ahora una aplicación al estudio de cuerpos.

Proposición 7.19. Sea A una extensión simple del cuerpo F, $A = F(d)$ y E un cuerpo extensión de F. Denotamos el polinomio mínimo de d sobre F como $\Phi(X)$. Entonces $A^E \cong E[X]/K$ con $K = \Phi(X)E[X]$.

Demostración. Sea $A' = (F[X] + K)/K \cong F[X]/K \cap F[X]$. Claramente, $K \cap F[X]$ es un ideal propio de $F[X]$ que contiene a $\Phi(X)F[X]$. Sin embargo, $\Phi(X)F[X]$ es un ideal maximal de $F[X]$ ya que $F[X]/\Phi(X)F[X] \cong F(d)$ es un cuerpo. Así, $K \cap F[X] = \Phi(X)F[X]$, de forma que $A' \cong A$. El isomorfismo $A^E \cong E[X]/K$ se sigue por tanto de la proposición anterior, ya que $A'E = E[X]/K$ y $\dim_E E[X]/K = \mathrm{gr}\Phi(X) = \dim_F A$.

Este resultado nos da una conexión entre la separabilidad y el comportamiento de cuerpos bajo extensiones escalares. Si el polinomio $\Phi(X)$ es separable, entonces se factoriza en componentes irreducibles distintas dos a dos en

$E[X]$. El teorema chino de los restos nos lleva a la conclusión de que A^E es isomorfo a un producto de cuerpos. Sin embargo, esto cambia si $\Phi(X)$ es inseparable. Por ejemplo, supongamos que car$F = p$ y $d = a^{1/p}$, donde $a \in F - F^p$. En ese caso, $\Phi(X) = X^p - a$. Si el cuerpo extensión E también contiene a d, entonces $\Phi(X) = (X-d)^p$ en $E[X]$. En consecuencia, el radical de $E[X]/K$ es distinto de cero: $J(E[X]/K) = (X-d)E[X]/K$.

7.4. Módulos inducidos

Terminaremos con un breve estudio de los módulos inducidos. Veremos que los productos tensoriales nos permiten convertir A-módulos en B-módulos con A una subálgebra de B. Este concepto tendrá aplicaciones importantes en representaciones de grupos. Para ello, tendremos que trabajar con productos tensoriales sobre álgebras no conmutativas.

Lema 7.20. Sean A y B R-álgebras. Si M es un A-módulo a derecha y N es un A-B-bimódulo, entonces $M \otimes_A N$ es un B-módulo a derecha con operaciones escalares que satisfacen

$$(u \otimes v)y = u \otimes (vy) \tag{7.7}$$

para todo $u \in M$, $v \in N$, $y \in B$.

Demostración. Si $y \in B$, definimos $\Phi_y : M \times N \to M \otimes_A N$ por $\Phi_y(u,v) = u \otimes vy$. Claramente, Φ_y es R-bilineal, y $\Phi_y(ux,v) = ux \otimes vy = u \otimes x(vy) = u \otimes (xv)y = \Phi_y(u,xv)$. Así, existe un endomorfismo de R-módulos ϕ_y de $M \otimes_A N$ que satisface $\phi_y(u \otimes v) = u \otimes vy$. Mediante cálculos directos se puede ver que $\phi_{ya+zb} = \phi_y a + \phi_z b$ y $\phi_z \phi_y = \phi_{yz}$. Así, $M \otimes_A N$ es un B-módulo a derecha con la operación escalar $wy = \phi_y(w)$ para todo $w \in M \otimes_A N$, $y \in B$. Además, $(u \otimes v)y = \phi_y(u \otimes v) = u \otimes (vy)$.

Repitiendo el argumento, vemos que si M es un B-A-bimódulo y N es un A-módulo a derecha, entonces $M \otimes_A N$ es un B-módulo a izquierda. Si M y N son ambos bimódulos, entonces $M \otimes_A N$ es también un bimódulo. De hecho, supongamos que M es un B-A-bimódulo y N es un A-C-bimódulo. Entonces $M \otimes_A N$ es un B-módulo a izquierda y un C-módulo a derecha. Si $y \in B$, $z \in C$, $u \in M$ y $v \in N$, entonces $y((u \otimes v)z) = yu \otimes vz = (y(u \otimes v))z$, lo que implica

asociatividad. Finalmente, si $a \in R$, $u \in M$ y $v \in N$, entonces $a(u \otimes v) = (au) \otimes v = (ua) \otimes v = u \otimes (av) = (u \otimes v)a$.

Tenemos así una ley de asociatividad generalizada para productos tensoriales sobre álgebras.

Corolario 7.21. Sean A y B R-álgebras. Si M es un A-módulo a derecha, N es un A-B-bimódulo y P es un B-módulo a izquierda, entonces $M \otimes_A (N \otimes_B P) \cong (M \otimes_A N) \otimes_B P$ como R-módulos. Si además M o P es un bimódulo, entonces el isomorfismo es un isomorfismo de módulos, y será un isomorfismo de bimódulos si ambos son bimódulos.

El caso más importante del lema es en el que A es subálgebra de B y $N = B$. Claramente, se puede considerar B como A-B-bimódulo. Por tanto, si M es un A-módulo a derecha, entonces $M \otimes_A B$ es un B-módulo a derecha inducido por M. Denotaremos $M \otimes_A B$ por M^B.

Lema 7.22. Sean A, B y C R-álgebras, con A una subálgebra de B y B una subálgebra de C, y sean M y N A-módulos a derecha. Entonces,

(I). $(M \oplus N)^B \cong M^B \oplus N^B$.

(II). $(M^B)^C \cong M^C$.

(III). $M^A \cong M$.

Además, si M y N son bimódulos, entonces los isomorfismos (I), (II) y (III) son isomorfismos de bimódulos.

La demostración de este lema es fundamentalmente un calco de la demostración del corolario 7.15. La fórmula (7.7) nos prueba que los isomorfismos preservan las operaciones escalares.

Si A es una subálgebra de B, entonces el funtor de olvido $N \mapsto N_A$ que describimos en 3.1 lleva B-módulos en A-módulos. Componiendo esta restricción de operaciones escalares con la aplicación inducción, obtenemos correspondencias $M \mapsto (M^B)_A$ y $N \mapsto (N_A)^B$.

Lema 7.23. Sean A, B y C R-álgebras, con A una subálgebra de B, y sea M un A-módulo a derecha y N un B-módulo a derecha. Entonces existen homomorfismos $\nu_M : M \to (M^B)_A$ (de A-módulos a derecha) y $\mu_N : (N_A)^B \to N$ (de B-módulos a derecha) tales que

$$\nu_M(u) = u \otimes 1_B, \quad \forall u \in M \tag{7.8}$$

$$\mu_N(v \otimes 1_B) = v, \quad \forall v \in N \tag{7.9}$$

Si M es un C-A-bimódulo, entonces ν_M es un homomorfismo de C-módulos; si N es un C-B-bimódulo, entonces μ_N es un homomorfismo de C-módulos.

Demostración. Claramente, (7.8) define un homomorfismo de R-módulos. Si $u \in M$ y $x \in A$, entonces $\nu_M(ux) = ux \otimes 1_B = u \otimes x = (u \otimes 1_B)x = \nu_M(u)x$. Así, ν es un homomorfismo de A-módulos. Si M es un C-A-bimódulo, entonces es claro que ν_M es un homomorfismo de C-módulos. La aplicación $N_A \times B \to N$ definida por $(v, y) \mapsto vy$ es claramente R-bilineal y equilibrada (en el sentido de la condición (2.21) y relativa a los elementos de A). Por tanto, existe un homomorfismo de R-módulos $\mu_N : N_A \otimes_A B \to N$ tal que $\mu_N(v \otimes y) = vy$. μ_N será por tanto un homomorfismo de B-módulos, y si N es un C-B-bimódulo entonces μ_N será trivialmente un homomorfismo de C-módulos.

Cuando no se preste a confusión, denotaremos simplemente ν por ν_M y μ por μ_N. Estas aplicaciones son útiles para relacionar los tipos de representación de A y B.

Proposición 7.24. Sean A y B álgebras artinianas tales que A es una subálgebra de B y B es finitamente generado como A-módulo a derecha. Entonces,

1. Supongamos que para todo A-módulo a derecha M, el homomorfismo $\nu_M : M \to (M^B)_A$ es inyectivo y de escisión. Si B tiene un tipo de representación finito, entonces A también.

2. Supongamos que para todo B-módulo a derecha N, el homomorfismo $\mu_N : (N_A)^B \to N$ es suprayectivo y de escisión. Si A tiene un tipo de representación finito, entonces B también.

Demostración. Probaremos (I) y la demostración de (II) será análoga. Sean $N_1, N_2, ...N_k$ representantes de las clases de isomorfía de B-módulos indescomponibles finitamente generados. Dado que B_A es un A-módulo finitamente generado, también lo es $(N_i)_A$. Por el teorema de Krull-Schmidt tenemos que cada $(N_i)_A$ se descompone de forma única en suma directa de A-módulos indescomponibles. Bastará probar que todo A-módulo indescomponible finitamente generado M es isomorfo a un sumando directo de algún $(N_i)_A$. Expresaremos $M^B \cong \bigoplus_{i=1}^{k} \bigoplus_{m_i} N_i$, con $m_i \geq 0$. Dado que $\nu_M : M \to (M^B)_A$ es inyectivo y de escisión, M es isomorfo a un sumando directo de $(M^B)_A \cong \bigoplus_{i=1}^{k} \bigoplus_{m_i} (N_i)_A$. El teorema de Krull-Schmidt nos lleva al resultado que queremos probar, que M es un sumando directo de algún $(N_i)_A$, ya que M es indescomponible.

Para poder aplicar esta proposición necesitaremos saber cuándo μ y ν son homomorfismos de escisión. A continuación trataremos únicamente la escisión de ν; la de μ requeriría de resultados intermedios que no vamos a tratar.

Proposición 7.25. Sea A una subálgebra de la R-álgebra B. Las siguientes condiciones son equivalentes.

1. $B = A \oplus N$ con N un A-submódulo a derecha e izquierda de B.
2. Para toda R-álgebra C y todo C-A-bimódulo M, $\nu : M \to (M^B)_A$ es un homomorfismo de C-A-bimódulos inyectivo y de escisión.

Demostración. (I) $\Rightarrow$ (II): Por (I), existe un homomorfismo de A-bimódulos $\pi : B \to A$ tal que $\pi|_A = \mathrm{id}_A$. Dado que π es un homomorfismo de A-módulos a izquierda, la aplicación de $M \times B$ en M definida por $(u, y) \mapsto u\pi(y)$ es bilineal y equilibrada. Así, existe un homomorfismo $\rho : M^B \to M$ tal que $\rho(u \otimes y) = u\pi(y)$. Claramente, ρ es un homomorfismo de C-módulos a izquierda, y es un homomorfismo de A-módulos a derecha ya que π es un homomorfismo de A-módulos a derecha. Finalmente, $1_B = 1_A \in A$, por lo que $\rho\nu(u) = \rho(u \otimes 1_B) = u1_A = u$. Por tanto, ν es inyectivo y de escisión. La propiedad (I) es un caso particular de (II) con $C = A$ y $M = A$ considerado como A-bimódulo.

La parte esencial de la proposición se puede expresar sucintamente: si ν_A es inyectivo y de escisión, entonces ν_M es inyectivo y de escisión para todo A-

módulo M. Llamaremos a B una extensión de escisión de A si A es una subálgebra de B tal que B_A es un A-módulo finitamente generado y $B = A \oplus N$ con N un A-submódulo a izquierda y derecha de B.

Podemos aplicarlo a álgebras de grupos con facilidad: si H es un subgrupo de un grupo finito G, entonces FG es una extensión de escisión de FH para todo cuerpo F. Efectivamente, $FG = FH \oplus N$ con $N = \sum_{y \in G-H} yF$, y N es un sub-A-bimódulo de FG ya que $x \in H$ y $y \in G$ implican que $xy \in G - H$ y $yx \in G - H$.

Corolario 7.26. Sean A y B álgebras artinianas tales que B es una extensión de escisión de A. Si B tiene un tipo de representación finito, entonces A también.

Este corolario es aplicación directa de las dos proposiciones de este apartado. Combinando el corolario 7.21 y el ejemplo anterior de álgebras de grupo, tenemos la mitad de la caracterización de Higman de álgebras de grupo de tipo de representación finito.

Corolario 7.27. Sea p un número primo, F un cuerpo de característica p y G un grupo finito tal que FG tiene tipo de representación finito. Entonces los p-subgrupos de Sylow de G son cíclicos.

8. Bibliografía

Bibliografía principal

[1] BOURBAKI, N. (1974). *Elements of Mathematics: Algebra I* (5.ª edición). París: Hermann.

[2] CURTIS, C. W.; REINER, I. (1962). *Representation Theory of Finite Groups and Associative Algebras*. Nueva York: Interscience Publishers.

[3] HUNGERFORD, T. W. (1974). *Algebra* (12.ª edición). Nueva York: Springer-Verlag.

[4] OLIVERT PELLICER, J. (1996). *Estructuras de álgebra multilineal*. Valencia: Universitat de València.

[5] PIERCE, R. S. (1982). *Associative Algebras*. Nueva York: Springer-Verlag.

Bibliografía complementaria

[1] ARTIN, E. (1957). *Geometric Algebra*. Nueva York: Interscience.

[2] AZUMAYA, G. (1951). On maximally central algebras. *Nagoya Math. J.* **2**, 119-150.

[3] BASS, H. (1968). *Algebraic K-Theory*. Reading: Addison-Wesley.

[4] BRAUER, R.; NOETHER, E. (1927). Über minimale Zerfällungskörper irreducibler Darstellungen. *Ak. Berlin S. B.* **27** 221-226.

[5] BRAUER, R.; WEISS, E. (1950). *Non-commutative Rings. Part I*. Cambridge: Harvard Univ. Press.

[6] CARTAN, H.; EILENBERG, S. (1956). *Homological Algebra*. Princeton: Princeton Univ. Press.

[7] DIVINSKI, N. J. (1965). *Rings and Radicals*. Toronto: Univ. of Toronto Press.

[8] GERSTENHABER, M. (1963). On the cohomology structure of an associative ring. *Ann. of Math.* (2) **78**, 267-288.

[9] HIGMAN, D. G. (1954). Indescomposable representations at characteristic p. *Duke Math. Jour.* **7**, 377-381.

[10] JACOBSON, N. (1956). *Structure of Rings*. Amer. Math. Soc. Colloquium Publ. vol. 37. Providence: Amer. Math. Soc.

[11] LAM, T. Y. (1973). *The Algebraic Theory of Quadratic Forms*. Reading: Addison-Wesley.

[12] PASSMAN, D. S. (1977). *The Algebraic Structure of Group Rings*. Nueva York: Wiley-Interscience.

[13] PEIRCE, B. O. (1881). Linear associative algebra. *Amer. Jour. of Math.* **4**, 97-229.

[14] WALLACE, D. A. R. (1961). On the radical of a group algebra. *Proc. Amer. Math. Soc.* **12**, 133-137.

[15] WEDDERBURN, J. H. M. (1907). On hypercomplex numbers. *Proc. Lond. Math. Soc.* (2) **6**, 77-118.