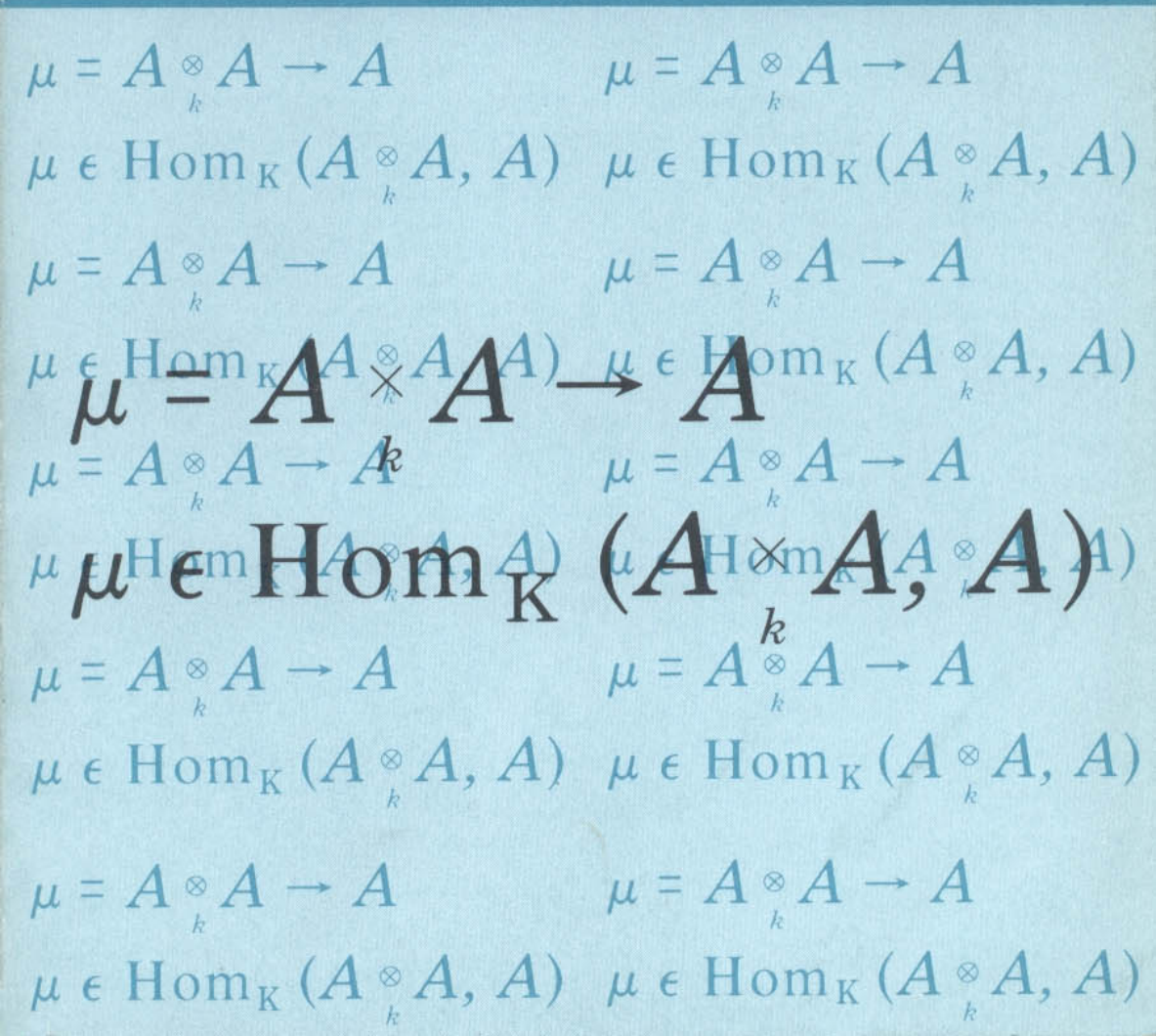
serie de matemática

monografía no. 24

ESTRUCTURAS ALGEBRAICAS VII (ESTRUCTURAS DE ALGEBRAS)

Secretaría General de la
Organización de los Estados Americanos
Programa Regional de Desarrollo Científico y Tecnológico



ESTRUCTURAS ALGEBRAICAS VII (ESTRUCTURAS DE ALGEBRAS)

por

Artibano Micali
Institut de Mathématiques
Université de Montpellier II
Montpellier, FRANCIA

Secretaría General de la
Organización de los Estados Americanos
Programa Regional de Desarrollo Científico y Tecnológico
Washington, D.C. - 1983

Esta monografía ha sido preparada para su publicación en el Departamento de Asuntos Científicos y Tecnológicos de la Secretaría General de la Organización de los Estados Americanos.

Editora: Eva V. Chesneau

Asesor Técnico: Dr. Héctor A. Merklen
Instituto de Matemática e Estatística
Cidade Universitária "Armando de Salles Oliveira"
São Paulo, Brasil

A los lectores

El programa de monografías científicas es una faceta de la vasta labor de la Organización de los Estados Americanos, a cargo del Departamento de Asuntos Científicos y Tecnológicos de la Secretaría General de dicha Organización, a cuyo financiamiento contribuye en forma importante el Programa Regional de Desarrollo Científico y Tecnológico.

Concebido por los Jefes de Estado Americanos en su Reunión celebrada en Punta del Este, Uruguay, en 1967, y cristalizado en las deliberaciones y mandatos de la Quinta Reunión del Consejo Interamericano Cultural, llevada a cabo en Maracay, Venezuela, en 1968, el Programa Regional de Desarrollo Científico y Tecnológico es la expresión de las aspiraciones preconizadas por los Jefes de Estado Americanos en el sentido de poner la ciencia y la tecnología al servicio de los pueblos latinoamericanos.

Demostrando gran visión, dichos dignatarios reconocieron que la ciencia y la tecnología están transformando la estructura económica y social de muchas naciones y que, en esta hora, por ser instrumento indispensable de progreso en América Latina, necesitan un impulso sin precedentes.

El Programa Regional de Desarrollo Científico y Tecnológico es un complemento de los esfuerzos nacionales de los países latinoamericanos y se orienta hacia la adopción de medidas que permitan el fomento de la investigación, la enseñanza y la difusión de la ciencia y la tecnología; la formación y perfeccionamiento de personal científico; el intercambio de informaciones, y la transferencia y adaptación a los países latinoamericanos del conocimiento y las tecnologías generadas en otras regiones.

En el cumplimiento de estas premisas fundamentales, el programa de monografías representa una contribución directa a la enseñanza de las ciencias en niveles educativos que abarcan importantísimos sectores de la población y, al mismo tiempo, propugna la difusión del saber científico.

La colección de monografías científicas consta de cuatro series, en español y portugués, sobre temas de física, química, biología y matemática. Desde sus comienzos, estas obras se destinaron a profesores y alumnos de ciencias de los primeros años de la universidad; de éstos se tiene testimonio de su buena acogida.

Este prefacio brinda al Programa Regional de Desarrollo Científico y Tecnológico de la Secretaría General de la Organización de los Estados Americanos la ocasión de agradecer al doctor Artibano Micali, autor de esta monografía, y a quienes tengan el interés y buena voluntad de contribuir a su divulgación.

noviembre de 1983

ÍNDICE

1

... às mangueiras do Pici.

INTRODUCCIÓN

Si tuviéramos que fijar una fecha para el origen de las matemáticas que se presentan en este fascículo, no hay la menor duda de que lo situaríamos en 1843, a partir de la construcción, por W. R. Hamilton (1805-1865),[1] del primer ejemplo de un cuerpo no conmutativo: el cuerpo de los cuaternios. Las ideas de Hamilton tuvieron importantes consecuencias como, por ejemplo, la elaboración axiomática del álgebra lineal, cuyos principios fueron enunciados en forma general por B. Pierce, en 1870. Además, el carácter no conmutativo de las operaciones de Hamilton ha constituido un valioso aporte a la noción de ley de composición.

El paso siguiente fue dado por F. G. Frobenius (1849-1917),[2] uno de los matemáticos más originales de la segunda mitad del siglo pasado. Frobenius demostró que el cuerpo de los cuaternios es la única álgebra asociativa, pero no conmutativa, sobre $\mathbb{R}$ de rango finito y sin divisores de cero. Este resultado también fue demostrado de manera independiente por Charles Sanders Peirce (1839-1914). Peirce, hombre de cultura universal, era hijo del matemático Benjamin Peirce, quien descubrió una importante identidad, la identidad de Peirce, a saber: en un álgebra alternativa A, para todo idempotente $e \in A$, se tiene $x = exe + (ex - exe) + (xe - exe) + (x - ex - xe + exe)$ y esto, para todo $x \in A$. Tal identidad permite dar una descomposición natural del álgebra A y sus consecuencias son importantes para el estudio de la estructura de álgebras alternativas semisimples.[3] Es la demostración dada por Dickson del teorema de Frobenius la que se consigna en este texto (cf. el teorema 2.3.1.).

Con la construcción del álgebra de Cayley (Arthur Cayley, 1821-1895),[4] que constituye el primer ejemplo de álgebra alternativa no asociativa, fue posible enunciar la forma general del teorema de Frobenius (cf. el teorema 2.3.2.).[5] Subsiguientemente, los trabajos fundamentales de la Escuela Norteamericana, cuyo máximo representante es A. A. Albert, hicieron lo que faltaba o sea la formulación de una teoría coherente de álgebras centrales simples. El libro de Albert,[6] publicado en 1939, es la síntesis de lo que hasta ese entonces se conocía sobre el tema. Una reformulación de la teoría la da N. Bourbaki[6] años más tarde (1958), pero hay que esperar hasta 1967[7] para contar con una teoría completa de álgebras centrales separables o álgebras de Azumaya sobre un anillo cualquiera. Por supuesto, no se pueden olvidar los importantes trabajos de M. Auslander[8] que contribuyeron a dar forma definitiva a la teoría de álgebras de Azumaya.

Para profundizar en el tema, desde el punto de vista histórico, se recomienda al lector consultar la nota histórica del libro de N. Bourbaki.[6]

Esta monografía es una introducción a la teoría de álgebras centrales simples o álgebras de Azumaya sobre un cuerpo, destinada a despertar en algunos jóvenes el deseo de conocer una de las más hermosas teorías matemáticas hasta hoy construida: la teoría de álgebras de Azumaya.

Deseo agradecer a todos los que de una manera u otra contribuyeron a la publicación de esta monografía y, muy particularmente, a los asesores técnicos de la Organización de los Estados Americanos, que me llevaron a escribir un texto más apropiado a la realidad latinoamericana.

Bibliografía Histórica

(1) HAMILTON, W. R. Elements of Quaternions, Chelsea Publ. Co., Nueva York, N. Y., 2 vols. (1969).

(2) FROBENIUS, F. G. Gesammelte Abhandlungen, Springer-Verlag, Berlín, 3 vols. (1968).

(3) SCHAFER R. D. An Introduction to Nonassociative Algebras, Academic Press, Nueva York, N. Y. (1966).

(4) CAYLEY, A. The Collected Mathematical Papers, Cambridge Univ. Press, Cambridge, 14 vols. (1889-1898).

(5) ALBERT, A. A. Structure of Algebras, AMS Colloquium Publications, N° 24, Providence, R. I. (1939).

(6) BOURBAKI, N. Algèbre, Hermann, París, cap. 8 (1958).

(7) BASS, H. Lectures on Topics in Algebraic K-Theory, Tata Inst. Fundamental Research, Bombay (1967).

(8) AUSLANDER, M. y GOLDMAN, O. The Brauer Group of a Commutative Ring, *Trans. Am. Math. Soc.*, 97, 367-409 (1960).

(9) ALBERT, A. A. Absolute Valued Real Algebras, *Ann. Math.*, 48, 495-501 (1947).

1

MÓDULOS SEMISIMPLES

En este capítulo se expondrán algunos conceptos complementarios sobre la teoría de módulos simples y semisimples. Se supone que el lector conoce los elementos de la teoría de anillos y módulos, así como también los productos tensoriales.[20]

En lo que sigue, por el término anillo se entenderá anillo con elemento unidad y que todo módulo es unitario. Además, salvo mención contraria, el término módulo significa módulo a la izquierda.

1.1. MÓDULOS SIMPLES

Sean A un anillo y M un A-módulo (a la izquierda). Se dice que M es un *A-módulo simple* o *irreducible*, si M es distinto de cero y si los únicos submódulos de M son M y el módulo cero. Es claro que si N es un submódulo de un A-módulo M, entonces el A-módulo cociente M/N es simple si, y sólo si, N es un submódulo maximal de M. Decir que N es un *submódulo maximal* de M quiere decir que $N \subsetneq M$, esto es, N es un submódulo propio de M, y si M' es un submódulo de M tal que $N \subset M' \subset M$, entonces $N = M'$ o $M' = M$. La siguiente proposición vale para módulo de tipo finito: 3

Proposición 1. 1. 1. *Sean A un anillo y M un A-módulo de tipo finito. Todo submódulo propio de M está contenido en un submódulo maximal de M.*

Si M es un A-módulo de tipo finito, la familia de todos los submódulos propios de M es *inductiva*.[5] En efecto, si $(M_i)_{i\in I}$ es una familia totalmente ordenada de submódulos propios de M, entonces $\bigcup_{i\in I} M_i$ es un submódulo propio de M, pues si se supone que $\bigcup_{i\in I} M_i = M$, existe un índice m tal que $M_m = M$. Para demostrar esto se recurre al hecho de que M es de tipo finito. En efecto, si $x_1, \ldots, x_n$ es un sistema de generadores de M, para cada índice i, $1 \leq i \leq n$, existe un índice $j(i)$ tal que $x_i \in M_{j(i)}$ y si $m = \max(j(1), \ldots, j(n))$, entonces $x_i \in M_m$ para todo i, o sea $M = M_m$. Por el *lema de Zorn* (cf. [5]), la familia de todos los submódulos propios de M admite un elemento maximal. Dado ahora un submódulo propio N de M, basta considerar la familia, no vacía, de submódulos propios de M que contienen a N y aplicar a tal familia un argumento análogo.

La siguiente proposición muestra otra manera de expresar el hecho de que un módulo sea simple:

Proposición 1. 1. 2. *Sean A un anillo y M un A-módulo. Las siguientes condiciones son equivalentes:* (i) *M es un A-módulo simple;* (ii) *toda aplicación A-lineal $f: M \to M'$ de M en un A-módulo M' es inyectiva o nula.*

En efecto, $f : M \to M'$ inyectiva equivale a $\mathrm{Ker}(f) = 0$ y f nula equivale a $\mathrm{Ker}(f) = M$, o $\mathrm{Im}(f) = 0$.

Si M es un A-módulo y x es un elemento de M, se denota por Ax el A-submódulo a la izquierda de M generado por x, o sea $Ax = \{ax \mid a \in A\}$ el conjunto de los múltiplos de x. La proposición que sigue ofrece también otra forma de expresar el hecho de que un módulo sea simple:

Proposición 1. 1. 3. *Para un A-módulo M, las siguientes condiciones son equivalentes:* (i) *M es un A-módulo simple, y* (ii) *para todo elemento x de M, $x \neq 0$ tenemos $Ax = M$.*

1. 2. MÓDULOS SEMISIMPLES

Sean A un anillo y M un A-módulo (a la izquierda). Se dice que M es un *A-módulo semisimple* si M es la suma directa de submódulos simples de M. Es claro que todo módulo simple es semisimple, pero hay ejemplos de módulos semisimples que no son simples.

Ejemplo 1. 2. 1. Sean K un cuerpo conmutativo y $A = M_n(K)$ el anillo de matrices cuadradas $n \times n$ con coeficientes en K, donde $n \geq 1$ es un entero. El A-módulo A es semisimple. En efecto, sea I_k el conjunto de matrices (a_{ij}) de A, donde $a_{ij} = 0$ para $i = 1, \ldots, n$, y para $j = 1, \ldots, n$, $j \neq k$. Es fácil ver que I_k es un ideal a la izquierda de A, o sea un A-submódulo a la izquierda de A, que $A = I_1 \oplus \ldots \oplus I_n$ y que cada I_k es un A-módulo simple. En consecuencia, A es un A-módulo semisimple.

Proposición 1. 2. 2. *Sean A un anillo y M un A-módulo. Las siguientes condiciones son equivalentes:* (i) *M es un A-módulo semisimple;* (ii) *M es suma de A-submódulos simples, y* (iii) *todo A-submódulo de M es sumando directo de M.*

La condición (ii) dice que M es suma, no necesariamente directa, de submódulos simples y resulta claro que la condición (i) implica (ii). Supóngase ahora que la condición (ii) se cumple y escribamos $M = \sum_{i \in I} M_i$, donde cada M_i es un A-submódulo simple de M. Sea N un A-submódulo de M y mostremos que N es un sumando directo de M. En efecto, sea $F(I)$ la familia, no vacía, de los subconjuntos J de I tales que la suma $N + \sum_{i \in J} M_i$ sea directa. La familia $F(I)$ es inductiva y, por el lema de Zorn, $F(I)$ admite un elemento maximal J_0, o sea la suma $P = N \oplus \bigoplus_{i \in J_0} M_i$ es directa. Es obvio que si $i \in J - J_0$, entonces $M_i \cap P \neq 0$, pues si fuera $M_i \cap P = 0$, entonces $J_0 \cup \{i\}$ pertenecería a $F(I)$ y, por lo tanto, J_0 no sería maximal. Como M_i es simple, resulta ser $M_i \cap P = M_i$, o sea $M_i \subset P$ para todo i en I. Esto significa que $M \subset P$, esto es $M = P$. Se ha mostrado así que $M = N \oplus \bigoplus_{i \in J_0} M_i$ o, lo que es equivalente, que N es un sumando directo de M. Esto demuestra que la condición (ii) implica (iii). Supóngase ahora que la condición (iii) se cumple y mostremos que el A-módulo M es semisimple, o sea que (iii) implica (i). Para esto, se mostrará inicialmente que M posee un submódulo simple. Sea x un elemento no nulo de M y consideremos la familia $F(x)$ de los submó-

dulos N de M tales que $x \notin N$. Una tal familia es no vacía y es inductiva y, por lo tanto, admite un elemento maximal N_0. Existe, entonces, por hipótesis, un submódulo P de M tal que $N_0 \oplus P = M$. Se afirma que el A-módulo P es simple. En efecto, sea $P_1 \neq 0$ un submódulo de P; por hipótesis, P_1 es sumando directo de P, o sea que existe un A-submódulo P_2 de P tal que $P = P_1 \oplus P_2$ y la maximalidad de N_0 implica que $x \in P_1 \oplus N_0$ y que $x \in P_2 \oplus N_0$, esto es, se puede escribir $x = x_1 + y_1 = x_2 + y_2$, donde $x_i \in P_i$ $(i = 1, 2)$ e $y_i \in N_0$ $(i = 1, 2)$. La condición $y_1 - y_2 = -x_1 + x_2 \in N_0 \cap P = 0$ establece que $x_1 = x_2 = 0$ y, por lo tanto, $x = y_1 = y_2 \in N_0$, lo que es absurdo. Esto demuestra que P es un A-módulo simple. Considérese ahora la familia $(P_i)_{i \in I}$ de los submódulos simples de M de manera tal que la suma $\sum_{i \in I} P_i$ sea directa y que, además, I sea maximal con esa propiedad. Una vez más esto es posible por el lema de Zorn. Resulta ser $M = \bigoplus_{i \in I} P_i$, pues si no lo fuera, se tendría $M = (\bigoplus_{i \in I} P_i) \oplus Q$, donde $Q \neq 0$ es un submódulo de M. Por lo dicho, Q contiene un submódulo simple P_k, con $k \notin I$, y es fácil ver que la suma $\sum_{i \in I \cup \{k\}} P_i$ es directa, lo que contradice la maximalidad de I.

Corolario 1. 2. 3. *Sean A un anillo y $0 \to M' \to M \to M'' \to 0$ una sucesión exacta de A-módulos. Entonces el A-módulo M es semisimple si, y sólo si, los A-módulos M' y M'' son semisimples y la sucesión es escindida.*

En virtud del corolario, todo submódulo y todo módulo cociente de un módulo semisimple es semisimple.

Proposición 1. 2. 4. *Sean A un anillo y M un A-módulo de tipo finito. El A-módulo M es semisimple si, y sólo si, M es suma directa de un número finito de A-módulos simples.*

Como M es semisimple, es suma directa de una familia $(M_i)_{i \in I}$ de A-módulos simples. Sea $\{x_1, \ldots, x_n\}$ un conjunto finito de generadores de M; existe entonces un subconjunto finito J de I tal que $x_i \in \bigoplus_{j \in J} M_j$ $(i = 1, \ldots, n)$, luego $M = \bigoplus_{j \in J} M_j$.

1. 3. ANILLOS SEMISIMPLES

Se dice que un anillo A con elemento unidad es *semisimple* si A, considerado como un A-módulo a la izquierda, es un A-módulo semisimple. El teorema siguiente caracteriza los anillos semisimples:

Teorema 1. 3. 1. *Para un anillo A con elemento unidad, las siguientes condiciones son equivalentes:* (i) *A es un anillo semisimple;* (ii) *todo A-módulo es semisimple;* (iii) *todo A-módulo es proyectivo;* (iv) *todo A-módulo es inyectivo, y* (v) *toda sucesión exacta de A-módulos $0 \to M' \to M \to M'' \to 0$ es escindida.*

La demostración de este importante teorema sobre anillos semisimples es bastante sencilla si se tiene en cuenta lo dicho en los parágrafos anteriores y algunos resultados elementales sobre módulos.

De hecho, si A es un anillo semisimple, esto es un A-módulo semisimple, todo A-módulo libre es semisimple, pues una suma directa de módulos semisimples es también semisimple (cf. el ejercicio 1. 7. 1.). Como todo módulo es cociente de un módulo libre, sigue que todo A-módulo es semisimple. Se demuestra así que (i) $\Rightarrow$ (ii). Supóngase ahora que la condición (ii) se cumpla y sea M un A-módulo. Se sabe que existe una sucesión exacta de A-módulos $0 \to R \to L \to M \to 0$, donde L es libre y R es un submódulo de L. Por el corolario 1. 2. 3., una tal sucesión se escinde y, por lo tanto, M es proyectivo, pues es sumando directo del A-módulo libre L. Esto dice que (ii) $\Rightarrow$ (iii). Admítase ahora que se cumple la condición (iii) y sea M un A-módulo. Se sabe que existe una sucesión exacta de A-módulos $0 \to M \to Q \to S \to 0$, donde Q es un A-módulo inyectivo. Como todo A-módulo es proyectivo, una tal sucesión se escinde y M resulta ser sumando directo de Q, luego inyectivo. Vemos así que (iii) $\Rightarrow$ (iv). Es claro, además, que (iv) (o (iii)) implica trivialmente (v) y que (v) implica inmediatamente (iii) y (iv). Supóngase, finalmente, que se cumple la condición (iii), o sea que todo A-módulo es proyectivo, y sea I un ideal a la izquierda de A. La sucesión exacta de A-módulos a la izquierda $0 \to I \to A \to A/I \to 0$ es, entonces, escindida y, por lo tanto, I es sumando directo de A. La proposición 1. 2. 2., (iii), dice que A es un anillo semisimple. Se ha mostrado que (iii) $\Rightarrow$ (i), con lo que termina la demostración del teorema.

En lo que sigue se darán algunos ejemplos de anillos semisimples.

6

Ejemplo 1. 3. 2. Todo cuerpo es un anillo semisimple. Sin embargo existen ejemplos menos triviales de anillos semisimples que están dados en los ejemplos siguientes.

Ejemplo 1. 3. 3. Sean K un cuerpo conmutativo y $A = M_n(K)$ el anillo de matrices cuadradas $n \times n$ con coeficientes en K. Entonces A es un anillo semisimple (cf. el ejemplo 1. 2. 1.), si bien más adelante se verá (cf. 1. 6.) que, en realidad, A es un anillo simple. Aún más, la conmutatividad de K no es esencial, o sea vale aquí un resultado más general: si K es un anillo con división, entonces $M_n(K)$ es un anillo simple y, recíprocamente, si A es un anillo simple existe un anillo con división K tal que A es isomorfo a $M_n(K)$ para algún entero n (Teorema de Artin-Wedderburn; cf. el teorema 1. 6. 5.).

El ejemplo siguiente muestra un caso importante y no trivial de anillos semisimples. Para ello, hay que recordar antes algunas nociones indispensables para entender el *teorema de Maschke*.

Sean, en efecto, G un grupo y K un anillo con elemento unidad y consideremos el conjunto $K[G]$ de las combinaciones lineales formales $\sum_{\sigma \in G} \lambda_\sigma \sigma$, donde los λ_σ están en K y son casi todos nulos, o sea en tal suma existe solamente un número finito de elementos σ de G, tales que $\lambda_\sigma \neq 0$. Asimismo cabe describir $K[G]$ como sigue: para toda aplicación $u : G \to K$, el *soporte* de u es el conjunto $\mathrm{Sop}(u) = \{\sigma \mid \sigma \in G,\ u(\sigma) \neq 0\}$ y $K[G]$ es el conjunto de las aplicaciones $u : G \to K$ con soporte finito. Es claro que $K[G]$ es un K-módulo a la izquierda libre y una base de $K[G]$ sobre K

está dada por las aplicaciones $e_\sigma : G \to K$, donde $\sigma \in G$, definidas por $e_\sigma(\tau) = \delta_{\sigma\tau}$ para todo τ en G y donde $\delta_{\sigma\tau}$ vale 1, si $\sigma = \tau$, y cero, si $\sigma \neq \tau$ (simbolo de Kronecker). La estructura de anillo con elemento unidad de $K[G]$ es dada por la multiplicación $(uu')(\tau) = \sum_{\sigma\sigma' = \tau} u(\sigma)\, u'(\sigma')$ para todo τ en G y cualesquiera que sean u y u' en $K[G]$. En términos de combinaciones lineales formales, la multiplicación de $K[G]$ se escribe $(\sum_\sigma \lambda_\sigma e_\sigma)(\sum_\sigma \mu_\sigma e_\sigma) = \sum_{\sigma,\tau} \lambda_\sigma \mu_\tau e_\sigma e_\tau$, donde los λ_σ y los μ_σ están en K y donde $e_\sigma\, e_\tau = e_{\sigma\tau}$, cualesquiera que sean σ y τ en G. De este modo, se define sobre $K[G]$ una estructura de anillo con elemento unidad. Además, *el anillo $K[G]$ es conmutativo si, y sólo si, K es un anillo conmutativo y G es un grupo abeliano*. Se dice que $K[G]$ es el *anillo de grupo* de G sobre K.

El tercer ejemplo de anillo semisimple está dado por el siguiente teorema:

Teorema 1.3.4 (Teorema de Maschke). *Sean K un cuerpo conmutativo y G un grupo finito de orden n. Si la característica de K no divide a n, entonces $K[G]$ es un anillo semisimple* (a la izquierda y a la derecha).

Sea N un ideal a la izquierda de $K[G]$; basta mostrar que N es un sumando directo de $K[G]$ y aplicar la proposición 1.2.2. (iii). En otras palabras, $K[G]$ es un anillo semisimple. Si se consideran N y $K[G]$, K-espacios vectoriales, N es un sumando directo de $K[G]$, luego existe una aplicación K-lineal $f : K[G] \to N$ tal que $f(x) = x$ para todo x en N. Por otra parte, el hecho de que la característica de K y n sean números primos entre sí implica que n tiene inverso en K o, precisando aún más, que $n \cdot 1$ tiene inverso en K, donde 1, es el elemento unidad de K. Cabe entonces considerar la aplicación $\varphi : K[G] \to N$ definida por

$$\varphi(x) = \frac{1}{n} \sum_{\sigma \in G} \sigma f(\sigma^{-1} x)$$

para todo x en $K[G]$. Mostremos que φ es $K[G]$-lineal. En efecto, para todo τ en G, se tiene $\varphi(\tau x) = \frac{1}{n} \sum_{\sigma \in G} \sigma f(\sigma^{-1}\tau x) = \tau(\frac{1}{n} \sum_{\sigma \in G} \tau^{-1}\sigma f((\tau^{-1}\sigma)^{-1} x) =$

$= \tau(\frac{1}{n} \sum_{\sigma \in G} \sigma f(\sigma^{-1} x)) = \tau\, \varphi(x)$, cualquiera que sea x en $K[G]$. Como φ es K-lineal, resulta que φ es también $K[G]$-lineal. Finalmente, como para todo x en N se tiene $\varphi(x) = \frac{1}{n} \sum_{\sigma \in G} \sigma\, \sigma^{-1} x = \frac{1}{n} \sum_{\sigma \in G} x = x$, se concluye que N es un $K[G]$-sumando directo de $K[G]$.

A continuación se estudiará con más detalle la teoría de anillos semisimples, para después pasar a los anillos simples.

Proposición 1.3.5. *Sea A un anillo semisimple. Todo A-módulo a la izquierda simple es isomorfo a un ideal a la izquierda minimal de A.*

Sean M un A-módulo a la izquierda simple y $x \neq 0$ un elemento de M. La aplicación A-lineal $A \to M$, definida por $a \mapsto ax$, es sobreyectiva y su núcleo I es un ideal a la izquierda de A, luego es un sumando directo de A, o sea existe un ideal a la izquierda J de A tal que $I \oplus J = A$. Esto dice que existen isomorfismos de A-módulos a la izquierda $J \approx A/I \approx M$ y que J es minimal, pues M es simple.

Corolario 1.3.6. *Sea A un anillo semisimple. Todo A-módulo a la izquierda es isomorfo a una suma directa de ideales a la izquierda minimales de A. En particular, todo A-módulo a la izquierda de tipo finito es isomorfo a una suma directa de un número finito de ideales a la izquierda minimales de A.*

El corolario resulta de la proposición anterior y de las proposiciones 1.2.2. y 1.2.4.

Proposición 1.3.7. *Sean A un anillo semisimple y $A = A_1 \oplus \ldots \oplus A_n$ una descomposición de A en suma directa de ideales a la izquierda minimales. Entonces, todo ideal a la izquierda minimal de A es isomorfo, como A-módulo a la izquierda, a algún A_i.*

Si I es un ideal a la izquierda minimal de A, no puede ser $A_i I = 0$ para todo i, pues en tal caso se tendría $AI = 0$, luego $I = 0$. Existe, por consiguiente un índice i, $1 \leq i \leq n$, tal que $A_i I \neq 0$, luego, en virtud del lema 1.3.8., I es isomorfo a A_i, ambos considerados A-módulos a la izquierda. El lema siguiente finaliza la demostración de la proposición:

Lema 1.3.8. *Sean A un anillo con elemento unidad e I y J ideales a la izquierda minimales de A. Entonces $IJ = 0$ o $I \approx J$, isomorfismo de A-módulos a la izquierda*

Si I y J son ideales a la izquierda del anillo A, el producto IJ es también un ideal a la izquierda de A contenido en J, y por la minimalidad de J, resulta ser $IJ = 0$ o $IJ = J$. Si $IJ = J$, existe un elemento $y \in J$, $y \neq 0$ tal que $Iy \neq 0$, luego $Iy = J$, pues Iy es un ideal a la izquierda de A contenido en J. La aplicación $I \to J$, definida por $x \mapsto xy$, es A-lineal, sobreyectiva y su núcleo es un ideal a la izquierda de A contenido en I. Como tal núcleo no puede ser igual a I, pues en tal caso se tendría $Iy = 0$, él es necesariamente nulo, debido a la minimalidad de I. Luego la aplicación $I \to J$ definida es un isomorfismo de A-módulos.

En realidad, la proposición 1.3.7. vale en condiciones más generales y su demostración es similar a la que se acaba de dar:

Proposición 1.3.9. *Sean A un anillo semisimple, M un A-módulo a la izquierda de tipo finito y $M = A_1 \oplus \ldots \oplus A_n$ una descomposición de M en ideales a la izquierda minimales de A. Entonces todo A-submódulo simple de M es isomorfo, como A-módulo a la izquierda, a algún A_i.*

1.4. SOBRE EL RADICAL

Se ha dicho ya que si A es un anillo con elemento unidad y M un A-módulo a la izquierda de tipo finito, entonces M tiene submódulos maximales (cf. la proposición 1.1.1.). Dado un A-módulo a la izquierda M, no necesariamente de tipo finito, el *radical* de M es el submódulo $R(M)$ de M, intersección de los submódulos maximales de M. Pero puede ocurrir que un módulo M no tenga submódulos maximales y en este caso se pondrá $R(M) = M$. Si M es un A-módulo de tipo finito, necesariamente $R(M) \subsetneq M$. El radical de un anillo A es el radical de A considerado como A-módulo a la izquierda.

Proposición 1.4.1. *El radical de un anillo A es un ideal bilátero de A.*

Es claro que si A es un anillo, $R(A)$ es un ideal a la izquierda de A, pues se trata de una intersección de ideales a la izquierda de A. Probemos que $R(A)$ es también un ideal a la derecha de A y para esto mostremos que cualesquiera que sean a en $R(A)$ y b en A, se tiene $ab \in R(A)$. En efecto, sean $a \in R(A)$ y $b \in A$, y considérese el conjunto $J = \{c \mid c \in A, cb \in I\}$, donde I es un ideal a la izquierda maximal de A. Es evidente que J es un ideal a la izquierda de A y, por lo tanto, surgen dos posibilidades: o bien $J = A$ y, en este caso, $a \in J$, o sea $ab \in I$, o bien $J \subsetneq A$ y, por lo tanto, J está contenido en un ideal a la izquierda maximal M de A. Mostremos que $J = M$. Sea $x \in M$ y consideremos el ideal a la izquierda $I + Axb$. Por la maximalidad de I resulta $I + Axb = I$ o $I + Axb = A$. En el primer caso, se tiene $xb \in I$, luego $x \in J$, y en el segundo caso, se escribe $b = c + axb$ con $c \in I$ y $a \in A$. Esto pone de manifiesto que $(1 - ax)b = c$ y, por lo tanto, $1 - ax \in J$, o sea $1 - ax \in M$. Como $ax \in M$, resulta $1 \in M$, lo que es absurdo. Así, hay que eliminar el segundo caso, esto es, vale solamente la primera posibilidad y ella es que $M = J$. Como $a \in R(A)$, resulta ser $a \in J$, luego $ab \in I$. Pero esto tiene validez cualquiera que sea el ideal a la izquierda maximal I de A, lo que implica que $ab \in R(A)$.

Proposición 1.4.2. *Sean A un anillo y M un A-módulo a la izquierda. Entonces $R(A)M \subset R(M)$.*

Sean $a \in R(A)$, $x \in M$ y mostremos que $ax \in R(M)$, o sea que para todo submódulo maximal N de M, $ax \in N$. Para esto, considérese la aplicación A-lineal $\varphi : A \to M/N$, definida por $c \mapsto c\bar{x}$, donde $\bar{x}$ en M/N es la clase de x módulo N. Como N es maximal en M, el A-módulo cociente M/N es simple y, por lo tanto, $\varphi(A) = 0$ ó $\varphi(A) = M/N$. En el primer caso, $x \in N$, luego $ax \in N$, y en el segundo caso, φ es sobreyectiva. Su núcleo I es un ideal maximal de A y φ induce un isomorfismo de A-módulos a la izquierda $A/I \cong M/N$ dado por $\bar{c} \mapsto c\bar{x}$, donde $\bar{c}$ en A/I es la clase de c módulo I. Como $\bar{a} = 0$ en A/I, pues $a \in I$, entonces $a\bar{x} = 0$ en M/N, luego $ax \in N$.

Adviértase que si el A-módulo M no tiene submódulos maximales, la proposición 1.4.2. es trivial pues en este caso $R(M) = M$.

Ejemplo 1.4.3. El $\mathbf{Z}$-módulo $\mathbf{Q}$ no admite ni submódulos simples ni módulos cocientes simples y, por lo tanto, el $\mathbf{Z}$-módulo $\mathbf{Q}$ no tiene submódulos maximales. Esto implica $R(\mathbf{Q}) = \mathbf{Q}$; $\mathbf{Q}$ se considera como $\mathbf{Z}$-módulo.

Proposición 1.4.4. (Lema de Nakayama). *Sean A un anillo, M un A-módulo a la izquierda de tipo finito y N un A-submódulo de M tal que $M = N + IM$, donde I es un ideal de A contenido en el radical $R(A)$ de A. Entonces $M = N$.*

Si se supone que $N \subsetneq M$, entonces N está contenido en algún submódulo maximal P de M; un tal submódulo existe, pues M es un A-módulo de tipo finito. Luego, $N + IM \subset P + R(A)M \subset M$, o sea $P + R(A)M = M$. Como, por la proposición anterior, $R(A)M \subset P$, entonces $P = M$, lo que es absurdo. Esto demuestra la proposición.

Otra versión del lema de Nakayama es la que sigue y es de utilidad para obtener resultados ulteriores.

Proposición 1.4.5. (Lema de Nakayama). *Sean A un anillo, M un A-módulo a la izquierda de tipo finito y N un A-submódulo de M tal que $N + R(M) = M$. Entonces $N = M$.*

Supóngase que $N \subsetneq M$, existe un submódulo maximal P de M tal que $N \subset P$, luego $M = N + R(M) \subset P + R(M) \subset M$, o sea $P + R(M) = M$ y como $R(M) \subset P$, sigue que $P = M$, lo que no es posible, pues P es maximal.

Esto permite demostrar ahora el siguiente teorema, el cual es una caracterización muy útil del radical de un módulo:

10

Teorema 1.4.6. *Sean A un anillo, M un A-módulo a la izquierda de tipo finito y $\{x_1, \ldots, x_n\}$ un conjunto finito de generadores de M. Una condición necesaria y suficiente para que un elemento $x \in M$ pertenezca a $R(M)$ es que cualesquiera que sean los elementos $a_1, \ldots, a_n$ de A, los elementos $x_1 + a_1x, \ldots, x_n + a_nx$ formen un sistema de generadores de M.*

En efecto, supóngase que $x \in R(M)$ y sea N el A-submódulo de M generado por los elementos $x_1 + a_1x, \ldots, x_n + a_nx$. La identidad $(x_i + a_ix) - a_ix = x_i$ $(i = 1, \ldots, n)$ dice que $N + R(M) = M$, luego $N = M$. Recíprocamente, supóngase que se cumple la hipótesis del teorema, pero que $x \notin R(M)$. Existe, entonces, un A-submódulo a la izquierda maximal N de M tal que $x \notin N$ y, por lo tanto, $Ax + N = M$. Luego, para cada índice i, $1 \leq i \leq n$, existe un elemento a_i en A tal que $x_i + (-a_i)x \in N$ $(i = 1, \ldots, n)$. Puesto que los elementos $x_i + (-a_i)x$ $(i = 1, \ldots, n)$ generan M como A-módulo a la izquierda, entonces $M = N$, lo que es absurdo.

Corolario 1.4.7. *Sea A un anillo. El radical $R(A)$ del anillo A es el conjunto de los elementos x de A tales que $1 - ax$ sea inversible a la izquierda en A, para todo elemento a en A.*

Por ser 1 generador del A-módulo a la izquierda A, basta aplicar el teorema anterior, que dice que una condición necesaria y suficiente para que un elemento x de A esté en $R(A)$ es que $1 - ax$ sea un generador del A-módulo a la izquierda A, para todo elemento $a \in A$. En consecuencia, esto ocurre si, y sólo si, se puede escribir $1 = a(1 - ax)$ con $a \in A$, o sea si, y sólo si, $1 - ax$ es inversible a la izquierda en A, para todo $a \in A$.

Corolario 1.4.8. *El radical $R(A)$ de un anillo A es el más grande de los ideales bilateros I de A tales que $1 - x$ sea inversible en A para todo elemento $x \in I$.*

Sea $x \in R(A)$. Por el corolario anterior, $1 - x$ es inversible a la izquierda en A, o sea existe un elemento $a \in A$ tal que $a(1 - x) = 1$. Sea $b = 1 - a$; como $b = 1 - a = -ax \in R(A)$, existe un elemento $c \in A$ tal que $1 = c(1 - b) = ca$, es decir, a es inversible también a la izquierda, luego a es inversible en A. Así, $1 - x = a^{-1}$ es también inversible en A. Esto demuestra el corolario.

1.5. ANILLOS ARTINIANOS

La noción de anillo artiniano aparece por primera vez en el trabajo fundamental de Artin,[3] y se define a partir del siguiente resultado:

Proposición 1.5.1. *Para un anillo A con elemento unidad, las siguientes condiciones son equivalentes:* (i) *Todo conjunto no vacío de ideales a la izquierda de A tiene un elemento mínimal.* (ii) *Toda cadena descendiente $I_1 \supset I_2 \supset \ldots \supset I_n \supset \ldots$ de ideales a la izquierda de A es estacionaria, esto es, existe un entero $m \geq 1$ tal que $I_k = I_m$ para todo $k \geq m$.*

Supóngase que se cumpla la condición (i) y considérese el conjunto $\mathcal{C} = \{I_1, \ldots, I_n, \ldots,\}$; $\mathcal{C}$ tiene, por hipótesis, un elemento minimal I_m, o sea $I_k \supset I_m$ para todo k. Pero, por otra parte, $I_k \subset I_m$ para todo $k \geq m$, o sea, $I_k = I_m$ para todo $k \geq m$. Esto demuestra la condición (ii). Si ahora se cumple la condición (ii), considérese un conjunto $\mathcal{C}$ no vacío de ideales a la izquierda de A. Tómese $I_1 \in \mathcal{C}$. O bien I_1 es minimal en $\mathcal{C}$ o I_1 contiene algún elemento I_2 de $\mathcal{C}$. De nuevo, o bien I_2 es minimal o I_2 contiene un elemento I_3 de $\mathcal{C}$. Se construye así una cadena descendiente $I_1 \supset I_2 \supset \ldots \supset I_n \supset \ldots$ de ideales a la izquierda de A y, por lo tanto, existe un entero $m \geq 1$ tal que $I_k = I_m$ para todo $k \geq m$. El elemento I_m es un elemento minimal de $\mathcal{C}$. Queda demostrado así que la condición (i) se verifica.

Un anillo que verifica las condiciones equivalentes de la proposición anterior se denomina *anillo artiniano a la izquierda*. Una definición análoga puede ser dada para *anillo artiniano a la derecha* y un anillo se dice *artiniano* si es, a la vez, artiniano a la izquierda y a la derecha.

Proposición 1.5.2. *Un anillo con elemento unidad es semisimple si, y sólo si, es artiniano y sin radical.*

Recuérdese que un anillo A con elemento unidad se dice *sin radical*, si $R(A) = 0$. Supóngase que A sea un anillo semisimple. Es claro que A es artiniano y se demostrará que $R(A) = 0$. Sean $a \neq 0$ un elemento de A y $A = A_1 \oplus \ldots \oplus A_n$ la descomposición de A en una suma directa de ideales a la izquierda minimales. Entonces $a = a_1 + \ldots + a_n$, donde $a_i \in A_i (i = 1, \ldots, n)$, y se puede suponer, por ejemplo, que $a_n \neq 0$. Resulta, entonces, que $a \notin A_1 \oplus \ldots \oplus A_{n-1}$ y como $A_1 \oplus \ldots \oplus A_{n-1}$ es un ideal a la izquierda maximal de A, se tiene $a \notin R(A)$. Recíprocamente, supóngase que A sea artiniano (a la izquierda) y que $R(A) = 0$ y muéstrese que A es semisimple. Para esto, sea I un ideal a la izquierda de A y muéstrese que I es sumando directo de A. Considérese entonces el conjunto de los ideales

a la izquierda J de A tales que $I + J = A$. Tal conjunto es no vacío, pues $I + A = A$, luego admite un elemento minimal J y basta mostrar ahora que $I \cap J = 0$. Supóngase que $I \cap J \neq 0$ y sea $B \neq 0$ un ideal a la izquierda minimal de A contenido en $I \cap J$. Como $R(A) = 0$, existe un ideal maximal M de A que no contiene a B y, por lo tanto, $A = B + M$. Por ser $B \subset J$, entonces $J \not\subset M$ y en consecuencia $J' = M \cap J \subsetneq J$, y como se tiene también $(B + M) \cap J \subset B + J'$, resulta $A = I + J = I + (B + M) \cap J \subset I + B + J' = I + J'$, o sea $A = I + J'$, lo que es contrario a que J sea minimal con la propiedad $A = I + J$. Luego, $I \cap J = 0$, lo que demuestra la proposición.

Corolario 1.5.3. *Si A es un anillo artiniano, el anillo cociente $A/R(A)$ es semisimple.*

Como el anillo cociente $A/R(A)$ es artiniano y $R(A/R(A)) = 0$, entonces $A/R(A)$ es un anillo semisimple.

Véase ahora cómo la noción de nilpotencia interviene en la teoría de anillos artinianos. Si A es un anillo, un elemento a de A se dice *nilpotente* si existe un entero $m \geq 1$ tal que $a^m = 0$ y un ideal a la izquierda I de A se dice *nilpotente* si existe un entero $m \geq 1$ tal que $I^m = 0$, donde I^m es el ideal a la izquierda de A definido inductivamente por $I^1 = I$ e $I^n = I^{n-1} I$. Adviértase que decir que $I^m = 0$ equivale a decir que para toda familia $a_1, \ldots, a_m$ de elementos de I se tiene $a_1 \ldots a_m = 0$. Resulta claro que si un ideal es nilpotente, sus elementos son todos nilpotentes, pero la recíproca es falsa.

12

Ejemplo 1.5.4. Sean $\mathbf{Z}$ el anillo de números enteros y $p \geq 2$ un número primo, y considérese, en el anillo producto $A = \prod_{n \geq 1} \mathbf{Z}/(p^n)$, el ideal I definido por $I = \bigoplus_{n \geq 1} (p)/(p^n)$. Es fácil ver que los elementos de I son todos nilpotentes, pero el ideal I no lo es.

Un ideal I de un anillo A se dice un *nilideal* si todo elemento de I es nilpotente. Así, si bien todo ideal nilpotente es un nilideal, un nilideal no es necesariamente nilpotente, como muestra el ejemplo dado (ejemplo 1.5.4.). Sin embargo, hay un caso en que esto es cierto, a saber:

Lema 1.5.5. *Sean A un anillo e I un ideal a la izquierda de A de tipo finito. Si I es un nilideal, entonces I es un ideal nilpotente.*

Sea, en efecto, $\{x_1, \ldots, x_n\}$ un conjunto de generadores del ideal I; para cada índice i, $1 \leq i \leq n$, existe un entero $m_i \geq 1$ tal que $x_i^{m_i} = 0$ ($i = 1, \ldots, n$). Basta tomar $m = m_1 + \ldots + m_n$ para ver que $I^m = 0$, o sea el ideal I es nilpotente.

Para un anillo A con elemento unidad, sea $J(A)$ la suma de todos los ideales a la izquierda nilpotentes de A. Es claro que $J(A)$ es un ideal a la izquierda de A y se tiene la siguiente proposición:

Proposición 1.5.6. *Sea A un anillo con elemento unidad. Todo nilideal a la izquierda de A está contenido en $R(A)$ y, en particular $J(A) \subset R(A)$.*

La proposición resulta inmediatamente del siguiente lema:

Lema 1.5.7. *Sean A un anillo con elemento unidad e I un ideal a la izquierda de A tal que $I \nsubseteq R(A)$. Entonces I contiene elementos no nilpotentes.*

Si I es un ideal a la izquierda de A tal que $I \nsubseteq R(A)$, existe un ideal a la izquierda maximal M de A tal que $I \nsubseteq M$, luego $I + M = A$. Se puede entonces escribir $1 = a + b$ con $a \in I$ y $b \in M$ y, por ende, $ab = a(1 - a) = (1 - a)a = ba$ y, por tanto, para todo entero $n \geq 1$ se tiene $1 = (a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$. Si a fuera nilpotente, existiría un entero $m \geq 1$ tal que $a^m = 0$ y esto implicaría $1 = \sum_{k=0}^{m} \binom{m}{k} a^k b^{m-k} = (b^{m-1} + \binom{m}{1} ab^{m-2} + \ldots + \binom{m}{m-1} a^{m-1})b$, o sea $1 \in M$, lo que es absurdo.

Proposición 1.5.8. *El radical de un anillo artiniano es un ideal nilpotente.*

Sean A un anillo artiniano y R su radical. La cadena descendiente $R \supset R^2 \supset \ldots \supset R^n \supset \ldots$ de ideales biláteros de A es estacionaria, es decir existe un entero $m \geq 1$ tal que $R^k = R^m$, para todo $k \geq m$. Sea $I = R^m$ y supóngase que R no sea nilpotente. El conjunto $\mathcal{C}$ de los ideales a la izquierda J de A tales que $IJ \neq 0$ e $IJ \subset I$ es no vacío, pues $I \neq 0$ e $I^2 = I$ y, por lo tanto, admite un elemento minimal J. Como $I(IJ) = IJ \neq 0$ e $I(IJ) = IJ \subset I$, entonces IJ pertenece aún al conjunto $\mathcal{C}$ y, por la minimalidad de J y el hecho de que $IJ \subset J$, resulta $IJ = J$. Si se muestra que J es un A-módulo a la izquierda de tipo finito, como $IJ = J$ e $I \subset R(A)$, por el lema de Nakayama $J = 0$, lo que es absurdo. Sean entonces $a \in I$ y $b \in J$ tales que ab sea un elemento no nulo de J. El ideal a la izquierda Ab está contenido en J y, además, $I(Ab) \neq 0$ e $I(Ab) \subset IJ \subset I$, o sea Ab pertenece al conjunto $\mathcal{C}$. Por la minimalidad de J se concluye que $J = Ab$ y J es un A-módulo a la izquierda de tipo finito. Esto concluye la demostración de la proposición.

Corolario 1.5.9. *En un anillo artiniano, el radical es la suma de todos los ideales a la izquierda (o a la derecha) nilpotentes.*

El corolario dice que si A es un anillo artiniano, el radical de A se escribe $R(A) = J(A)$. Además, la proposición 1.5.8. también puede enunciarse de la siguiente manera: *el radical de un anillo artiniano A es el más grande ideal bilatero nilpotente de A.* En el caso de un anillo conmutativo se pueden dar resultados más precisos, a saber:

Corolario 1.5.10. *El radical de un anillo artiniano conmutativo es el conjunto de sus elementos nilpotentes.*

Finalmente, para terminar este parágrafo se mencionará el *teorema de estructura de anillos artinianos conmutativos*, pero sin demostrarlo. Su demostración requiere técnicas de álgebra conmutativa cuyo planteamiento sería muy largo de exponer aquí (cf. [4], teorema 8.7.).

Teorema 1.5.11. (Teorema de Estructura). *Un anillo artiniano conmutativo es, de manera única a menos de un isomorfismo, un producto directo de un número finito de anillos artinianos conmutativos locales.*

El Teorema de Estructura tiene una consecuencia muy importante, parte de la cual está dada por la proposición 1. 5. 2. :

Corolario 1. 5. 12. *Para un anillo conmutativo A con elemento unidad, las siguientes condiciones son equivalentes:* (i) *A es un anillo artiniano y su único elemento nilpotente es cero;* (ii) *A es un anillo semisimple, y* (iii) *A es producto directo de un número finito de cuerpos.*

1. 6. ANILLOS SIMPLES

Un anillo artiniano A se llama *simple* si $A \neq 0$ y si A no tiene ideales bilateros propios, o sea los únicos ideales bilateros de A son 0 y A. Como el radical de un anillo es un ideal bilátero, se sigue (cf. proposición 1. 5. 2.) que *todo anillo simple es semisimple.* Sin embargo, hay ejemplos de anillos semisimples que no son simples (cf. el teorema 1. 3. 4.). Obsérvese que un anillo simple A no es necesariamente un A-módulo a la izquierda (o a la derecha) simple (cf. el ejemplo 1. 6. 4.).

Teorema 1. 6. 1. *Un anillo A es simple si, y sólo si, A se descompone como suma directa de ideales a la izquierda mínimales, todos isomorfos entre sí como A-módulos a la izquierda.*

Sea A un anillo semisimple; si A admite una descomposición $A = A_1 \oplus \ldots \oplus A_n$ como suma directa de ideales a la izquierda minimales dos a dos no isomorfos (cf. la proposición 1. 3. 7.), entonces $A_i A_j = 0$, para $i \neq j$, y $A_i A = A_i A_i \subset A_i$, o sea $A_i A = A_i$ para $i = 1, \ldots, n$. Esto quiere decir que cada A_i es también un ideal a la derecha y, por consiguiente, un ideal bilátero de A.

Resulta entonces de esta observación que si A es un anillo simple, puede escribirse $A = A_1 \oplus \ldots \oplus A_n$ como suma directa de ideales a la izquierda minimales (pues A es semisimple) todos isomorfos entre ellos, puesto que A tiene como únicos ideales biláteros a 0 y A. La recíproca del teorema es inmediata.

Corolario 1. 6. 2. *Un anillo es semisimple si, y sólo si, es el producto directo de un número finito de anillos simples.*

Sea A un anillo semisimple. Hemos visto que A admite una descomposición $A = A_1 \oplus \ldots \oplus A_n$, donde cada A_i es un ideal bilátero de A y $A_i A_j = 0$ para $i \neq j$. Además, es claro que cada A_i es un anillo simple y que $A = A_1 \oplus \ldots \oplus A_n$ es un producto directo de anillos. La recíproca es inmediata.

El paso siguiente es el *Teorema de Wedderburn* que dice esencialmente que todo anillo simple es el anillo de endomorfismos de un módulo libre de rango finito sobre un anillo con división. Obsérvese que un anillo A se dice un *anillo con división* si cualesquiera que sean a y b en A, $a \neq 0$, las ecuaciones $ax = b$ y $xa = b$ tienen soluciones únicas en A.

Lema 1. 6. 3. *Sean A un anillo con división y M un A-módulo libre de rango n. Entonces el anillo $\mathrm{End}_A(M)$ de los A-endomorfismos de M es simple.*

Como $\mathrm{End}_A(M)$ es isomorfo al anillo $M_n(A)$ de matrices cuadradas $n\times n$ con coeficientes en A, donde n es el rango de M, es suficiente mostrar que el anillo $M_n(A)$ es simple. Para esto, designemos por A_i el conjunto de las matrices $n\times n$ de $M_n(A)$, cuyas columnas distintas de la i-ésima son todas nulas, y donde $1 \leq i \leq n$. Es evidente que A_i es un ideal a la izquierda de $M_n(A)$ y que $M_n(A) = A_1 \oplus \ldots \oplus A_n$. Además, cada A_i es un ideal minimal de $M_n(A)$. En efecto, si a y b son elementos de A_i, con $a \neq 0$, existe un elemento x en $M_n(A)$ tal que $xa = b$, pues si se supone, por ejemplo, que $a = (a_{ij})$ y que existen índices i y j tales que $a_{ij} \neq 0$, basta definir $x = (x_{kl})$ por $x_{kl} = 0$ si $l \neq i$ y $x_{ki}a_{ij} = b_{kj}$, donde $b = (b_{kj})$. Entonces $xa = b$, lo que demuestra la minimalidad de $A_i (i = 1, \ldots, n)$. Se demostrará ahora que los A_i son todos isomorfos cuando se consideran ideales a la izquierda de $M_n(A)$. Considérese para esto la aplicación $f : A_i \to A_j$, definida por $a \mapsto f(a)$, donde $f(a)_{kl} = 0$ si $l \neq j$ y $f(a)_{kj} = a_{ki}$, donde indicamos con $a = (a_{ij})$. Es inmediato verificar que $f(ab) = af(b)$, cualesquiera que sean $a \in M_n(A)$ y $b \in A_i$, o sea f es una aplicación $M_n(A)$-lineal. Además, $f : A_i \to A_j$ es un isomorfismo de $M_n(A)$-módulos a la izquierda, con lo que termina la demostración del lema.

Ejemplo 1.6.4. El lema anterior expresa, en particular, que si K es un cuerpo conmutativo, el anillo $A = M_n(K)$ de matrices cuadradas $n\times n$ con coeficientes en K es un anillo simple, es decir no tiene otros ideales bilateros que 0 y A, aunque sí tiene ideales a la izquierda no nulos propios. Esto muestra que A es simple como anillo, pero no como A-módulo a la izquierda.

Sean A un anillo con elemento unidad, M un A-módulo a la izquierda y considérese el anillo $A' = \mathrm{End}_A(M)$ de A-endomorfismos de M. La ley de composición $a'x = a'(x)$ cualesquiera que sean $a' \in A'$ y $x \in M$ define sobre M una estructura de A'-módulo a la izquierda y, por lo tanto, se puede considerar el anillo $A'' = \mathrm{End}_{A'}(M)$ de los A'-endomorfismos de M. Sea $L : A \to A''$ la aplicación definida por $a \mapsto L_a$, donde $L_a(x) = ax$ para todo $x \in M$. Cualesquiera que sean $a \in A$, $b' \in A'$ y $x \in M$ se tiene $L_a(b'x) = L_a(b'(x)) = ab'(x) = b'(ax) = b'ax = b'L_a(x)$, o sea $L_a \in A''$ para todo $a \in A$. Resulta fácil ver que cualesquiera que sean a y b en A, $L_{ab} = L_a \circ L_b$; en otras palabras, $L : A \to A''$ es un morfismo de anillos.

Veamos ahora bajo qué condiciones $L : A \to A''$ es un isomorfismo de anillos. Se sabe que $\mathrm{Ker}(L)$ es un ideal bilátero de A y $\mathrm{Ker}(L) \neq A$, o sea $L \neq 0$ pues $L(1) = \mathrm{id}_M$. Luego, si A es un anillo simple, necesariamente $\mathrm{Ker}(L) = 0$. Esto dice que si A es un anillo simple, el morfismo de anillos $L : A \to A''$ es inyectivo.

Respecto a la sobreyectividad de $L : A \to A''$, supóngase que M sea un ideal a la izquierda de A, $M \neq 0$, pues si $M = 0$, L es trivialmente sobreyectivo. Entonces $L(M)$ es un ideal a la izquierda de $L(A)$ y se mostrará que, de hecho, $L(M)$ es un ideal a la izquierda de A''. En efecto, obsérvese que cualesquiera que sean $a \in A$ y $x, y \in M$, se tiene $R_x(ay) = (ay)x = a(yx) = aR_x(y)$, o sea $R_x \in A'$ para todo $x \in M$. Así, para todo $a'' \in A''$ y cualquiera que sea $x \in M$, se tiene $(a'' \circ L_x)(y) = a''(L_x(y)) = a''(R_y(x)) = a''(R_yx) = R_ya''(x) = a''(x)y = L_{a''(x)}(y)$, para todo $y \in M$, esto es $a'' \circ L_x = L_{a''(x)}$ cualesquiera que sean $a'' \in A''$ y $x \in M$. Se ha demostrado así que $L(M)$ es un ideal a la izquierda de A''. Es sabido ya que $AM \subset M$, pues M es un ideal a la izquierda de A y sea MA el ideal a la de-

recha de A definido por M. Cualesquiera que sean $y \in A$ y $xa \in MA$ se tiene $y(xa) = (yx)a \in MA$, es decir MA es también un ideal a la izquierda, esto es un ideal biláteo de A. Como A es un anillo simple y $MA \neq 0$, necesariamente $MA = A$. Esto permite escribir $1 = \sum_i x_i a_i$ (suma finita), donde los x_i están en M y los a_i están en A. Se mostrará que, para todo elemento $a'' \in A''$, se tiene $a'' = L(\sum_i a''(x_i)a_i)$, con lo que se demuestra que el morfismo $L : A \to A''$ es sobreyectivo y, por lo tanto, es un isomorfismo de anillos. Para demostrar la última fórmula basta observar que $L(\sum_i a''(x_i)a_i) = \sum_i L_{a''(x_i)} \circ L_{a_i}$ y que, para todo $x \in M$, se tiene $(\sum_i L_{a''(x_i)} \circ L_{a_i})(x) = \sum_i L_{a''(x_i)}(a_i x) = \sum_i (a'' \circ L_{x_i})(a_i x) = \sum_i a''(x_i a_i x) = a''((\sum_i x_i a_i)x) = a''(x)$, esto es $a'' = L(\sum_i a''(x_i)a_i)$.

Esta demostración, debida a M. A. Rieffel,[22] da una parte del siguiente teorema (de Wedderburn o de Artin-Wedderburn):

Teorema 1.6.5 (Teorema de Wedderburn). *Sean A un anillo simple, $A = A_1 \oplus \ldots \oplus A_n$ la descomposición de A como suma directa de ideales a la izquierda minimales isomorfos, $M \neq 0$ un ideal a la izquierda de A y $A' = \mathrm{End}_A(M)$ el anillo de A-endomorfismos de M. Entonces, el morfismo $L : A \to \mathrm{End}_{A'}(M)$ es un isomorfismo de anillos. Si, además, M es minimal, A' es un anillo con división y M es un A'-módulo libre de rango n.*

16

Parte del teorema ya fue demostrada. Supóngase ahora que M sea un ideal a la izquierda minimal de A y sean $a', b' \in A'$, $a' \neq 0$. Se trata de resolver, en A', las ecuaciones $a' \circ x' = b'$ y $x' \circ a' = b'$. Veamos la primera ecuación, a saber: $a' \circ x' = b'$. O bien $b' = 0$ y, en este caso, una solución de la ecuación $a' \circ x' = 0$ es $x' = 0$ o $b' \neq 0$ y, en este caso, una solución de $a' \circ x' = b'$, si tal solución existe, es $x' \neq 0$. Así, dado $x \in M$, existe $y \in M$ tal que $a'(y) = b'(x)$, pues M es minimal y $a' \neq 0$ y $b' \neq 0$. Si se define $x' : M \to M$ por $x'(x) = y$, es claro que $x' \in A'$ y $a' \circ x' = b'$. Una consideración análoga permite resolver, en A', la ecuación $x' \circ a' = b'$. Para mostrar que tales soluciones *son únicas*, sean $a', b' \in A'$ tales que $a' \circ b' = 0$. Si se supone que $b' \neq 0$, existe un elemento $x \in M$ tal que $b'(x) \neq 0$, luego $\mathrm{Ker}(a') \neq 0$, pues $b'(x) \in \mathrm{Ker}(a')$. La minimalidad de M dice que $\mathrm{Ker}(a') = M$, o sea $a' = 0$. Esto demuestra que A' es un anillo con división. Finalmente, la descomposición $A = A_1 \oplus \ldots \oplus A_n$ expresa que $1 = e_1 + \ldots + e_n$, donde $e_i \in A_i$ $(i = 1, \ldots, n)$, $e_i^2 = e_i$ $(i = 1, \ldots, n)$ y $e_i e_j = 0$ para $i \neq j (i, j = 1, \ldots, n)$. Como, para todo $x \in M$ se tiene $x = e_1 x + \ldots + e_n x$, entonces $M = e_1 M \oplus \ldots \oplus e_n M$ y se demostrará que ésta es una descomposición de M como suma directa de A'-módulos. En efecto, para todo $a' \in A'$ y para todo $x \in M$, $a' e_i x = a'(e_i x) = e_i a'(x) \in e_i M (i = 1, \ldots, n)$, lo que muestra que cada $e_i M$ es un A'-módulo. Además, es evidente que la suma $M = e_1 M + \ldots + e_n M$ es directa.

Vamos a demostrar que cada $e_i M$ es isomorfo a A', isomorfismo de A'-módulos. Para esto, como todos los ideales a la izquierda de A son

isomorfos, sea, para un índice i fijo, $1 \leq i \leq n$, y $h : M \simeq A_i$ un tal isomorfismo de A-módulos. Resulta entonces que la aplicación $\bar{h} : \mathrm{Hom}_A(A_i, M) \to \mathrm{Hom}_A(M, M) = \mathrm{End}_A(M) = A'$, definida por $g \mapsto g \circ h$, es también un isomorfismo de A-módulos. Por otra parte, cabe suponer (cf. el lema 1.6.6.) que A_i sea generado, como ideal a la izquierda, por el ídempotente e_i y la aplicación $f : e_i M \to \mathrm{Hom}_A(A_i, M)$, definida por $f(e_i x)(ae_i) = ae_i x$, cualesquiera que sean $a \in A$ y $x \in M$, es un isomorfismo de A-módulos. Luego, $\bar{h} \circ f : e_i M \to A'$ es un isomorfismo de A-módulos, para $i = 1, \ldots, n$. Sin embargo es fácil ver que $\bar{h} \circ f$ es también un isomorfismo de A'-módulos. Esto demuestra que M es un A'-módulo libre de rango n. El lema siguiente termina la demostración del teorema:

Lema 1.6.6. *Sea A un anillo semisimple. Todo ideal a la izquierda de A es principal y es generado por un ídempotente. Además, si e es un ídempotente de A y M es un ideal a la izquierda de A, existe un isomorfismo de grupos $eM \simeq \mathrm{Hom}_A(Ae, M)$.*

Si I es un ideal a la izquierda de A, I es sumando directo de A, o sea existe un ideal a la izquierda I' de A tal que $A = I \oplus I'$. Esto dice que $1 = e + e'$ con $e \in I$ y $e' \in I'$, luego $ee' = e - e^2 \in I \cap I' = 0$, lo que se puede también escribir $ee' = 0$ y $e^2 = e$. Además, para todo elemento $a \in I$, se tiene $a = ae$ y de esto sigue que I es generado, como ideal a la izquierda de A, por el ídempotente e. Finalmente, si e es un ídempotente de A y M un ideal a la izquierda de A, la aplicación $eM \to \mathrm{Hom}_A(Ae, M)$, definida por $ex \mapsto (ae \mapsto aex)$, es un isomorfismo de grupos.

Según el teorema de Wedderburn, dado un anillo simple A, existe un anillo con división D y un entero $n \geq 1$ tales que $A \approx M_n(D)$, isomorfismo de anillos. Aún más, se ha demostrado que n y D son determinados de manera única con tal propiedad, o sea si existe un anillo con división D' y un entero $n' \geq 1$ tales que $A \approx M_{n'}(D')$, entonces $n = n'$ y $D \approx D'$, isomorfismo de anillos.

Sean A un anillo semisimple a la izquierda y $A = A_1 \times \ldots \times A_n$ la descomposición de A en producto de número finito n de anillos simples (cf. el corolario 1.6.2.). Por el Teorema de Wedderburn, para cada índice i, $1 \leq i \leq n$, existe un entero $m_i \geq 1$ y un anillo con división D_i, unívocamente determinados, tales que $A_i \approx M_{m_i}(D_i)$ $(i = 1, \ldots, n)$. Como cada anillo de matrices $M_{m_i}(D_i)$ es un anillo simple a la izquierda y a la derecha, resulta que todo anillo semisimple a la izquierda lo es también a la derecha, y recíprocamente, la semisimplicidad a la derecha implica la semisimplicidad a la izquierda. Por consiguiente, a partir de este momento, se dirá sencillamente anillo semisimple, sin mencionar a la derecha o a la izquierda.

1.7. EJERCICIOS

Los ejercicios que se ofrecen a continuación responden a lo dicho anteriormente en este capítulo, si bien algunos de ellos complementan la teoría expuesta.

1.7.1. Muestre que una suma directa de módulos semisimples es un módulo semisimple.

1.7.2. Sean A un anillo y I un ideal a la izquierda de A. Muestre que el A-módulo A/I es simple si, y sólo si, el ideal I es maximal en A.

1.7.3. Sean A un anillo y M un A-módulo a la izquierda simple. Muestre que el *anulador* $\mathrm{Ann}(x) = \{a \mid a \in A,\ ax = 0\}$ de un elemento $x \neq 0$ de M es un ideal a la izquierda maximal de A. Además, la aplicación A-lineal $A \to M$, definida por $a \mapsto ax$, es sobreyectiva; su núcleo es el anulador de x y existe un isomorfismo de A-módulos $A/\mathrm{Ann}(x) \cong M$.

1.7.4. Sean A un anillo y $M \neq 0$ un A-módulo de tipo finito. Muestre que existe un ideal bilátero I de A tal que $IM \neq M$. *Sugerencia:* Como M es un A-módulo de tipo finito, admite un A-submódulo maximal N y sea I el anulador del A-módulo simple M/N. La relación $I(M/N) = 0$ implica $IM \subset N$.

1.7.5. Sean A un anillo, M y N dos A-módulos y $f : M \to N$ una aplicación A-lineal. Demuestre las siguientes propiedades: (1) si M es simple, f es inyectivo o nulo; (2) si N es simple, f es sobreyectivo o nulo; (3) si M y N son simples, f es un isomorfismo o nulo.

1.7.6. Sea K un cuerpo conmutativo y considérese el producto directo de anillos $A = K \times K$. Muestre que A es un anillo semisimple, pero que A no es simple. *Sugerencia:* El anillo A se descompone en una suma directa $A = I \oplus J$ de ideales minimales $I = \{(a, 0) \mid a \in K\}$ y $J = \{(0, a) \mid a \in K\}$ y estos dos ideales son isomorfos a K como anillos, pero I y J no son isomorfos como ideales, o sea como A-módulos.

1.7.7. Lema de Schur. Muestre que la proposición 1.1.2., también conocida por lema de Schur, puede traducirse de la siguiente manera: si A es un anillo y M es un A-módulo simple, el anillo $\mathrm{End}_A(M)$ de los A-endomorfismos (lineales) de M es un cuerpo no necesariamente conmutativo.

1.7.8. Sean A un anillo con elemento unidad y $N(A)$ el conjunto de los elementos nilpotentes de A. Muestre que si A es conmutativo, $N(A)$ es un ideal de A y $N(A) \subset R(A)$, pero que si A no es conmutativo, un elemento nilpotente de A no pertenece necesariamente a $R(A)$. Aún más, todo elemento nilpotente de A que pertenece al centro de A está necesariamente en $R(A)$. Se dice que $N(A)$ es el *nilradical* de A.

1.7.9. Muestre que si A es un anillo con elemento unidad no conmutativo, todo elemento nilpotente de A está contenido en un ideal a la izquierda nilpotente de A.

1.7.10. A partir de la proposición 1.5.8., muestre que si A es un anillo conmutativo con elemento unidad y artiniano, entonces $N(A) = R(A)$.

1.7.11. Dé un ejemplo de un anillo conmutativo A con elemento unidad, necesariamente no artiniano, para el cual se tiene $N(A) \subsetneq R(A)$.

1.7.12. Muestre que si A^0 es el anillo opuesto de un anillo A con elemento unidad, entonces $R(A^0) = R(A)$.

1.7.13. Muestre que el radical de un anillo no es necesariamente un ideal nilpotente ni un nilideal. Muestre, por ejemplo, que si $A =$

$= K[[X_1, \ldots, X_n]]$ es el anillo de series formales en las indeterminadas $X_1, \ldots, X_n$ con coeficientes en un cuerpo conmutativo K, el único nilpotente de $R(A)$ es el cero.

1.7.14. Sea $(A_i)_{i\in I}$ una familia de anillos con elemento unidad. Muestre que $R(\prod_{i\in I} A_i) = \prod_{i\in I} R(A_i)$.

1.7.15. Sean K un cuerpo conmutativo y $A = K[X_1, \ldots, X_n]$ el anillo de polinomios en las indeterminadas $X_1, \ldots, X_n$ con coeficientes en K. Muestre que $R(A) = 0$.

1.7.16. Sean A un anillo semisimple e I un ideal a la izquierda de A. Muestre que existe un idempotente e de A tal que $I = Ae = Ie$.

1.7.17. Sean A un anillo con elemento unidad e I un ideal a la izquierda minimal de A tal que $I^2 \neq 0$. Muestre que existe un idempotente e de A tal que $I = Ae$.

1.7.18. Muestre que el anillo opuesto de un anillo semisimple es un anillo semisimple.

1.7.19. Para un ideal bilátero propio P de un anillo A con elemento unidad, las siguientes condiciones son equivalentes: (i) cualesquiera que sean a y b en A, la relación $aAb \subset P$ implica $a \in P$ o $b \in P$; (ii) cualesquiera que sean los ideales bilateros I y J de A, la relación $IJ \subset P$ implica $I \subset P$ o $J \subset P$. Un ideal bilátero propio P de un anillo A con elemento unidad que verifica las condiciones equivalentes dadas se denomina *ideal primo*. Un anillo A se denomina *anillo primo* si el ideal (o) es primo. 19

1.7.20. Muestre que el centro de un anillo primo es un anillo de integridad.

1.7.21. Sean A un anillo con elemento unidad y $M_n(A)$ el anillo de matrices cuadradas $n\times n$ con coeficientes en A. Muestre que todo ideal primo de $M_n(A)$ es de la forma $M_n(P)$, donde P es un ideal primo de A y que $R(M_n(A)) = M_n(R(A))$.

1.7.22. Sean A un anillo conmutativo con elemento unidad y $A[X_1, \ldots, X_n]$ el anillo de polinomios en las indeterminadas $X_1, \ldots, X_n$ con coeficientes en A. Pruebe que $R(A[X_1, \ldots, X_n]) = R(A)[X_1, \ldots, X_n]$. ¿Es tal resultado verdadero si el anillo A no es conmutativo?

1.7.23. Sean A un anillo con elemento unidad y B un subanillo de A cuyo elemento unidad es el de A. Muestre que $B \cap R(A) \subset R(B)$ y que si B está contenido en el centro de A, entonces $B \cap R(A) = R(B)$.

1.7.24. Sean K un cuerpo conmutativo y $K \to A$ un morfismo de anillos unitarios. Muestre que si L es una extensión (de cuerpos) de K, entonces $R(A \otimes_K L) \cap A = R(A)$ y que si L es una extensión separable de K, se tiene $R(A \otimes_K L) = R(A) \otimes_K L$.

1.7.25. **Formas cuadráticas.** Sean K un anillo conmutativo con elemento unidad y M un K-módulo. Se dice que una aplicación $f : M \to K$ es una *forma cuadrática* sobre M si $f(ax) = a^2 f(x)$ cualesquiera que sean a en K y x en M y si la aplicación $\varphi : M \times M \to K$ definida por $(x, y) \mapsto f(x + y) - f(x) - f(y)$ es K-bilineal, necesariamente simétrica. Se dice que φ es la *forma K-bilineal simétrica asociada* a f. Decimos que $f : M \to K$ es una forma cuadrática *no degenerada* si la aplicación K-lineal $M \to M^* = \mathrm{Hom}_K(M, K)$ definida por $x \mapsto (y \mapsto \varphi(x, y))$ es un isomorfismo de K-módulos. Si M es un K-módulo libre de base $\{e_1, \ldots, e_n\}$, la matriz cuadrada $(\varphi(e_i, e_j))_{1 \le i, j \le n}$ se llama *matriz* de f relativamente a la base $\{e_1, \ldots, e_n\}$. Demuestre los siguientes resultados:

1. Si M es un K-módulo libre de tipo finito, una condición necesaria y suficiente para que una forma cuadrática $f : M \to K$ sea no degenerada es que la matriz de f relativamente a una base cualquiera de M sea inversible.

2. Si M es un K-módulo proyectivo de tipo finito, una condición necesaria y suficiente para que una forma cuadrática $f : M \to K$ sea no degenerada es que para todo ideal primo $\mathfrak{p}$ de K, la forma cuadrática $f_{\mathfrak{p}} : M_{\mathfrak{p}} \to K_{\mathfrak{p}}$ definida por $\frac{x}{s} \mapsto \frac{f(x)}{s^2}$ sea no degenerada ($M_{\mathfrak{p}}$ es un $K_{\mathfrak{p}}$-módulo libre).

3. Si A es el álgebra de los complejos o de los cuaternios o el álgebra de Cayley y si $N : A \to R$ es la norma (véanse los ejemplos 2.1.2., 2.1.3. y 2.1.4.), entonces N es una forma cuadrática no degenerada y multiplicativa.

20

1.7.26. Sean K un cuerpo conmutativo y $A = K[[X_1, \ldots, X_n]]$ el anillo de series formales en las variables o indeterminadas $X_1, \ldots, X_n$ con coeficientes en K. Calcule el radical y el nilradical de A.

2

ÁLGEBRAS SEMISIMPLES

En este capítulo se denotará por K un cuerpo conmutativo y toda álgebra es un álgebra sobre K o una K-álgebra. Se darán algunas nociones indispensables sobre álgebras y la estructura de álgebras semisimples y, en el capítulo siguiente, se abordará la construcción del grupo de Brauer de un cuerpo. Por supuesto, muchos de los conceptos que se van a expresar en este capítulo y en los siguientes acerca de álgebras sobre cuerpos son válidos si se reemplaza el cuerpo base por un anillo conmutativo con elemento unidad.

2.1. DEFINICIONES Y EJEMPLOS

Sean K un cuerpo conmutativo y A un K-espacio vectorial. Se dice que A es una *K-álgebra* o un *álgebra sobre K* si existe una aplicación K-bilineal $\mu : A \times A \to A$ que se denominará *multiplicación* de A y que se denotará $\mu(x, y) = xy$, cualesquiera que sean x e y en A. Así, dar una estructura de álgebra sobre un K-espacio vectorial A es lo mismo que dar una aplicación K-lineal $\mu : A \underset{K}{\otimes} A \to A$, o sea un elemento $\mu \in \mathrm{Hom}_K(A \underset{K}{\otimes} A, A)$. Como existe un isomorfismo natural de K-espacios vectoriales $\mathrm{Hom}_K(A \underset{K}{\otimes} A, A) \approx \mathrm{Hom}_K(A, \mathrm{End}_K(A))$ (cf. [20], proposición 2.9.4.), donde $\mathrm{End}_K(A)$ es el anillo de K-endomorfismos (lineales) de A, el hecho de dar una estructura $\mu : A \times A \to A$ de álgebra sobre A equivale a dar un elemento $\mu \in \mathrm{Hom}_K(A, \mathrm{End}_K(A))$.

Una K-álgebra A se dice *asociativa*, si la multiplicación de A es asociativa, es decir si cualesquiera que sean x, y, z en A, se tiene $\mu(x, \mu(y, z)) = \mu(\mu(x, y), z)$. En términos de multiplicación (yuxtaposición de elementos), se puede también escribir $x(yz) = (xy)z$. Esto lleva a considerar la aplicación K-trilineal $\alpha : A \times A \times A \to A$, definida por $\alpha(x, y, z) = x(yz) - (xy)z$, que denominaremos *asociador* del álgebra A. Así, decir que un álgebra es asociativa equivale a decir que su asociador es nulo. Pero hay ejemplos de álgebras para las cuales su asociador es nulo sólo sobre cierto tipo de elementos. La proposición siguiente ofrece un ejemplo de tales álgebras.

Proposición 2.1.1. *Sean K un cuerpo conmutativo y A una K-álgebra. Las siguientes condiciones son equivalentes:* (i) *el asociador $\alpha : A \times A \times A \to A$ de A es una aplicación K-trilineal alternada;* (ii) *cualesquiera que sean x e y en A se tiene $x(xy) = x^2y$ y $(xy)y = xy^2$.*

En efecto, como $\alpha(x, x, y) = x(xy) - x^2y$, y $\alpha(x, y, y) = xy^2 - (xy)y$, cualesquiera que sean x e y en A, es evidente que (i) $\Rightarrow$ (ii). Recíprocamente, las condiciones de (ii) implican que $\alpha(x, x, y) = 0$ y que $\alpha(x, y, y) = 0$ y mostraremos que se tiene también $\alpha(x, y, x) = 0$, cualesquiera que sean x e y en A. Para esto, basta observar que $0 = \alpha(x+y, x+y, x) = \alpha(x, x, x) + \alpha(x, y, x) + \alpha(y, x, x) + \alpha(y, y, x) = \alpha(x, y, x)$, lo que demuestra la proposición.

Un álgebra que verifica las condiciones equivalentes de la proposición anterior se llama *álgebra alternativa*. Claro está que toda álgebra asociativa es alternativa, pero hay ejemplos de álgebras alternativas que no son asociativas (cf. el ejemplo 2. 1. 4. ; álgebras de Cayley).

Si, para una K-álgebra A, existe un elemento de A, que se designa por 1 y que verifica $x1 = 1x = x$ para todo $x \in A$, se dice que A es un *álgebra con elemento unidad* y que 1 es el *elemento unidad* de A. Si un tal elemento existe, es único. Hay ejemplos importantes de álgebras que no tienen elemento unidad (cf. el ejemplo 2. 1. 5.). Por otra parte, dada un álgebra sin elemento unidad, existe una manera natural de agregarle un elemento unidad y el álgebra de partida se sumerge en ésta como ideal bilátero (cf. el ejercicio 2. 8. 1.).

A continuación nos referiremos a la conmutatividad. Se dice que una K-álgebra A es *conmutativa* si $xy = yx$, cualesquiera que sean x e y en A. Esto nos lleva a considerar la aplicación K-bilineal $\gamma : A \times A \to A$, definida por $(x,y) \mapsto xy - yx$, que se denomina *conmutador* del álgebra A. Es evidente que *A es conmutativa si, y sólo si, su conmutador es nulo*. Esta observación trivial muestra que hay interés en el estudio del conmutador de un álgebra (cf. el ejercicio 2. 8. 4.).

Ejemplo 2.1.2. **Los números complejos.** Sean $\mathbb{C}$ el $\mathbb{R}$-espacio vectorial de los números complejos y $[1,t]$ la base natural de $\mathbb{C}$ sobre $\mathbb{R}$, donde $t^2 = -1$. Todo número complejo, o sea todo elemento de $\mathbb{C}$ se escribe, de manera única, en la forma $a + bt$, donde a y b están en $\mathbb{R}$. La estructura de álgebra conmutativa y asociativa con elemento unidad de $\mathbb{C}$ está dada por la multiplicación

$$(a + bt)(a' + b't) = (aa' - bb') + (ab' + a'b)t,$$

cualesquiera que sean a, b, a' y b' en $\mathbb{R}$. Además, el álgebra $\mathbb{C}$ es de integridad, o sea sin divisores de cero. La *norma* de un número complejo $a + bt$ es, por definición, el número real $N(a + bt) = (a + bt)(a - bt) = a^2 + b^2$ y es evidente que $N(a + bt) = 0$ si, y sólo si, $a = b = 0$. Se concluye que si $x = a + bt$ es un número complejo no nulo y $\bar{x} = a - bt$ su *conjugado*, entonces el inverso de x en $\mathbb{C}$ se escribe $\frac{1}{N(x)}\bar{x}$, lo que demuestra que $\mathbb{C}$ es un cuerpo llamado el *cuerpo de los números complejos*. Obsérvese además que la aplicación $N : \mathbb{C} \to \mathbb{R}$, definida por $x \mapsto N(x)$, tiene las siguientes propiedades: (i) $N(ax) = a^2 N(x)$, cualesquiera que sean a en $\mathbb{R}$ y x en $\mathbb{C}$; (ii) la aplicación $\Phi : \mathbb{C} \times \mathbb{C} \to \mathbb{R}$, definida por $(x,y) \mapsto N(x + y) - N(x) - N(y)$, es $\mathbb{R}$-bilineal simétrica, pues $\Phi(x,y) = x\bar{y} + \bar{x}y$ cualesquiera que sean x e y en $\mathbb{C}$; (iii) $N(xy) = N(x)N(y)$, cualesquiera que sean x e y en $\mathbb{C}$. Las propiedades (i) y (ii) se traducen diciendo que $N : \mathbb{C} \to \mathbb{R}$ es una *forma cuadrática* sobre $\mathbb{C}$ y la propiedad (iii) dice que la forma cuadrática N es *multiplicativa* (cf. 1. 7. 25).

Adviértase que $\mathbb{C}$, como extensión de $\mathbb{R}$, es una *extensión de Galois* de $\mathbb{R}$, cuyo grupo de Galois es el grupo cíclico de orden 2. En efecto, si $\sigma : \mathbb{C} \to \mathbb{C}$ es un $\mathbb{R}$-automorfismo de $\mathbb{C}$, entonces $\sigma(a) = a$ para todo a en $\mathbb{R}$ y aplicando σ a la identidad $t^2 = -1$, se tiene $\sigma(t)^2 = -1$, o sea $\sigma(t) = \pm t$. Si $\sigma(t) = t$, entonces σ es la identidad sobre $\mathbb{C}$, y si $\sigma(t) = -t$, en-

tonces $\sigma(x) = \bar{x}$ para todo x en $\mathbb{C}$. Así, el único $\mathbb{R}$-automorfismo σ de $\mathbb{C}$ distinto de la identidad es el que lleva todo número complejo x en su conjugado $\bar{x}$ y es evidente que $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}_{\mathbb{C}}, \sigma\}$ con $\sigma^2 = \mathrm{id}_{\mathbb{C}}$.

Ejemplo 2.1.3. **El cuerpo no conmutativo de los cuaternios.** Sea $\mathbb{H}$ un $\mathbb{R}$-espacio vectorial de dimensión 4, por ejemplo, $\mathbb{H} = \mathbb{R}^4$, y sea $\{1, e_1, e_2, e_3\}$ una base de $\mathbb{H}$ sobre $\mathbb{R}$. Defínase sobre $\mathbb{H}$ una estructura de álgebra asociativa con elemento unidad, pero no conmutativa, mediante la siguiente tabla de multiplicación relativa a la base mencionada:

	1	e_1	e_2	e_3
1	1	e_1	e_2	e_3
e_1	e_1	-1	e_3	$-e_2$
e_2	e_2	$-e_3$	-1	e_1
e_3	e_3	e_2	$-e_1$	-1

Si $x = a_0 + \sum_{i=1}^{3} a_i e_i$ es un elemento de $\mathbb{H}$, donde los a_i están en $\mathbb{R}$, el *conjugado* de x es el vector $\bar{x} = a_0 - \sum_{i=1}^{3} a_i e_i$ y la *norma* es la aplicación $N : \mathbb{H} \to \mathbb{R}$, definida por $x \mapsto x\bar{x}$. Claro está que $N(a_0 + \sum_{i=1}^{3} a_i e_i) = \sum_{i=0}^{3} a_i^2$, donde los a_i están en $\mathbb{R}$ y que, por lo tanto, $N(x) = 0$ con x en $\mathbb{H}$ si, y sólo si, $x = 0$. Luego, todo elemento $x \neq 0$ de $\mathbb{H}$ tiene un inverso en $\mathbb{H}$, a saber $\frac{1}{N(x)}\bar{x}$. Esto demuestra que $\mathbb{H}$ es un cuerpo, si bien no conmutativo. Se dice que $\mathbb{H}$ es el *cuerpo de los cuaternios* y es el primer ejemplo de cuerpo no conmutativo (cf. el teorema de Wedderburn sobre cuerpos finitos; teorema 3.6.1.).

Es fácil ver que $N : \mathbb{H} \to \mathbb{R}$ es una forma cuadrática multiplicativa, cuya forma $\mathbb{R}$-bilineal simétrica asociada $\Phi : \mathbb{H} \times \mathbb{H} \to \mathbb{R}$ se escribe $\Phi(x, y) = x\bar{y} + y\bar{x} = \bar{x}y + \bar{y}x$ cualesquiera que sean x e y en $\mathbb{H}$. Obsérvese que, en $\mathbb{H}$, la conjugación $\mathbb{H} \to \mathbb{H}$, $x \mapsto \bar{x}$ es una aplicación $\mathbb{R}$-lineal que cumple las siguientes condiciones: $\bar{\bar{x}} = x$ para todo x en $\mathbb{H}$ y $\overline{xy} = \bar{y}\bar{x}$ cualesquiera que sean x, y en $\mathbb{H}$.

Ejemplo 2.1.4. **Algebra de Cayley.** La construcción del álgebra de Cayley o de los octonios se hace de modo similar a la de los complejos o de los cuaternios. Sea, pues, C un $\mathbb{R}$-espacio vectorial de dimensión 8 y denótese por $\{1, e_1, \ldots, e_7\}$ una base de C sobre $\mathbb{R}$. La estructura de álgebra de C sobre $\mathbb{R}$ está dada conforme a la siguiente tabla de multiplicación:

	1	e_1	e_2	e_3	e_4	e_5	e_6	e_7
1	1	e_1	e_2	e_3	e_4	e_5	e_6	e_7
e_1	e_1	-1	e_3	$-e_2$	e_5	$-e_4$	$-e_7$	e_6
e_2	e_2	$-e_3$	-1	e_1	e_6	e_7	$-e_4$	$-e_5$
e_3	e_3	e_2	$-e_1$	-1	e_7	$-e_6$	e_5	$-e_4$
e_4	e_4	$-e_5$	$-e_6$	$-e_7$	-1	e_1	e_2	e_3
e_5	e_5	e_4	$-e_7$	e_6	$-e_1$	-1	$-e_3$	e_2
e_6	e_6	e_7	e_4	$-e_5$	$-e_2$	e_3	-1	$-e_1$
e_7	e_7	$-e_6$	e_5	e_4	$-e_3$	$-e_2$	e_1	-1

El R-espacio vectorial, $\mathcal{O}$ resulta ser una R-álgebra con elemento unidad, no conmutativa ni asociativa. Pero $\mathcal{O}$ es un álgebra alternativa. Además, es fácil ver que todo elemento $x \neq 0$ de $\mathcal{O}$ tiene un inverso en $\mathcal{O}$. En efecto, si $x = a_0 + \sum_{i=1}^{7} a_i e_i$ es un elemento de $\mathcal{O}$, donde los a_i están en R, el *conjugado* de x se define por $\bar{x} = a_0 - \sum_{i=1}^{7} a_i e_i$ y la norma de x se escribe $N(x) = x\bar{x} = \bar{x}x = \sum_{i=0}^{7} a_i^2$. Claro está que $N(x) = 0$ si, y sólo si, $x = 0$ y, por lo tanto, el *inverso* de $x \neq 0$ en $\mathcal{O}$ es $\frac{1}{N(x)}\bar{x}$. Obsérvese que $N : \mathcal{O} \to \mathbf{R}$ es una forma cuadrática multiplicativa y no degenerada. La aplicación $\mathcal{O} \to \mathcal{O}$, definida por $x \mapsto \bar{x}$, es R-lineal y verifica $\bar{\bar{x}} = x$ y $\overline{xy} = \bar{y}\bar{x}$, cualesquiera que sean x e y en $\mathcal{O}$ (cf. el ejercicio 2.8.6.).

Ejemplo 2.1.5. El álgebra $\mathcal{O}^*$. Sea $\mathbf{C}$ el R-espacio vectorial de los complejos y considérese el álgebra $\mathcal{O}^*$ sobre R, que coincide con $\mathbf{C}$ como espacio vectorial, pero cuya estructura de álgebra está dada por $x^*y = \bar{x}\bar{y}$ cualesquiera que sean x e y en $\mathcal{O}^*$, donde $\bar{x}$, por ejemplo, designa el conjugado de x y el producto $\bar{x}\bar{y}$ es tomado en $\mathbf{C}$. El álgebra $\mathcal{O}^*$ no es asociativa ni tampoco tiene elemento unidad. Es fácil ver que $\mathcal{O}^*$ tiene sólo tres idempotentes no nulos, a saber, 1, $e_1 = \frac{-1 + \sqrt{3}\, t}{2}$ y $e_2 = \frac{-1 - \sqrt{3}\, t}{2}$, donde $t^2 = -1$ y que $1*1 = 1$, $1*t = t*1 = -t$, $t*t = -1$, $1*e_1 = e_1*1 = e_2$, $1*e_2 = e_2*1 = e_1$ y $1 + e_1 + e_2 = 0$. Además, $\{1, e_1\}$, $\{1, e_2\}$ y $\{e_1, e_2\}$ son bases de $\mathcal{O}^*$ sobre R.

Ejemplo 2.1.6. Sean K un cuerpo conmutativo y $A = M_n(K)$ el anillo de matrices cuadradas $n \times n$ con coeficientes en K, donde $n \geq 1$ es un entero. Se sabe que A tiene una estructura natural de K-espacio vectorial para el cual una base es formada por las matrices e_{ij}, $1 \leq i, j \leq n$, donde e_{ij} es la matriz que tiene 1 en el cruce de la i-ésima fila y de la

j-ésima columna y cero en todas las otras posiciones. La estructura de K-álgebra de A está dada por la tabla de multiplicación $e_{ij}e_{kl} = \delta_{jk}e_{il}$ $(i, j, k, l = 1, \ldots, n)$. El elemento unidad de A es la matriz $e = \sum_{i=1}^{n} e_{ii}$.

Ejemplo 2.1.7. Sean K un cuerpo conmutativo, G un grupo y $K[G]$ el anillo de grupo G sobre K (cf. 1.3.). Es inmediato que $K[G]$ tiene una estructura natural de K-espacio vectorial por la multiplicación $\lambda \sum_{\sigma \in G} \mu_\sigma e_\sigma = \sum_{\sigma \in G} (\lambda\mu_\sigma)e_\sigma$, cualesquiera que sean los λ y μ_σ en K. Luego, $K[G]$ tiene una estructura de K-álgebra y se llama *álgebra de grupo* G sobre K con coeficientes en K.

Ejemplo 2.1.8. Sean K un cuerpo conmutativo y $K[X_1, \ldots, X_n]$ el anillo de polinomios en las indeterminadas $X_1, \ldots, X_n$ con coeficientes en K; $K[X_1, \ldots, X_n]$ tiene una estructura natural de K-espacio vectorial y por consiguiente de álgebra sobre K. Se dice que $K[X_1, \ldots, X_n]$ es el *álgebra de polinomios* en las indeterminadas $X_1, \ldots, X_n$ con coeficientes en K.

2.2. PRODUCTO TENSORIAL DE ÁLGEBRAS

Sean K un cuerpo conmutativo y A y B dos K-álgebras. Sobre el K-espacio vectorial $A \otimes_K B$ (cf. [20]) se define una estructura de K-álgebra mediante la multiplicación $(x \otimes y)(x' \otimes y') = xx' \otimes yy'$ para x y x' en A e y e y' en B. Se obtiene así sobre el K-espacio vectorial $A \otimes_K B$ una estructura de álgebra que se llama *producto tensorial* de las K-álgebras A y B.

Si $K \hookrightarrow K'$ es una extensión de cuerpos y A es una K-álgebra, existe sobre el K'-espacio vectorial $K' \otimes_K A$ una estructura de K'-álgebra por la multiplicación $(a' \otimes x)(b' \otimes y) = a'b' \otimes xy$ para a' y b' en K' y x e y en A. Obsérvese que la estructura de K'-espacio vectorial de $K' \otimes_K A$ es dada por $a'(b' \otimes y) = a'b' \otimes y$ para a' y b' en K' e y en A. Se dice que $K' \otimes_K A$ es la K'-álgebra obtenida a partir de la K-álgebra A por *extensión del cuerpo de escalares*, a saber, $K \hookrightarrow K'$.

Ejemplo 2.2.1. Sean G y H dos grupos y K un cuerpo conmutativo. La aplicación $K[G] \times K[H] \to K[G \times H]$ definida por $(\sum_{\sigma \in G} \lambda_\sigma e_\sigma, \sum_{\tau \in H} \mu_\tau e_\tau) \mapsto \sum_{\sigma, \tau} \lambda_\sigma\mu_\tau e_{(\sigma, \tau)}$, donde $G \times H$ es el producto directo de los grupos G y H, es K-bilineal, y define, por tanto, una aplicación K-lineal $K[G] \otimes_K K[H] \to K[G \times H]$, que es, además, un isomorfismo de K-álgebras. Resulta que, a menos de un isomorfismo, se puede escribir $K[G \times H] = K[G] \otimes_K K[H]$.

Ejemplo 2.2.2. Sean K un cuerpo conmutativo y X e Y dos indeterminadas sobre K. La aplicación K-bilineal $K[X] \times K[Y] \to K[X, Y]$ definida por $(\sum_{i\geq 0} \lambda_i X^i, \sum_{j\geq 0} \mu_j Y^j) \to \sum_{i,j\geq 0} \lambda_i \mu_j X^i Y^j$ se extiende a un isomorfismo de K-álgebras $K[X] \underset{K}{\otimes} K[Y] \simeq K[X, Y]$. Advierta el lector que se sabía ya que el anillo de polinomios $K[X, Y]$ se construye como el anillo de polinomios en la indeterminada Y con coeficientes en $K[X]$, esto es $K[X, Y] = K[X][Y]$ o también $K[X, Y] = K[Y][X]$ (construcción inductiva). Otra manera de construirlo es mediante el producto tensorial, o sea $K[X, Y] = K[X] \underset{K}{\otimes} K[Y]$.

Ejemplo 2.2.3. Sean K un cuerpo conmutativo y A y B dos K-espacios vectoriales. La aplicación K-bilineal $\mathrm{End}_K(A) \times \mathrm{End}_K(B) \to \mathrm{End}_K(A \underset{K}{\otimes} B)$ definida por $(f, g) \mapsto f \otimes g$ induce un morfismo inyectivo de K-álgebras $\mathrm{End}_K(A) \underset{K}{\otimes} \mathrm{End}_K(B) \to \mathrm{End}_K(A \underset{K}{\otimes} B)$. La demostración de este hecho, bastante fácil, se deja al lector. En particular, si A y B son espacios vectoriales de dimensión finita sobre K, entonces $\mathrm{End}_K(A) \underset{K}{\otimes} \mathrm{End}_K(B)$ y $\mathrm{End}_K(A \underset{K}{\otimes} B)$ tienen misma dimensión, a saber, m^2n^2 si $m = \dim_K(A)$ y $n = \dim_K(B)$ y, por lo tanto, $\mathrm{End}_K(A) \underset{K}{\otimes} \mathrm{End}_K(B) \simeq \mathrm{End}_K(A \underset{K}{\otimes} B)$ es un isomorfismo de K-álgebras. Un caso particular es el isomorfismo de las álgebras de matrices $M_m(K) \underset{K}{\otimes} M_n(K) \simeq M_{mn}(K)$, cualesquiera que sean los enteros $m, n \geq 1$.

Ejemplo 2.2.4. Sean ahora K un cuerpo conmutativo y A una K-álgebra. La aplicación K-bilineal $M_n(K) \times A \to M_n(A)$, definida por $((\lambda_{ij}), x) \mapsto (\lambda_{ij}x)$, induce un morfismo inyectivo de K-álgebras $M_n(K) \underset{K}{\otimes} A \to M_n(A)$, que es, además, un isomorfismo. En efecto, hasta probar que tal morfismo es sobreyectivo y para esto denótese por e_{ij} $1 \leq i, j \leq n$, la base canónica del A-módulo libre $M_n(A)$. Un elemento $\sum_{i,j=1}^{n} x_{ij}e_{ij}$ de $M_n(A)$, donde los x_{ij} están en A, proviene del elemento $\sum_{i,j=1}^{n} e_{ij} \otimes x_{ij}$ de $M_n(K) \underset{K}{\otimes} A$ por el morfismo $M_n(K) \underset{K}{\otimes} A \to M_n(A)$. Esto prueba que $M_n(K) \underset{K}{\otimes} A \simeq M_n(A)$ es un isomorfismo de K-álgebras. Este ejemplo es de utilidad para lo que sigue. Por supuesto, A es un álgebra asociativa.

2.3. ÁLGEBRAS CON DIVISIÓN Y EL TEOREMA DE FROBENIUS

Sean K un cuerpo conmutativo y A una K-álgebra. Para todo elemento x de A, considérense las aplicaciones K-lineales $R_x : A \to A$, definida por $y \mapsto yx$ (*traslación a la derecha* definida por x), y $L_x : A \to A$, definida por $y \mapsto xy$ (*traslación a la izquierda* definida por x). Es evidente que cualesquiera que sean a y b en A con $a \neq 0$, las ecuaciones $ax = b$ y $xa = b$ tienen soluciones únicas en A si, y sólo si, las aplicaciones K-lineales R_a y L_a tienen inversas R_a^{-1} y L_a^{-1}. Un álgebra que cumple tales condiciones se llama un *álgebra con división*.

Teorema 2.3.1. (Teorema de Frobenius). *Salvo isomorfismos, las únicas álgebras con división, de dimensión finita, y asociativas sobre los números reales son* $\mathbb{R}$, $\mathbb{C}$ *y* $\mathbb{H}$.

La demostración del teorema de Frobenius que se da a continuación se debe a L. E. Dickson.[12] Sea, pues, A una $\mathbb{R}$-álgebra y $n = \dim_{\mathbb{R}}(A)$. Si $n = 1$, necesariamente $A \simeq \mathbb{R}$, isomorfismo de $\mathbb{R}$-álgebras. Supóngase entonces que $n \geq 2$ y que $\mathbb{R} \subset A$ como subálgebra, y demuéstrese que existe un elemento e_1 en A tal que $e_1^2 = -1$. En efecto, como $n \geq 2$, existe un elemento x en A tal que $x \notin \mathbb{R}$ y como los vectores $1, x, \ldots, x^n$ son $\mathbb{R}$-linealmente dependientes existen números reales $\lambda_0, \lambda_1, \ldots, \lambda_n$ no todos nulos tales que $\sum_{i=0}^{n} \lambda_i x^i = 0$. Considérese el polinomio $f = \sum_{i=0}^{n} \lambda_i X^i$ con coeficientes reales y sea $f = f_1 \ldots f_m$ su descomposición en $\mathbb{R}[X]$ en factores f_i de grado 1 ó 2. Como $0 = f(x) = f_1(x) \ldots f_m(x)$ y como A es un álgebra con división, existe un índice t, $1 \leq t \leq m$, tal que $f_t(x) = 0$, o sea x es raíz de un polinomio de segundo grado $X^2 + \alpha X + \beta$ con α y β en $\mathbb{R}$. Luego $x^2 + \alpha x + \beta = 0$ con $(2x + \alpha)^2 = \alpha^2 - 4\beta < 0$, pues $x \notin \mathbb{R}$. Si se toma $e_1 = \frac{1}{\sqrt{4\beta - \alpha^2}} (2x + \alpha)$ en A, resulta $e_1^2 = -1$. Si $n = 2$, $\{1, e_1\}$ es una base de A sobre $\mathbb{R}$ y, por lo tanto, A es isomorfo a $\mathbb{C}$.

Supóngase ahora que se tenga $n \geq 3$. Existen vectores e_1 y e_2 en A tales que $e_1^2 = -1$ y $e_2^2 = -1$ y como todo vector de A que no está en $\mathbb{R}$ es raíz de un polinomio de segundo grado con coeficientes en $\mathbb{R}$, se tiene $(e_1 + e_2)^2 + \alpha(e_1 + e_2) + \beta = 0$ y $(e_1 - e_2)^2 + \gamma(e_1 - e_2) + \delta = 0$ con α, β, γ y δ en $\mathbb{R}$. Sumando estas dos ecuaciones se tiene $(\alpha + \gamma)e_1 + (\alpha - \gamma)e_2 + \beta + \delta - 4 = 0$, o sea $\alpha = \gamma = 0$ y $\beta + \delta = 4$. Se puede escribir entonces $e_1e_2 + e_2e_1 = 2 - \beta = 2\lambda$, con $\lambda = 1 - \frac{1}{2}\beta$, luego $(e_1 + e_2)^2 = 2(\lambda - 1) < 0$ y $(e_1 - e_2)^2 = -2(\lambda + 1) < 0$, o sea $-1 < \lambda < 1$. Las inecuaciones $\lambda - 1 < 0$ y $\lambda + 1 > 0$ dicen también que $1 - \lambda^2 > 0$ y como $(\frac{1}{\sqrt{1 - \lambda^2}} (\lambda e_1 + e_2))^2 = -1$, reemplazando e_2 por $\frac{1}{\sqrt{1 - \lambda^2}} (\lambda e_1 + e_2)$ cabe suponer que $e_1^2 = -1$, $e_2^2 = -1$ y $e_1e_2 = -e_2e_1$. Por cierto que e_1e_2 no puede escribirse como combinación lineal con coeficientes en $\mathbb{R}$ de los vectores $1, e_1$ y e_2, pues si así fuera existirían números reales α, β y γ tales que $e_1e_2 = \alpha + \beta e_1 + \gamma e_2$. Multiplicando a la izquierda por e_1 se tiene $-e_2 = \alpha e_1 - \beta + \gamma e_1 e_2$, o sea $e_2 = -\alpha e_1 + \beta - \gamma(\alpha + \beta e_1 + \gamma e_2)$ y esto dice, en particular, que $\gamma^2 = -1$, lo que es absurdo. Queda demostrado así que $n \geq 4$ y es claro que si $n = 4$, $\{1, e_1, e_2, e_1e_2\}$ es una base de A sobre $\mathbb{R}$ y A es isomorfa al álgebra $\mathbb{H}$ de los cuaternios.

Se demostrará que no puede ser $n \geq 5$. En efecto, sea $e_3 = e_1e_2$ y supóngase que exista un vector e_4 en A tal que $e_4^2 = -1$ y que $\{1, e_1, e_2, e_3, e_4\}$ es un conjunto $\mathbb{R}$-linealmente independiente de vectores de A. Sean los números reales $\alpha = e_1e_4 + e_4e_1$, $\beta = e_2e_4 + e_4e_2$ y $\gamma = e_3e_4 + e_4e_3$. Se tiene $e_4e_3 = e_4(e_1e_2) = (e_4e_1)e_2 = (\alpha - e_1e_4)e_2 = \alpha e_2 - e_1(\beta - e_2e_4) = \alpha e_2 - \beta e_1 + e_3e_4$, o sea $2e_4e_3 = \gamma - \beta e_1 + \alpha e_2$. Si se multiplica a la derecha por e_3, se tiene $-2e_4 = \alpha e_1 + \beta e_2 + \gamma e_3$, lo que es absurdo, pues los vectores

1, e_1, e_2, e_3 y e_4 son R-linealmente independientes y esto demuestra el teorema.

En el caso de álgebras alternativas, el teorema de Frobenius tiene un enunciado más completo y para su demostración se recomienda la obra citada en [18].

Teorema 2.3.2. (Teorema de Frobenius). *Salvo isomorfismos, las únicas álgebras con división, de dimensión finita, y alternativas sobre los reales son* R, C, H *y* O.

Uno puede preguntarse si el teorema de Frobenius sigue siendo verdadero cuando se reemplaza la hipótesis de que el álgebra es *alternativa* por *flexible* (cf. el ejercicio 2.8.5.). Este ha sido un tema de investigación en los últimos años.[18, 19]

2.4. ÁLGEBRAS DE CUATERNIOS

La construcción de un álgebra de cuaternios puede hacerse sobre un cuerpo conmutativo cualquiera o lo que es lo mismo sobre un anillo conmutativo con elemento unidad. Sean pues K un cuerpo conmutativo, a y b elementos de K y considérese el álgebra A sobre K de dimensión 4 definida sobre una base $\{1, e_1, e_2, e_3\}$ por la siguiente tabla de multiplicación:

	1	e_1	e_2	e_3
1	1	e_1	e_2	e_3
e_1	e_1	a	e_3	ae_3
e_2	e_2	$-e_3$	b	$-be_1$
e_3	e_3	$-ae_2$	be_1	$-ab$

Se dice que A es el *álgebra de cuaternios* sobre K correspondiente al par (a, b), que algunas veces también se denota $\left(\frac{a, b}{K}\right)$.

El álgebra de cuaternios así definida no es necesariamente un cuerpo ni tampoco es un álgebra con división. Por ejemplo, la construcción dada en el ejemplo 2.1.3. en el caso de los números reales puede repetirse para los números complejos (álgebra de bicuaternios), pero en este caso se obtiene un álgebra en la cual la división por elementos no nulos no siempre es posible. En efecto, si A es un tal álgebra, A es de dimensión 4 sobre C y tiene una base formada por $\{1, e_1, e_2, e_1e_2\}$ con $e_1^2 = -1$, $e_2^2 = -1$ y $e_1e_2 = -e_2e_1$. Es inmediato verificar que $(te_1 - e_1e_2)(t + e_2) = 0$ y, no obstante, $te_1 - e_1e_2 \neq 0$ e $t + e_2 \neq 0$.

En realidad, en el caso de los complejos o de un cuerpo algebraicamente cerrado, tal fenómeno se explica mediante el siguiente resultado:

Proposición 2.4.1. *Sean K un cuerpo algebraicamente cerrado y A una K-álgebra asociativa con elemento unidad y de dimensión finita. Si A es un álgebra con división, entonces A es isomorfo a K como álgebra.*

Sean $n = \dim_K(A)$ y x en A. Como $1, x, \ldots, x^n$ son K-linealmente dependientes, existen escalares $\lambda_0, \lambda_1, \ldots, \lambda_n$ en K, no todos nulos, tales que $\sum_{i=0}^{n} \lambda_i x^i = 0$ y considérese el polinomio $f = \sum_{i=0}^{n} \lambda_i X^i$ en $K[X]$. Por cierto que es posible suponer que $\lambda_n = 1$ y, sin perder la generalidad requerida, que K sea una subálgebra de A, o sea se identifica todo elemento λ de K al elemento $\lambda \cdot 1$ de A, donde 1 es el elemento unidad de A. Como K es algebraicamente cerrado, existen elementos $a_1, \ldots, a_n$ en K tales que $f = \prod_{i=1}^{n} (X - a_i)$. Luego $0 = f(x) = \prod_{i=1}^{n} (x - a_i)$ y como A es un álgebra con división, necesariamente $x - a_t = 0$ para un índice t conveniente, $1 \leq t \leq n$. Se concluye que $x = a_t \in K$, esto es $A = K$.

Veamos ahora bajo qué condiciones un álgebra de cuaternios $\left(\frac{a,b}{K}\right)$ es un cuerpo (no conmutativo). La respuesta a esta pregunta está dada por el siguiente resultado:

Proposición 2.4.2. *Sean K un cuerpo conmutativo de característica $\neq 2$, a y b elementos de K y $A = \left(\frac{a,b}{K}\right)$ el álgebra de cuaternios sobre K correspondiente al par (a, b). Una condición necesaria y suficiente para que A sea un cuerpo es que la relación $\alpha^2 - \beta^2 a - \gamma^2 b + \delta^2 ab = 0$, con α, β, γ y δ en K, sea equivalente a $\alpha = \beta = \gamma = \delta = 0$.*

En efecto, sea $\{1, e_1, e_2, e_1e_2\}$ la base natural de A sobre K, esto es $e_1^2 = a$, $e_2^2 = b$ y $(e_1e_2)^2 = -ab$. Para todo vector $x = \alpha + \beta e_1 + \gamma e_2 + \delta e_1 e_2$ de A donde α, β, γ y δ están en K, el *conjugado* de x está definido por $\bar{x} = \alpha - \beta e_1 - \gamma e_2 - \delta e_1 e_2$ y la *norma* es $N(x) = x\bar{x} = \bar{x}x = \alpha^2 - \beta^2 a - \gamma^2 b + \delta^2 ab$. La hipótesis hecha dice que $N(x) = 0$ si, y sólo si, $x = 0$. Por lo tanto, si $x \neq 0$ es un vector de A, su inverso en A se escribe $\frac{1}{N(x)} \bar{x}$ (cf. 2.8.15.).

2.5. ÁLGEBRAS SIMPLES Y SEMISIMPLES

La teoría de anillos semisimples introducida en 1.3. se aplica de inmediato al caso de álgebras. Precisando aún más, si K es un cuerpo conmutativo y A una K-álgebra con elemento unidad, se dice que A es una *K-álgebra semisimple* si A es semisimple como anillo. Una definición análoga vale para *álgebra simple*. Por supuesto, en el caso de la simplicidad, se supone que el anillo sea artiniano (cf. 1.6.) y esto se asegura suponiendo que el álgebra sea de dimensión finita. Aún más, si A es una K-álgebra de dimensión finita, entonces A es a la vez un anillo artiniano y noetheriano. Recíprocamente, si A es un álgebra sobre K y si A es noetheriana, entonces A es de dimensión finita y, por lo tanto, es también artiniana. Pero la artinianidad de un álgebra no implica que el álgebra sea de dimensión finita. Así, por ejemplo, el álgebra de cuaternios $\mathbb{H}$ sobre $\mathbb{R}$ correspondiente al par $(-1, -1)$

particular, si A es una K-álgebra central, entonces $A \underset{K}{\otimes} L$ es una L-álgebra central.

Proposición 2.6.5. *Sean K un cuerpo conmutativo y A una K-álgebra central simple. Para toda K-álgebra B, existe una biyección entre la familia de los ideales bilíteros de B y la familia de los ideales bilíteros de $A \underset{K}{\otimes} B$. Además, esa biyección preserva el orden.*

En efecto, considérense las aplicaciones $I \mapsto A \underset{K}{\otimes} I$ (I ideal de B) y $J \mapsto J \cap B$ (J ideal de $A \underset{K}{\otimes} B$), donde B está inmerso en $A \underset{K}{\otimes} B$ en virtud de la aplicación natural $x \mapsto 1 \otimes x$. Se mostrará que tales aplicaciones son inversas una de la otra. Si I es un ideal de B, $A \underset{K}{\otimes} I$ es un ideal de $A \underset{K}{\otimes} B$ y $(A \underset{K}{\otimes} I) \cap B = I$. Por otra parte, sea J un ideal de $A \underset{K}{\otimes} B$ y escríbase $J \cap B = I$ (ideal de B). Claro está que $A \underset{K}{\otimes} I \subset J$, pues si $z = \sum_i a_i \otimes x_i$ (suma finita), es un elemento de $A \underset{K}{\otimes} I$, donde los a_i están en A y los x_i están en I, entonces los elementos $1 \otimes x_i$ están en J y como J es un ideal de $A \underset{K}{\otimes} B$ y $z = \sum_i (a_i \otimes 1)(1 \otimes x_i)$, se sigue que $z \in J$. Se mostrará que, efectivamente, se tiene $A \underset{K}{\otimes} I = J$. Sea, para esto, $\{e_\iota\}_{\iota \in \Lambda}$ una base de B sobre K. Todo elemento y de J se escribe, de manera única, en la forma $y = \sum_{\jmath \in \Lambda_0} y_\jmath \otimes e_\jmath$, donde los $y_\jmath$ están en A y Λ_0 es un subconjunto finito de Λ. Para todo $k \in \Lambda_0$, se define $I_k = \{x \mid x \in A, \exists y \in J, y = \sum_{\jmath \in \Lambda_0} y_\jmath \otimes e_\jmath \text{ y } y_k = x\}$; I_k es un ideal bilátero de A y como A es una K-álgebra simple, resulta $I_k = A$ o $I_k = 0$. Como el caso $I_k = 0$ se puede descartar fácilmente, supóngase que exista un índice $k \in \Lambda_0$ para el cual $I_k = A$. En este caso, si $\sum_{\jmath \in \Lambda_0} y_\jmath \otimes e_\jmath$ es un elemento de J y si $y_k \neq 0$, entonces existe un elemento $\sum_{\jmath \in \Lambda_0} y_\jmath \otimes e_\jmath$ en J para el cual $y_k = 1$. Se puede elegir la base $\{e_\iota\}_{\iota \in \Lambda}$ de B sobre K, suponiendo que $\{e_\iota\}_{\iota \in \Lambda_1}$ sea una base de I donde $\Lambda = \Lambda_1 \cup \Lambda_2$ y $\Lambda_1 \cap \Lambda_2 = \emptyset$. Supóngase que exista un elemento y en J tal que $y \notin A \underset{K}{\otimes} I$ y escríbase $y = \sum_{\jmath \in \Lambda_0} y_\jmath \otimes e_\jmath$ con Λ_0 minimal. Entonces $\Lambda_1 \cap \Lambda_0 = \emptyset$. En efecto, suponiendo que exista un índice k en $\Lambda_1 \cap \Lambda_0$, el elemento $y - y_k \otimes e_k = \sum_{\jmath \in \Lambda_0 \setminus \{k\}} y_\jmath \otimes e_\jmath$ estaría en J, pero no en $A \underset{K}{\otimes} I$, lo que contradice la minimalidad de Λ_0. Así, si existe un índice k en Λ_0 tal que $y_k \neq 0$, entonces existe $y = \sum_{\jmath \in \Lambda_0} y_\jmath \otimes e_\jmath$ con $y_k = 1$, luego $y = 1 \otimes e_k + \sum_{\jmath \in \Lambda_0 \setminus \{k\}} y_\jmath \otimes e_\jmath$ es $\neq 0$ y para todo elemento x de A, tenemos $yx - xy = \sum_{\jmath \in \Lambda_0 \setminus \{k\}} (y_\jmath x - x y_\jmath) \otimes e_\jmath$ en J, o sea, por la minimalidad de Λ_0, $yx - xy = 0$, lo que se puede también escribir $y_\jmath x = x y_\jmath$ para todo x en A.

De este modo, $y_j \in Z_K(A) = K$ para todo j en Λ_0 y como $y = \sum_{j \in \Lambda_0} y_j \otimes e_j =$ $= 1 \otimes \sum_{j \in \Lambda_0} y_j e_j \in J$, se sigue que $\sum_{j \in \Lambda_0} y_j e_j \in I$. Pero el hecho de que $\{e_j\}_{j \in \Lambda_1}$ sea una base de I, que $\Lambda_1 \cap \Lambda_0 = \emptyset$ y que $\{e_j\}_{j \in \Lambda_1 \cup \Lambda_0}$ forma parte de una base de B sobre K, contradicen la independencia lineal de los e_j sobre K.

Corolario 2.6.6. *Sean A una K-álgebra central simple y L una extensión* (de cuerpos) *de K. Entonces $A \underset{K}{\otimes} L$ es una L-álgebra central simple.*

Corolario 2.6.7. *Sea A una K-álgebra central simple. Para toda K-álgebra simple B, la K-álgebra $A \underset{K}{\otimes} B$ es simple.*

Corolario 2.6.8. *Sean K un cuerpo conmutativo y A una K-álgebra central simple de dimensión n. Existe entonces un isomorfismo de K-álgebras $A \underset{K}{\otimes} A^0 \simeq M_n(K)$, donde A^0 es el álgebra opuesta de A.*

Considérense las aplicaciones K-lineales $\alpha : A \to \mathrm{End}_K(A)$, $a \mapsto (x \mapsto ax)$ y $\beta : A^0 \to \mathrm{End}_K(A)$, $a \mapsto (x \mapsto xa)$ (representaciones de A). Es inmediato verificar que las imágenes de α y β conmutan en $\mathrm{End}_K(A)$, y en consecuencia se puede definir un morfismo de K-álgebras $\alpha \otimes \beta : A \underset{K}{\otimes} A^0 \to \mathrm{End}_K(A)$, dado por $a \otimes b \mapsto \alpha(a)\,\beta(b)$. Como $A \underset{K}{\otimes} A^0$ es simple, re-
32 sulta que $\alpha \otimes \beta$ es inyectivo y, por razones de dimensión, $\alpha \otimes \beta$ es un isomorfismo de K-álgebras.

Corolario 2.6.9. *Si A es una K-álgebra central simple de dimensión finita, entonces su dimensión sobre K es un cuadrado* (cuadrado de un número entero).

En efecto, si $\overline{K}$ es una clausura algebraica de K, la K-álgebra $A \underset{K}{\otimes} \overline{K}$ es central simple y, por el teorema de Wedderburn (cf. el teorema 1.6.5.), existe una $\overline{K}$-álgebra con división D y un entero $n \geq 1$ tales que $A \underset{K}{\otimes} \overline{K} \approx M_n(D)$ (isomorfismo de $\overline{K}$-álgebras). Por la proposición 2.4.1., se tiene que $D = \overline{K}$, luego $\dim_K(A) = \dim_{\overline{K}}(A \underset{K}{\otimes} \overline{K}) = n^2$.

2.7. REPRESENTACIÓN REGULAR Y UNA CARACTERIZACIÓN DE ÁLGEBRAS CENTRALES SIMPLES

Sean K un cuerpo conmutativo y A una K-álgebra asociativa con elemento unidad. Recuérdese que la multiplicación a la izquierda de A es la aplicación K-lineal $L : A \to \mathrm{End}_K(A)$, definida por $a \mapsto L_a$, donde $L_a(x) = ax$ para todo x en A. Además, L es un morfismo de K-álgebras, o sea $L_{ab} = L_a L_b$, cualesquiera que sean a y b en A. El morfismo $L : A \to \mathrm{End}_K(A)$ es inyectivo, pues si $L_a = L_b$ con a y b en A, entonces $ax = bx$ cualquiera que sea x en A. En particular, para $x = 1$ se tiene $a = b$. De este modo por el morfismo inyectivo $L : A \to \mathrm{End}_K(A)$, A es isomorfa a una K-subálgebra de $\mathrm{End}_K(A)$. Si A es de dimensión finita sobre K de base $\{e_1, \ldots, e_n\}$, el isomorfismo mencionado está dado por $L(\sum_{i=1}^{n} \lambda_i e_i) =$

$= \sum_{i=1}^{n} \lambda_i L_{e_i}$. Además, si γ_{ijk} son las constantes de estructura del álgebra A respecto a la base $\{e_1, \ldots, e_n\}$, o sea si $e_i e_j = \sum_{k=1}^{n} \gamma_{ijk} e_k$ $(i, j = 1, \ldots, n)$, la matriz de L_{e_i} respecto a la base $\{e_1, \ldots, e_n\}$ se escribe

$$\begin{pmatrix} \gamma_{i11} & \gamma_{i21} & \cdots & \gamma_{in1} \\ \gamma_{i12} & \gamma_{i22} & \cdots & \gamma_{in2} \\ \cdots & \cdots & \cdots & \cdots \\ \gamma_{i1n} & \gamma_{i2n} & & \gamma_{inn} \end{pmatrix}$$

pues $L_{e_i}(e_j) = e_i e_j = \sum_{k=1}^{n} \gamma_{ijk} e_k$ $(i, j = 1, \ldots, n)$. Esto muestra que A es isomorfa a la K-subálgebra de $M_n(K)$ generada por las matrices que se acaban de describir. Esta subálgebra de $M_n(K)$ se denota A_L y se llama la *representación regular a la izquierda* de A respecto a la base $\{e_1, \ldots, e_n\}$.

Una construcción análoga permite construir la *representación regular a la derecha* de A, que se denotará por A_R. En efecto, basta considerar la aplicación K-lineal $R : A \to \mathrm{End}_K(A)$, definida por $a \mapsto R_a$, donde $R_a(x) = xa$ para todo x en A. Pero, en este caso, se tiene $R_{ab} = R_b R_a$, cualesquiera que sean a y b en A. Se deja al lector la tarea de terminar la descripción del álgebra A_R.

Ejemplo 2.7.1. La aplicación $L : \mathbb{C} \to \mathrm{End}_{\mathbb{R}}(\mathbb{C}) = M_2(\mathbb{R})$, definida por $\alpha + \beta i \mapsto \begin{pmatrix} \alpha & -\beta \\ \beta & \alpha \end{pmatrix}$, es la representación regular del álgebra $\mathbb{C}$ de los números complejos como $\mathbb{R}$-subálgebra del álgebra $M_2(\mathbb{R})$ de matrices cuadradas 2x2 con coeficientes en $\mathbb{R}$. Como $\mathbb{C}$ es un álgebra conmutativa, las representaciones a la izquierda y a la derecha coinciden.

Ejemplo 2.7.2. Sea $\mathbb{H}$ la $\mathbb{R}$-álgebra de los cuaternios relativa al par $(-1, -1)$ y denótese por $[1, e_1, e_2, e_3]$ una base de $\mathbb{H}$ sobre $\mathbb{R}$, donde $e_i^2 = -1$ $(i = 1, 2, 3)$, $e_i e_j = -e_j e_i$ para $i \neq j$ y $e_1 e_2 = e_3$, $e_2 e_3 = e_1$ y $e_3 e_1 = e_2$. La aplicación $L : \mathbb{H} \to \mathrm{End}_{\mathbb{R}}(\mathbb{H}) = M_4(\mathbb{R})$, definida por

$$\alpha_0 + \alpha_1 e_1 + \alpha_2 e_2 + \alpha_3 e_3 \mapsto \begin{pmatrix} \alpha_0 & -\alpha_1 & -\alpha_2 & -\alpha_3 \\ \alpha_1 & \alpha_0 & -\alpha_3 & \alpha_2 \\ \alpha_2 & \alpha_3 & \alpha_0 & -\alpha_1 \\ \alpha_3 & -\alpha_2 & \alpha_1 & \alpha_0 \end{pmatrix}$$

es la representación regular a la izquierda de $\mathbb{H}$ como $\mathbb{R}$-subálgebra del álgebra $M_4(\mathbb{R})$.

El teorema que sigue es una caracterización de las álgebras centrales simples mediante el centralizador del álgebra.

Teorema 2.7.3. *Sean K un cuerpo conmutativo y B una K-álgebra asociativa con elemento unidad. Si B es de dimensión finita, una con-*

dición necesaria y suficiente para que B sea una K-álgebra central simple es que para toda K-álgebra asociativa A que contenga B como K-subálgebra y el mismo elemento unidad que B, se tenga $A = C_A(B) \underset{K}{\otimes} B$.

La demostración de este teorema requiere dos lemas preliminares, el primero de los cuales es susceptible de ser demostrado de inmediato.

Lema 2.7.4. *Sean K un cuerpo conmutativo y A y B dos K-álgebras asociativas con elemento unidad. Si $A \underset{K}{\otimes} B$ es una K-álgebra simple (respectivamente central simple), las K-álgebras A y B son simples (respectivamente centrales simples).*

Lema 2.7.5. *Sean K un cuerpo conmutativo y A y B dos K-álgebras asociativas con elemento unidad, donde B es una K-subálgebra de A con el mismo elemento unidad que A. Si existe un entero $n \geq 1$ tal que $B \approx M_n(K)$* (isomorfismo de K-álgebras), *entonces $A = C_A(B) \underset{K}{\otimes} B$.*

Supóngase que $B = M_n(K)$ y sea $(e_{ij})_{1 \leq i,\, j \leq n}$ la base canónica del álgebra de matrices B (cf. el ejemplo 2.1.6.). La aplicación $\varphi : C_A(B) \underset{K}{\otimes} B \to A$, definida por $\sum_I x_i \otimes y_i \mapsto \sum_I x_i y_i$ (suma finita), es un morfismo de K-álgebras que, en verdad, es un isomorfismo. Para demostrarlo, dado un elemento x en A, considérense los elementos $x_{ij} = \sum_{k=1}^{n} e_{ki} x e_{jk}$ $(i, j = 1, \ldots, n)$ de A. Teniendo en cuenta la tabla de multiplicación $e_{ij}e_{kl} = \delta_{jk} e_{il}$ $(i, j, k, l = 1, \ldots, n)$, se obtiene $x_{ij}e_{rs} = e_{ri} x e_{js}$ y $e_{rs}x_{ij} = e_{ri} x e_{js}$, o sea $x_{ij}e_{rs} = e_{rs}x_{ij}$ $(r, s = 1, \ldots, n)$. Esto significa que $x_{ij} \in C_A(B)$ $(i, j = 1, \ldots, n)$, luego $\varphi\left(\sum_{i,j=1}^{n} x_{ij} \otimes e_{ij}\right) = \sum_{i,j=1}^{n} x_{ij} e_{ij} = \sum_{i,j,k=1}^{n} e_{ki} x e_{jk} e_{ij} =$

$= \sum_{i,j,k=1}^{n} e_{ki} x \delta_{ki} e_{jj} = \sum_{i,j=1}^{n} e_{ii} x e_{jj} = x$, pues $\sum_{i=1}^{n} e_{ii} = 1$. Queda demostrado así que el morfismo φ es sobreyectivo. Vamos a demostrar que φ es inyectivo y para ello sea $\sum_{i,j=1}^{n} x_{ij} \otimes e_{ij}$ un elemento de $C_A(B) \underset{K}{\otimes} B$ tal que $\varphi\left(\sum_{i,j=1}^{n} x_{ij} \otimes e_{ij}\right) = \sum_{i,j=1}^{n} x_{ij} e_{ij} = 0$. Se tiene $0 = \sum_{k=1}^{n} e_{kl} \left(\sum_{i,j=1}^{n} x_{ij} e_{ij}\right) e_{mk} = x_{lm}$ $(l, m = 1, \ldots, n)$, lo que demuestra la inyectividad de φ.

Demostración del Teorema 2.7.3. Sean pues B una K-álgebra central simple y sea A una K-álgebra asociativa que contiene a B como una K-subálgebra y cuyos elementos unidades coinciden. Si se escribe $A' = A \underset{K}{\otimes} B^0$ y $B' = B \underset{K}{\otimes} B^0$, donde B^0 es el álgebra opuesta de B, entonces B' es una K-subálgebra de A' y tiene el mismo elemento unidad que A'. Por el corolario 2.6.8., existe un entero $n \geq 1$ tal que $B' \approx M_n(K)$, isomorfismo de K-álgebras, donde $n = \dim_K(B)$. Por el lema 2.7.5., $A' = C_{A'}(B') \underset{K}{\otimes} B'$. Pero, por la proposición 2.6.1., $C_{A'}(B') = C_A(B) \underset{K}{\otimes} C_{B^0}(B^0) = C_A(B) \underset{K}{\otimes} K = C_A(B)$ y, por lo tanto, $A \underset{K}{\otimes} B^0 = A' = C_A(B) \underset{K}{\otimes} B \underset{K}{\otimes} B^0$, o sea $A = C_A(B) \underset{K}{\otimes} B$.

Recíprocamente, en virtud de la representación regular a la izquierda de B se puede suponer que B sea una K-subálgebra del álgebra de matrices $M_n(K)$, donde $n = \dim_K(B)$ y que el elemento unidad de B coincide con el de $M_n(K)$. Por hipótesis se tiene $M_n(K) = C_{M_n(K)}(B) \underset{K}{\otimes} B$ y como $M_n(K)$ es una K-álgebra central simple, el lema 2.7.4. dice que B es una K-álgebra central simple.

2.8. EJERCICIOS Y COMPLEMENTOS

En este parágrafo se dan algunos ejercicios que son más bien complementos a la teoría enunciada. En otros casos se trata de simples ejercicios.

2.8.1. Álgebras sin elemento unidad. Sean K un anillo conmutativo con elemento unidad, A una K-álgebra sin elemento unidad y considérese el K-módulo $A' = K \times A$ (producto directo). Sobre A' se define la siguiente multiplicación: $(a, x)(b, y) = (ab, ay + bx + xy)$, cualesquiera que sean los elementos a y b en K y x e y en A. Muestre que se define así sobre A' una estructura de K-álgebra con elemento unidad y que la aplicación $A \to A'$ definida por $x \mapsto (0, x)$ es un morfismo inyectivo de K-álgebras. Si se identifica A con su imagen en A' por tal morfismo, lo que equivale a hacer la identificación $x = (0, x)$ para todo x en A, entonces A es un ideal bilátero de A' y existe un isomorfismo de K-álgebras $A'/A \approx K$. Además, A es un ideal bilátero maximal de A' si, y sólo si, K es un cuerpo. Es evidente que A' es un álgebra conmutativa si, y sólo si, A también lo es. Dar las condiciones necesarias y si posible suficientes sobre A y K para que A' sea asociativa (respectivamente alternativa, flexible, de Lie, de Malcev, etc.).

2.8.2. Identidad de Teichmüller. Sean K un cuerpo conmutativo, A una K-álgebra y $\alpha : A \times A \times A \to A$ su asociador. Muestre que cualesquiera que sean x, y, z y t en A se tiene $\alpha(xy, z, t) - \alpha(x, yz, t) + \alpha(x, y, zt) = \alpha(x, y, z)t + x\alpha(y, z, t)$. Esta identidad vale, en general, sin ninguna hipótesis sobre el álgebra. Por supuesto que si el álgebra es asociativa, la identidad es trivial.

2.8.3. Muestre que si $\gamma : A \times A \to A$ es el conmutador de una K-álgebra A, existe una única aplicación K-lineal $\overline{\gamma} : \bigwedge^2 A \to A$ tal que $\overline{\gamma}(x \wedge y) = \gamma(x, y)$, cualesquiera que sean x e y en A, o sea, $\overline{\gamma} \in \mathrm{Hom}_K(\bigwedge^2 A, A)$.

2.8.4. Álgebras de Lie y de Malcev. Sean K un cuerpo conmutativo y A una K-álgebra. El *jacobiano* de A es la aplicación K-trilineal $J : A \times A \times A \to A$ definida por $(x, y, z) \mapsto (xy)z + (yz)x + (zx)y$. Se dice que A es *un álgebra de Lie* (respectivamente *Malcev*) si $x^2 = 0$ para todo x en A y si su jacobiano verifica $J(x, y, z) = 0$ (respectivamente $J(x, y, xz) = J(x, y, z)x$) cualesquiera que sean x, y y z en A. Es claro que toda álgebra de Lie es de Malcev, pero si K es un cuerpo de característica $\neq 3$ y A es la K-álgebra de dimensión 4 cuya tabla de multiplicación relativamente a una base $\{e_1, e_2, e_3, e_4\}$ está dada por

	e_1	e_2	e_3	e_4
e_1	0	$-\frac{1}{3}e_4$	e_1	0
e_2	$\frac{1}{3}e_4$	0	e_2	0
e_3	$-e_1$	$-e_2$	0	e_4
e_4	0	0	$-e_4$	0

entonces A es un álgebra de Malcev y no de Lie. Muestre para esto que $J(e_1, e_2, e_3) = e_4$.

1) Muestre que toda álgebra de Malcev de dimensión ≤ 3 es de Lie.

2) Sea A una K-álgebra y modifíquese la multiplicación de A escribiendo $x \cdot y = xy - yx$ (= conmutador de x e y), cualesquiera que sean x e y en A. Muestre que si A es asociativa (respectivamente alternativa), entonces A es de Lie (respectivamente Malcev) para esta nueva multiplicación.

N. B. La clasificación de álgebras de Malcev de dimensión finita es un problema no resuelto.[17]

36 **2.8.5. Álgebras flexibles.** Se dice que una K-álgebra A es *flexible* si su asociador verifica la condición $\alpha(x, y, x) = 0$ o $(xy)x = x(yx)$ cualesquiera que sean x e y en A. Toda álgebra alternativa es flexible, así como toda álgebra conmutativa es flexible. Muestre que el álgebra A de dimensión 2 sobre un cuerpo K de característica $\neq 2$, cuya tabla de multiplicación sobre una base $\{e_1, e_2\}$ está dada por $e_1^2 = e_1$, $e_1e_2 = e_2e_1 = \frac{1}{2}e_1 + \frac{1}{2}e_2$ y $e_2^2 = e_2$, es flexible, pero no es alternativa.

2.8.6. Álgebras de Cayley. Sea $\mathcal{C}$ el álgebra de Cayley construida en el ejemplo 2.1.4. y denótese $\mathcal{C} \times \mathcal{C} \to \mathbf{R}$, $(x, y) \mapsto (x|y)$ el producto escalar canónico, o sea $(e_i \mid e_j) = \delta_{ij}$ $(i, j = 1, \ldots, 7)$, $(1|e_i) = 0$ $(i = 1, \ldots, 7)$ y $(1|1) = 1$.

1) Muestre que cualesquiera que sean x, y y z en $\mathcal{C}$, se tiene $x(\bar{y}z) + y(\bar{x}z) = 2(x|y)z$, $(x|x(\bar{y}z)) = \|x\|^2 (y|z)$, $(y|x(\bar{y}z)) = -\|y\|^2 (x|z) + 2(x|y)(y|z)$, $(z|x(\bar{y}z)) = \|z\|^2 (x|y)$, donde $\|x\|$, por ejemplo, es la *norma* de x, o sea $\|x\| = \sqrt{(x|x)}$.

2) Muestre que la aplicación $u : \overset{3}{\wedge}\mathcal{C} \to \mathcal{C}$, definida por $x \wedge y \wedge z \mapsto -x(\bar{y}z) + (y|z)x - (x|z)y + (x|y)z$, es $\mathbf{R}$-lineal y cumple las condiciones $(u(x \wedge y \wedge z) \mid x) = 0$ y

$$\|u(x \wedge y \wedge z)\|^2 = \det \begin{pmatrix} (x|x) & (x|y) & (x|z) \\ (x|y) & (y|y) & (y|z) \\ (x|z) & (y|z) & (z|z) \end{pmatrix}$$

cualesquiera que sean x, y y z en $\mathcal{C}$.

2.8.7. Sea $\mathbb{C}$ el álgebra de los complejos sobre $\mathbb{R}$ y $\{1, t\}$ su base natural. Una base de la $\mathbb{R}$-álgebra $\mathbb{C} \underset{\mathbb{R}}{\otimes} \mathbb{C}$ está dada por $\{1\otimes 1, 1\otimes t, t\otimes 1, t\otimes t\}$ y considérense los elementos $e_1 = \frac{1}{2}(1\otimes 1 + t\otimes t)$ y $e_2 = \frac{1}{2}(1\otimes 1 - t\otimes t)$. Muestre que e_1 y e_2 verifican las condiciones $e_1^2 = e_1$, $e_2^2 = e_2$, $e_1 + e_2 = 1\otimes 1$ y $e_1e_2 = 0$, o sea e_1 y e_2 son idempotentes ortogonales de $\mathbb{C} \underset{\mathbb{R}}{\otimes} \mathbb{C}$. Muestre que todo elemento $\alpha 1\otimes 1 + \beta 1\otimes t + \gamma t\otimes 1 + \delta t\otimes t$ de $\mathbb{C} \underset{\mathbb{R}}{\otimes} \mathbb{C}$, donde los elementos α, β, γ y δ están en $\mathbb{R}$, se escribe en la forma $(\alpha 1\otimes 1 + \delta 1\otimes 1 - \beta t\otimes 1 - \gamma 1\otimes t)e_1 + (\alpha 1\otimes 1 - \delta 1\otimes 1 + \beta t\otimes 1 + \gamma 1\otimes t)e_2$ y, por lo tanto, cabe escribir $\mathbb{C} \underset{\mathbb{R}}{\otimes} \mathbb{C} = \mathbb{C} \underset{\mathbb{R}}{\otimes} \mathbb{C} \cdot e_1 \oplus \mathbb{C} \underset{\mathbb{R}}{\otimes} \mathbb{C} \cdot e_2$, donde por $\mathbb{C} \underset{\mathbb{R}}{\otimes} \mathbb{C} \cdot e_1$ se indica el ideal de $\mathbb{C} \underset{\mathbb{R}}{\otimes} \mathbb{C}$ generado por e_1 $(t = 1, 2)$. Muestre, además, que $\mathbb{C} \underset{\mathbb{R}}{\otimes} \mathbb{C} \cdot e_1 \approx \mathbb{C}$ $(t = 1, 2)$ es un isomorfismo de $\mathbb{R}$-álgebras. Esto demuestra que $\mathbb{C} \underset{\mathbb{R}}{\otimes} \mathbb{C}$ es isomorfo, como $\mathbb{R}$-álgebra, a un producto directo de dos álgebras isomorfas con $\mathbb{C}$.

2.8.8. Sea $\mathbb{H}$ el álgebra de cuaternios sobre $\mathbb{R}$ (cf. el ejemplo 2.1.3.) y considérense las aplicaciones $\mathbb{R}$-lineales $L : \mathbb{H} \to \mathrm{End}_{\mathbb{R}}(\mathbb{H})$ y $R : \mathbb{H} \to \mathrm{End}_{\mathbb{R}}(\mathbb{H})$ definidas, respectivamente, por $x \mapsto L_x$ y $x \mapsto R_x$, donde $L_x(y) = xy$ y $R_x(y) = y\bar{x}$ para todo y en $\mathbb{H}$. Muestre que cualesquiera que sean x e y en $\mathbb{H}$, se tiene $L_x \circ R_y = R_y \circ L_x$, luego L y R inducen un morfismo de $\mathbb{R}$-álgebras $\mathbb{H} \underset{\mathbb{R}}{\otimes} \mathbb{H} \to \mathrm{End}_{\mathbb{R}}(\mathbb{H})$, definido por $x\otimes y \to L_x \circ R_y$. Muestre que tal morfismo es un isomorfismo de $\mathbb{R}$-álgebras. Si ahora se considera el hecho que $\mathbb{H}$ es un $\mathbb{R}$-espacio vectorial de dimensión 4, resulta el isomorfismo de $\mathbb{R}$-álgebras $\mathbb{H} \underset{\mathbb{R}}{\otimes} \mathbb{H} \cong M_4(\mathbb{R})$.

2.8.9. Muestre que existe un isomorfismo de $\mathbb{R}$-álgebras y también de $\mathbb{C}$-álgebras $\mathbb{C} \underset{\mathbb{R}}{\otimes} \mathbb{H} \cong M_2(\mathbb{C})$.

2.8.10. Sean K un cuerpo conmutativo y A y B dos K-álgebras. Muestre que si A y B son K-álgebras de tipo finito, lo mismo ocurre con $A \underset{K}{\otimes} B$. Muestre que si A y B son K-álgebras con elemento unidad y si $A \underset{K}{\otimes} B$ es asociativa, entonces A y B son asociativas.

2.8.11. Sea $\mathbb{Z}[t]$ el *anillo de enteros de Gauss*, esto es, el anillo obtenido a partir de $\mathbb{Z}$, por adjunción del número complejo t $(t^2 = -1)$. Muestre que $\mathbb{R} \underset{\mathbb{Z}}{\otimes} \mathbb{Z}[t] = \mathbb{C}$.

2.8.12. Pruebe que el centro de un álgebra simple A es un subcuerpo conmutativo de A.

2.8.13. Sean A y B dos K-álgebras asociativas con elemento unidad, B una K-subálgebra de A y supóngase que los elementos unidades de A y B coinciden. Muestre que $C_A(B) \cap B = Z_K(B)$, donde $C_A(B)$ es el centralizador de B en A y $Z_K(B)$ es el centro de la K-álgebra B. En particular, $C_A(A) = Z_K(A)$.

2.8.14. Álgebras artinianas. Sean K un cuerpo conmutativo y A una K-álgebra asociativa con elemento unidad. Pruebe que una condición necesaria y suficiente para que A sea una K-álgebra artiniana es que A sea de dimensión finita.

2.8.15. Es evidente que la proposición 2.4.2. es verdadera sin ninguna hipótesis sobre la característica del cuerpo K. Pero, si K es de característica 2, el álgebra de cuaternios $A = \left(\frac{a, b}{K}\right)$ es conmutativa y, por lo tanto, A deja de ser central, como es el caso en la característica $\neq 2$.

2.8.16. **Las álgebras $A(\lambda)$.** Sean K un cuerpo conmutativo de característica $\neq 2$, A una K-álgebra asociativa y λ un elemento de K. Sobre el K-espacio vectorial A se define una nueva estructura de K-álgebra mediante la fórmula $x * y = \lambda xy + (1 - \lambda)yx$, cualesquiera que sean x e y en A. Por $A(\lambda)$ se denota el álgebra así definida sobre el K-espacio vectorial A. Demuestre los siguientes resultados:

1. Para todo $\lambda \in K$, $A(\lambda)$ es un álgebra de Jordán, o sea $(x * y) * (x * x) = x * (y * (x * x))$ y $(x * x) * (y * x) = ((x * x) * y) * x$, cualesquiera que sean x e y en $A(\lambda)$.

2. Sea A una K-álgebra simple. Una condición necesaria para que $A(\lambda)$ sea un álgebra con división es que A también lo sea.

3. Dé un ejemplo en que A es un álgebra con división, pero $A(\lambda)$ no lo es.

4. Sea A un álgebra con división. Entonces $A(\frac{1}{2})$ no es un álgebra con división si, y sólo si, existe un elemento x en A tal que $A_x \supsetneq Ax$, donde A_x es el K-espacio vectorial definido por $A_x = \{y \mid y \in A,\ xy = yx\}$.

3

EL GRUPO DE BRAUER

Este capítulo tiene por finalidad construir el grupo de Brauer de un cuerpo conmutativo, así como también indicar cómo lograr la construcción del grupo de Brauer de un anillo. Además, se presentan algunos ejemplos de grupos de Brauer.

3. 1. GRUPO DE BRAUER

Sean K un cuerpo conmutativo y A una K-álgebra central simple de dimensión finita. Se sabe que existen un entero $n \geq 1$ y una K-álgebra central de dimensión finita y con división D tales que $A \approx M_n(D) \approx M_n(K) \otimes_K D$ (isomorfismos de K-álgebras). Además, n está determinado de manera única y D es única salvo un isomorfismo de K-álgebras. Se dice que dos K-álgebras centrales simples A y B de dimensión finita son *semejantes* si existe una K-álgebra central de dimensión finita y con división D y enteros m, $n \geq 1$, tales que $A \approx M_m(D)$ y $B \approx M_n(D)$. Se indicará la relación de semejanza entre dos álgebras A y B por $A \sim B$.

Así, para toda K-álgebra central D con división y de dimensión finita se tiene $M_n(D) \sim D$ y esto para todo entero $n \geq 1$. Si A y B son dos K-álgebras simples de misma dimensión y semejantes, entonces A y B son isomorfas como K-álgebras. En efecto, se sabe que existen enteros m, $n \geq 1$, y una K-álgebra central D con división y de dimensión finita tales que $A \approx M_m(K) \otimes_K D$ y $B \approx M_n(K) \otimes_K D$. La condición $\dim_K(A) = \dim_K(B)$ implica $m = n$, luego A y B son isomorfas.

Sean D y D' dos K-álgebras centrales de dimensión finita y con división. Si $D \sim D'$, entonces D y D' son isomorfas como K-álgebras. La verificación de este hecho es inmediata.

La definición de semejanza entre álgebras centrales simples puede formularse también de la siguiente manera:

Proposición 3. 1. 1. *Sean K un cuerpo conmutativo y A y B dos K-álgebras centrales simples de dimensión finita. Entonces $A \sim B$ si, y sólo si, existen enteros r, $s \geq 1$, tales que $A \otimes_K M_r(K) \approx B \otimes_K M_s(K)$, isomorfismo de K-álgebras.*

En efecto, si $A \sim B$, existen enteros $m, n \geq 1$, y una K-álgebra D de dimensión finita y con división tales que $A \approx M_m(K) \otimes_K D$ y $B \approx M_n(K) \otimes_K D$, luego $A \otimes_K M_n(K) \approx B \otimes_K M_m(K)$, isomorfismo de K-álgebras.

Recíprocamente, supóngase que $A \otimes_K M_r(K) \approx B \otimes_K M_s(K)$, isomorfismo de K-álgebras. Como A y B son K-álgebras centrales simples de dimensión finita, existen enteros $m, n \geq 1$, y dos K-álgebras centrales con división D y D' de dimensión finita tales que $A \approx M_m(K) \otimes_K D$ y $B \approx M_n(K) \otimes_K D'$,

isomorfismos de K-álgebras. Se tiene así un isomorfismo de K-álgebras $M_{mr}(D) \approx M_{ns}(D')$, luego $mr = ns$ y $D \approx D'$, isomorfismo de K-álgebras. Esto implica que $A \sim B$.

Corolario 3. 1. 2. *Sean K un cuerpo conmutativo y A, B, A' y B' cuatro álgebras centrales simples. Si $A \sim B$ y $A' \sim B'$, entonces $A \otimes_K A' \sim B \otimes_K B'$.*

En efecto, decir que $A \sim B$ y $A' \sim B'$ equivale a decir que existen enteros m, n y $r, s \geq 1$, tales que $A \otimes_K M_m(K) \approx B \otimes_K M_n(K)$ y $A' \otimes_K M_r(K) \approx B' \otimes_K M_s(K)$, luego $A \otimes_K A' \otimes_K M_{mr}(K) \approx B \otimes_K B' \otimes_K M_{ns}(K)$, o sea $A \otimes_K A' \sim B \otimes_K B'$.

Es fácil ver que la relación de semejanza es una relación de equivalencia sobre el conjunto de clases de isomorfismos de álgebras centrales simples. Denótese $[A]$ la clase definida por una K-álgebra central simple A módulo la relación $\sim$. Denótese, además, $\mathrm{Br}(K)$ el conjunto de los símbolos $[A]$, para toda K-álgebra central simple A. Sobre el conjunto $\mathrm{Br}(K)$ se define la ley de composición $[A] + [A'] = [A \otimes_K A']$, cualesquiera que sean las K-álgebras centrales simples A y A'. El corolario 3. 1. 2. muestra que tal ley de composición es bien definida. Además, la conmutatividad y la asociatividad de esa ley resultan, respectivamente, de la conmutatividad y asociatividad del producto tensorial. El elemento neutro para esa ley de composición es representado por $[K]$. Obsérvese que, por ser $K \sim M_n(K)$ para todo entero $n \geq 1$, entonces $[M_n(K)] = [K]$. Finalmente, para toda K-álgebra central simple A, existe un isomorfismo de K-álgebras $A \otimes_K A^0 \approx M_n(K)$, donde $n = \dim_K(A) < \infty$ y A^0 es el álgebra opuesta de A. Se sigue que $[A] + [A^0] = [M_n(K)] = 0$, o sea el opuesto del elemento $[A]$ es $[A^0]$. Se demuestra así el siguiente resultado:

Proposición 3. 1. 3. *Sea K un cuerpo conmutativo. El producto tensorial sobre K define sobre el conjunto $\mathrm{Br}(K)$ una estructura de grupo abeliano.*

Se dice que $\mathrm{Br}(K)$ es el *grupo de Brauer* del cuerpo conmutativo K. A continuación se darán algunas propiedades del grupo de Brauer.

Sean K un cuerpo conmutativo y L una extensión (de cuerpos) de K. Para toda K-álgebra central simple A, $A \otimes_K L$ es una L-álgebra central simple y, por lo tanto, la aplicación $A \mapsto A \otimes_K L$ induce un morfismo de grupos abelianos $\mathrm{Br}(K) \to \mathrm{Br}(L)$. El núcleo de este morfismo, que se denotará $\mathrm{Br}(L/K)$, se llama el *grupo de Brauer relativo*, y consiste de las clases $[A]$ para las cuales $A \otimes_K L \approx M_n(L)$, isomorfismo de L-álgebras, para algún entero $n \geq 1$. Se dice que la clase $[A]$ se *escinde* por L y L se llama un *cuerpo de descomposición* (splitting field) para la clase $[A]$ o para el álgebra A. Y cabe la pregunta si toda K-álgebra central simple de dimensión finita tiene un cuerpo de descomposición que es una extensión finita de K. La respuesta la da la siguiente proposición:

Proposición 3. 1. 4. *Sean K un cuerpo conmutativo y A una K-álgebra central simple de dimensión finita. Existe una extensión* (de cuerpos) *finita L de K y un entero $n \geq 0$ tales que $A \otimes_K L \approx M_n(L)$, isomorfismo de L-álgebras.*

Si $\overline{K}$ es una clausura algebraica de K, existe un entero $n \geq 1$ tal que $A \otimes_K \overline{K} \approx M_n(\overline{K})$, isomorfismo de $\overline{K}$-álgebras (cf. el corolario 2. 6. 9.). Considérese el morfismo inyectivo de K-álgebras $A \to A \otimes_K \overline{K} = M_n(\overline{K})$ definido por $x \mapsto x \otimes 1$. Sean $\{e_1, \ldots, e_n\}$ una base de A sobre K y u_i en $M_n(\overline{K})$ la imagen de e_i por tal morfismo, esto es $u_i = e_i \otimes 1 (i = 1, \ldots, m)$. Si γ_{ijk} son las constantes de estructura del álgebra A relativamente a la base $\{e_1, \ldots, e_n\}$ o sea $e_i e_j = \sum_{k=1}^{n} \gamma_{ijk} e_k (i, j = 1, \ldots, m)$, se tiene, en $M_n(\overline{K})$, $u_i u_j = \sum_{k=1}^{n} \gamma_{ijk} u_k (i, j = 1, \ldots, m)$. Por otra parte, si $(e_{ij})_{1 \leq i, j \leq n}$ es la base natural de la $\overline{K}$-álgebra $M_n(\overline{K})$ (cf. el ejemplo 2. 1. 6.), se puede escribir $u_k = \sum_{i,j=1}^{n} \lambda_{ijk} e_{ij} (k = 1, \ldots, m)$, donde los λ_{ijk} están en $\overline{K}$. Sea ahora S el conjunto finito formado por los γ_{ijk} y los λ_{ijk}. Como $\overline{K}$ es algebraico sobre K, el conjunto S genera, en $\overline{K}$, una extensión finita L de K y es evidente que $A \otimes_K L \approx M_n(L)$, isomorfismo de L-álgebras (cf. el teor. 3. 2. 2.).

Para toda K-álgebra central simple A de dimensión finita, se sabe (cf. el corolario 2. 6. 9.) que $\dim_K(A)$ es un cuadrado y el entero $\sqrt{\dim_K(A)}$ se denominará *grado* del álgebra A y representará por $g(A)$. Por otra parte, existen un entero $m \geq 1$ y una K-álgebra central con división D de dimensión finita tales que $A \approx M_m(K) \otimes_K D$, isomorfismo de K-álgebras. Luego, $\dim_K(A) = m^2 \dim_K(D)$ y si se extrae la raíz cuadrada, se tiene $g(A) = m g(D)$. El grado de D se denomina *índice* del álgebra A, y se denotará $i(A)$. Obsérvese que si $A \sim B$, entonces $i(A) = i(B)$ y, por lo tanto, se define el índice de la clase $[A]$ como el índice de A. Así, $i : Br(K) \to \mathbb{N}^*$ es una aplicación definida en el grupo de Brauer de K con valores en el monoide multiplicativo $\mathbb{N}^*$ de los enteros ≥ 1 (cf. 3. 9. 13).

3. 2. SUBCUERPOS MAXIMALES

Sean K un cuerpo conmutativo y D una K-álgebra con división. Un subcuerpo conmutativo L de D se dice un *subcuerpo maximal* de D si la condición $L \subset L' \subsetneq D$ con L' un subcuerpo conmutativo de D implica $L = L'$. Necesariamente $Z_K(D) \subset L$, pues en caso contrario L estaría contenido propiamente en $Z_K(D)(L)$, que es el cuerpo obtenido por adjunción de los elementos de L a $Z_K(D)$.

Lema 3. 2. 1. *Sean K un cuerpo conmutativo, D una K-álgebra con división y L un subcuerpo conmutativo de D. Las siguientes condiciones son equivalentes:* (i) *L es un subcuerpo maximal de D;* (ii) $L = C_D(L)$.

Supóngase que L sea un subcuerpo maximal de D y sea $x \in C_D(L)$. Entonces $L \subset L(x)$, cuerpo obtenido por adjunción de x a L, luego $L = L(x)$ y, por lo tanto, $x \in L$. Esto demuestra que $C_D(L) \subset L$ y, como se tiene trivialmente $C_D(L) \supset L$, se sigue que $C_D(L) = L$.

Recíprocamente, sea L un subcuerpo conmutativo de D y supóngase que $L = C_D(L)$. Si L' es un subcuerpo conmutativo de D que contiene a L,

necesariamente $L' \subset C_D(L) = L$, luego $L' = L$. Esto demuestra que L es maximal.

A partir de esto se puede demostrar el teorema: todo subcuerpo maximal de un álgebra con división es un cuerpo de descomposición (splitting field) para el álgebra. Precisando aún más, tenemos el siguiente teorema:

Teorema 3.2.2. *Sean K un cuerpo conmutativo, D una K-álgebra central con división y de dimensión finita y F un subcuerpo maximal de D. Existe entonces un isomorfismo de F-álgebras $D \otimes_K F \approx M_n(F)$, donde $n = \dim_F(D)$.*

Obsérvese inicialmente que si D^0 es el álgebra opuesta de D, entonces F es un subcuerpo maximal de D si, y sólo si, F es un subcuerpo maximal de D^0. Por lo tanto, si F es un subcuerpo maximal de D, por el lema 3.2.1. se tiene $C_D(F) = F$. En cambio, como D es una K-álgebra central simple, se tiene un isomorfismo de K-álgebras $D \otimes_K D^0 \approx \mathrm{End}_K(D)$ y la imagen de $1 \otimes_K F$ en $\mathrm{End}_K(D)$ por ese isomorfismo es el cuerpo $F_L = \{L_\alpha \mid \alpha \in F, L_\alpha(x) = \alpha x, \forall x \in D\}$, luego $D \otimes_K F = D \otimes_K C_D(F) = C_{D \otimes_K D^0}(1 \otimes_K F) = C_{\mathrm{End}_K(D)}(F_L)$. Mostremos que $C_{\mathrm{End}_K(D)}(F_L) = \mathrm{End}_F(D)$. En efecto, $f \in C_{\mathrm{End}_K(D)}(F_L)$ si, y sólo si, para todo $\lambda \in F$, se tiene $f \circ L_\lambda = L_\lambda \circ f$. Luego, $f(\lambda x) = f(L_\lambda(x)) = L_\lambda(f(x)) = \lambda f(x)$, cualesquiera que sean $\lambda \in F$ y $x \in D$, o sea, $f \in \mathrm{End}_F(D)$. En particular, si $n = \dim_F(D)$, se sigue que $D \otimes_K F \approx M_n(F)$, isomorfismo de F-álgebras.

Corolario 3.2.3. *Sean K un cuerpo conmutativo, D una K-álgebra central con división y de dimensión finita. Para todo subcuerpo maximal F de D, se tiene* $\dim_F(D) = \dim_K(F) = \sqrt{\dim_K(D)}$.

Por el teorema anterior, si $\dim_F(D) = n$, existe un isomorfismo de F-álgebras $D \otimes_K F \approx M_n(F)$, luego $\dim_K(D) = \dim_F(D \otimes_K F) = n^2$ y como $n^2 = \dim_K(D) = \dim_K(F) \dim_F(D) = n \dim_K(F)$ resulta $\dim_K(F) = n$.

3.3. EL TEOREMA DE SKOLEM-NOETHER

Sean K un cuerpo y A una K-álgebra. Se dice que un K-automorfismo de álgebras $\sigma : A \to A$ es *interior* si existe un vector x en A, x inversible, tal que $\sigma(z) = xzx^{-1}$ para todo $z \in A$. En lo que sigue, se probará que si A es una K-álgebra central simple, todo K-automorfismo de A es interior.

Teorema 3.3.1. (Teorema de Skolem-Noether). *Sean K un cuerpo conmutativo y A y B dos K-álgebras simples, donde A es central y B es de dimensión finita. Si $f, g : B \to A$ son dos morfismos inyectivos de K-álgebras, existe un automorfismo interior σ de A tal que $g = \sigma \circ f$,*

Por ser A una K-álgebra central simple, existen un anillo con división D y un D-módulo a la derecha libre M de rango finito tales que $A \approx \mathrm{End}_D(M)$. Además, M es isomorfo a un ideal a la izquierda minimal de A (cf. el teorema 1.6.5.). Si D^0 es la K-álgebra opuesta de D, se sabe que $D^0 \otimes_K B$ es también una K-álgebra simple. Se definen sobre M las si-

guientes dos estructuras de $D^0 \underset{K}{\otimes} B$-módulo a la izquierda: $(\sum_i a_i^0 \otimes b_i)x = \sum_i f(b_i)xa_i$ y $(\sum_i a_i^0 \otimes b_i)x = \sum_i g(b_i)xa_i$ (sumas finitas), cualesquiera que sean los a_i^0 en D^0, los b_i en B y x en M. Es inmediato verificar que quedan definidas así sobre M dos estructuras de $D^0 \underset{K}{\otimes} B$-módulo a la izquierda mediante f y g, y M dotado de tales estructuras será denotado M_f y M_g, respectivamente. Como $D^0 \underset{K}{\otimes} B$ es una K-álgebra simple, entonces M_f (resp. M_g) es un $D^0 \underset{K}{\otimes} B$-módulo semisimple y, por tanto, se descompone en suma directa de módulos simples, o sea $M_f = \bigoplus_i M_i'$ y $M_g = \bigoplus_j M_j''$, donde los M_i' y los M_j'' son $D^0 \underset{K}{\otimes} B$-módulos simples a la izquierda. Como, en ambas representaciones M_f y M_g hay el mismo número de componentes simples, se deduce que $M_f \approx M_g$, isomorfismo de $D^0 \underset{K}{\otimes} B$-módulos a la izquierda. Esto dice que existe un isomorfismo $\alpha : M_f \to M_g$ de $D^0 \underset{K}{\otimes} B$-módulos tal que cualesquiera que sean $a^0 \in D^0$, $b \in B$ y $x \in M$, se tiene $\alpha((a^0 \otimes b)x) = (a^0 \otimes b)\alpha(x)$, o sea $\alpha(f(b)xa) = g(b)\alpha(x)a$. En particular, para $b = 1$, $\alpha(xa) = \alpha(x)a$ y esto significa que $\alpha \in \mathrm{End}_D(M) \approx A$. Existe entonces un elemento $z \in A$ tal que $\alpha(x) = zx$ para todo $x \in M$ y como α es un isomorfismo, el elemento z es inversible en A. La relación $\alpha(f(b)xa) = g(b)\alpha(x)a$ puede escribirse entonces $zf(b)xa = g(b)zxa$, luego $(zf(b) - g(b)z)xa = 0$. En particular, $(a = 1)$ se tiene $(zf(b) - g(b)z)x = 0$, cualesquiera que sea $b \in B$ y para todo $x \in M$. Como M es un A-módulo fiel, resulta $zf(b) = g(b)z$, o sea $g(b) = zf(b)z^{-1}$, para todo $b \in B$.

Corolario 3.3.2. *Sean K un cuerpo conmutativo y A una K-álgebra semisimple de dimensión finita. Todo K-automorfismo de A que deja fijos a los elementos del centro de A es interior.*

Como A es semisimple, A se descompone en un producto directo finito de K-álgebras simples $A_i (i = 1, \ldots, n)$ y cada A_i es generada por un fdempotente central e_i, o sea $e_i \in Z_K(A) (i = 1, \ldots, n)$. Si $\sigma : A \to A$ es un K-automorfismo de A que deja fijos a los elementos de $Z_K(A)$, se tiene $\sigma(e_i) = e_i (i = 1, \ldots, n)$ y, por lo tanto, $\sigma(A_i) = A_i (i = 1, \ldots, n)$. Como $\dim_K(A) = \sum_{i=1}^{n} \dim_K(A_i)$ y $\dim_K(A) < \infty$, entonces $\dim_K(A_i) < \infty$ $(i = 1, \ldots, n)$. Pero, por otra parte, $Ke_i \subset Z_K(A_i) \subset A_i$, luego A_i es de dimensión finita sobre $Z_K(A_i)$ $(i = 1, \ldots, n)$. De esta manera se demuestra que $\sigma : A_i \to A_i$ es un $Z_K(A_i)$-automorfismo y A_i es una $Z_K(A_i)$-álgebra central de dimensión finita. Luego, por el teorema de Skolem-Noether, σ es interior, o sea existe un elemento inversible $a_i \in A_i$ tal que $\sigma(x) = a_i x a_i^{-1}$ para todo $x \in A_i (i = 1, \ldots, n)$. Si se toma ahora $a = \sum_{i=1}^{n} a_i \in A_1 \times \ldots \times A_n = A$, entonces a es un elemento inversible de A y su inverso se escribe $a^{-1} = \sum_{i=1}^{n} a_i^{-1}$. Además, para todo $x \in A$, $\sigma(x) = axa^{-1}$.

Corolario 3.3.3. *Sean K un cuerpo conmutativo y A una K-álgebra central simple. Todo K-automorfismo de A es interior.*

Este corolario es un caso particular del corolario anterior, pero teniendo en cuenta la importancia de su resultado, se enuncia aparte.

Teorema 3.3.4. *Sean K un cuerpo conmutativo y A una K-álgebra central simple de dimensión finita. Para toda K-subálgebra simple B de A que contiene a K, se tiene:* (i) *El centralizador $C_A(B)$ es una K-álgebra simple.* (ii) *El duplo centralizador de B coincide con B, o sea $C_A(C_A(B)) = B$.* (iii) *Si $C = C_A(B)$, $\dim_K(A) = \dim_K(B)\dim_K(C)$.*

La aplicación K-lineal $B \to \mathrm{End}_K(B)$, definida por $b \mapsto \overline{b}$, donde $\overline{b}(x) = bx$ para todo $x \in B$, es un morfismo inyectivo de K-álgebras y, por lo tanto, B es isomorfa a una K-subálgebra $\overline{B}$ de $\mathrm{End}_K(B)$. El centralizador de $\overline{B}$ en $\mathrm{End}_K(B)$ está dado por $f \in C_{\mathrm{End}_K(B)}(\overline{B})$ si, y sólo si, para todo $b \in B$ se tiene $f\overline{b} = \overline{b}f$, o sea si, y sólo si, $f(b) = (f \circ \overline{b})(1) = (\overline{b} \circ f)(1) = \overline{b}(f(1)) = bf(1) = R_{f(1)}(b)$, para todo $b \in B$. Esto significa que $C_{\mathrm{End}_K(B)}(\overline{B})$ es la K-subálgebra de $\mathrm{End}_K(B)$ de las multiplicaciones a la derecha por elementos de B. Considérense los morfismos inyectivos de K-álgebras, $B \to A \otimes_K \mathrm{End}_K(B)$ definido por $b \mapsto b \otimes 1$, y $B \to A \otimes_K \mathrm{End}_K(B)$ definido por $b \mapsto 1 \otimes \overline{b}$. Como $A \otimes_K \mathrm{End}_K(B)$ es una K-álgebra central simple existe, por el teorema de Skolem-Noether (cf. el teorema 3.3.1.), un K-automorfismo (de K-álgebras) σ de $A \otimes_K \mathrm{End}_K(B)$ tal que $\sigma : B \otimes_K 1 \cong 1 \otimes_K \overline{B}$, isomorfismo de K-álgebras. Por lo tanto, σ induce un isomorfismo de K-álgebras (entre los centralizadores) $\sigma : C_{A \otimes_K \mathrm{End}_K(B)}(B \otimes_K 1) \cong C_{A \otimes_K \mathrm{End}_K(B)}(1 \otimes_K \overline{B})$, o sea $C_A(B) \otimes_K \mathrm{End}_K(B) \cong A \otimes_K C_{\mathrm{End}_K(B)}(\overline{B})$. Como la K-álgebra $A \otimes_K C_{\mathrm{End}_K(B)}(\overline{B})$ es central simple, se sigue (cf. el lema 2.7.4.) que la K-álgebra $C_A(B)$ es central simple y esto demuestra (i). Calculando las dimensiones de

$C_A(B) \otimes_K \mathrm{End}_K(B) \cong A \otimes_K C_{\mathrm{End}_K(B)}(\overline{B})$, resulta $\dim_K(C)(\dim_K(B))^2 = \dim_K(A)\dim_K(C_{\mathrm{End}_K(B)}(\overline{B}))$, donde $C = C_A(B)$. Como $\dim_K(C_{\mathrm{End}_K(B)}(\overline{B})) = \dim_K(B)$, entonces $\dim_K(A) = \dim_K(B)\dim_K(C)$. Se demuestra así la condición (ii). Finalmente, como $C_A(B)$ es una K-subálgebra simple de A, la condición (ii) dice que $\dim_K(A) = \dim_K(C_A(B))\dim_K(C_A(C_A(B)))$, luego $\dim_K(B) = \dim_K(C_A(C_A(B)))$. El hecho de que $B \subset C_A(C_A(B))$, por ser una subálgebra, implica que $B = C_A(C_A(B))$ *(teorema del duplo centralizador)* y esto demuestra la condición (iii).

Corolario 3.3.5. *Sean K un cuerpo conmutativo y A una K-álgebra central simple de dimensión finita. Para todo subcuerpo conmutativo L de A que contiene a K, las siguientes condiciones son equivalentes:* (i) $L = C_A(L)$; (ii) *L es un subcuerpo conmutativo maximal de A;* (iii) $\dim_K(A) = (\dim_K(L))^2$.

La equivalencia (i) $\Leftrightarrow$ (ii) es inmediata (cf. el lema 3.2.1.) y (i) $\Rightarrow$ (iii) es una consecuencia del teorema 3.3.4. Mostremos que (iii) $\Rightarrow$ (i). En efecto, las condiciones (iii) del corolario y (iii) del teorema anterior implican que $\dim_K(L) = \dim_K(C_A(L))$ y como $L \subset C_A(L)$ (como K-subálgebra), pues L es conmutativo, se sigue que $L = C_A(L)$.

3.4. GRUPO DE BRAUER DE UN CUERPO ALGEBRAICAMENTE CERRADO

Sean K un cuerpo algebraicamente cerrado. Si A es una K-álgebra central simple de dimensión finita, existe un entero $n \geq 1$ (determinado de manera única) y una K-álgebra con división D (determinada de manera única salvo un isomorfismo) tales que $A \approx M_n(D)$, isomorfismo de

K-álgebras. Pero, por la proposición 2.4.1., $D \approx K$, isomorfismo de K-álgebras, luego $A \approx M_n(K)$ y, por lo tanto, $[A] = 0$ en $\mathrm{Br}(K)$. Esto demuestra que $\mathrm{Br}(K) = 0$ (grupo trivial). En particular, $\mathrm{Br}(\mathbb{C}) = 0$.

3.5. GRUPO DE BRAUER DE UN CUERPO SEPARABLEMENTE CERRADO

Un cuerpo conmutativo K es *separablemente cerrado* si toda extensión separable de K coincide con K. Por ejemplo, $\mathbb{C}$ de los complejos es un cuerpo separablemente cerrado. Un ejemplo menos trivial de cuerpo separablemente cerrado se da a continuación.

Ejemplo 3.5.1. Sea $\mathbb{F}_p$ el cuerpo finito de característica $p > 0$ y con p elementos, y sea $\mathbb{F}_p(t)$ el cuerpo obtenido a partir de $\mathbb{F}_p$ por adjunción de una indeterminada t. Si Ω es una clausura algebraica de $\mathbb{F}_p$ y K es el conjunto de dos elementos de Ω que son separables sobre $\mathbb{F}_p(t)$, entonces K es un cuerpo separablemente cerrado. Obsérvese que $K \subsetneq \Omega$, pues $t^{1/p} \in \Omega$, pero $t^{1/p} \notin K$.

Para calcular el grupo de Brauer de un cuerpo separablemente cerrado se requiere el siguiente resultado:

Teorema 3.5.2. *Sean K un cuerpo conmutativo y D una K-álgebra central con división y de dimensión finita. Existe entonces un subcuerpo maximal L de D tal que L es una extensión separable de K. En particular, L es un cuerpo de descomposición para D.*

Corolario 3.5.3. *Sean K un cuerpo conmutativo separablemente cerrado y D una K-álgebra central simple de dimensión finita. Existe un entero $n \geq 1$ tal que $D \approx M_n(K)$, isomorfismo de K-álgebras.*

Si L es un subcuerpo maximal de D, extensión separable de K, existe un entero $n \geq 1$ tal que $D \otimes_K L \approx M_n(L)$, isomorfismo de L-álgebras. Como K es separablemente cerrado, $K = L$, luego $D \approx M_n(K)$.

Corolario 3.5.4. *Si K es un cuerpo conmutativo separablemente cerrado, entonces* $\mathrm{Br}(K) = 0$.

Para demostrar el teorema 3.5.2. es necesario el siguiente lema, cuya demostración si bien se omite aquí, puede consultarse en la obra citada en (11) en la bibliografía.

Lema 3.5.5. *Sean K un cuerpo conmutativo y D una K-álgebra central con división y de dimensión finita ≥ 2. Existe entonces un elemento $x \in D$, $x \notin K$ tal que x es separable sobre K.*

En particular, el lema dice que el cuerpo $K(x)$ es una extensión separable de K.

Demostración del teorema 3.5.2. El teorema resulta ser trivial si D es un álgebra conmutativa, pues en este caso $D = K$. Supóngase entonces que $\dim_K(D) \geq 2$. Por el lema 3.5.5., existen cuerpos intermediarios entre K y D que son separables sobre K. Sea, pues, L un sub-

cuerpo conmutativo de D que contiene a K y maximal con tal propiedad; L es un subcuerpo maximal de D y para esto basta mostrar que $C_D(L) = L$ (cf. el lema 3.2.1.). Si se muestra que $C_D(L)$ es una L-álgebra central (de centro L) con división y si se supone que $L \subsetneq C_D(L)$, el lema 3.5.5. dice que existe un elemento $x \in C_D(L)$, $x \notin L$, x separable sobre L. Pero, entonces, $L(x)$ es una extensión separable de L y $L(x) \supsetneq L$, lo que es absurdo ya que esto contradice la maximalidad de L como extensión separable de K contenida en D. Se demuestra así que $L = C_D(L)$.

Resulta claro, además, que si $n = \dim_L(D)$, entonces $D \otimes_K L \approx M_n(L)$, isomorfismo de L-álgebras, o sea L es un cuerpo de descomposición para D. Con el lema siguiente se concluye la demostración del teorema 3.5.2.

Lema 3.5.6. *Sean K un cuerpo conmutativo y A una K-álgebra central simple de dimensión finita. Para todo subcuerpo conmutativo F de A que contiene a K, el centralizador $C_A(F)$ es una F-álgebra central simple.*

Se sabe ya (cf. el corolario 2.6.8.) que si A° es el álgebra opuesta de A y si $\dim_K(A) = n$, existe un isomorfismo de K-álgebras $A \otimes_K A^\circ \approx$ $\approx A_R A_L = M_n(K)$, donde A_R y A_L son, respectivamente, las representaciones regulares a la derecha y a la izquierda (cf. 2.7.). Resulta, entonces, que $F \otimes_K 1 \approx F_R$, subálgebra de A_R formada por las multiplicaciones
46 a la derecha $R_\lambda : A \to A$, $x \mapsto x\lambda$ con $\lambda \in F$. Se ve así que $f \in C_{\mathrm{End}_K(A)}(F_R)$ si, y sólo si, para todo $\lambda \in F$, $f \circ R_\lambda = R_\lambda \circ f$, o sea $f(x\lambda) = f(R_\lambda(x)) = R_\lambda(f(x)) = f(x)\lambda$ y esto vale cualesquiera que sean $\lambda \in F$ y $x \in A$, o sea $C_{\mathrm{End}_K(A)}(F_R) = \mathrm{End}_F(A)$. Si $m = \dim_F(A)$, resulta $M_m(F) \approx \mathrm{End}_F(A) = C_{A \otimes_K A^\circ}(F \otimes_K 1) = C_A(F) \otimes_K A^\circ$. Como $F \otimes_K A^\circ$ es una F-álgebra central simple, subálgebra de $C_A(F) \otimes_K A^\circ$, por el teorema 2.7.3. se obtiene $C_A(F) \otimes_K A^\circ = (F \otimes_K A^\circ) \otimes_F C_{C_A(F)} \otimes_K A^\circ(F \otimes_K A^\circ) = (F \otimes_K A^\circ) \otimes_F (C_{C_A(F)}(F) \otimes_K C_{A^\circ}(A^\circ))$. Obsérvese, de paso, que se aplica aquí también la proposición 2.6.1. Finalmente, como $C_{A^\circ}(A^\circ) = Z_K(A^\circ) = K$ y $C_{C_A(F)}(F) = C_A(F)$, resulta $M_m(F) \approx (F \otimes_K A^\circ) \otimes_F C_A(F)$, y por el lema 2.7.4., la F-álgebra $C_A(F)$ es central simple.

3.6. GRUPO DE BRAUER DE UN CUERPO FINITO

Para el cálculo del grupo de Brauer de un cuerpo finito es necesario el siguiente teorema:

Teorema 3.6.1 (Teorema de Wedderburn). *Toda álgebra con división finita es conmutativa.*

En efecto, sean A un álgebra con división finita de centro K y L un subcuerpo conmutativo maximal de A; está claro que L contiene a K como subcuerpo (cf. 3.2.). Se sabe que todos los subcuerpos maximales de A tienen la misma dimensión (cf. el corolario 3.2.3.) y sea r tal dimensión, luego los subcuerpos maximales de A son todos isomorfos como cuerpos de descomposición del polinomio $X^{q^r} - X$, donde $q = \mathrm{card}(K)$. Por el teorema de Skolem-Noether (cf. el teorema 3.3.1), los subcuer-

pos maximales de A son todos conjugados con L, o sea si L' es otro subcuerpo conmutativo maximal de A, existe un elemento $a \neq 0$ de A tal que $L' = aLa^{-1}$. Sin embargo, todo elemento de A pertenece siempre a algún subcuerpo maximal de A, luego $A = \bigcup_{a \in A \setminus 0} aLa^{-1}$. Sean L^* el grupo multiplicativo de los elementos no nulos de L y A^* el grupo multiplicativo de los elementos no nulos de A. Entonces $A^* = \bigcup_{a \in A \setminus 0} aL^*a^{-1}$ y $L^* = A^* \cap L$. Pero, un grupo finito no puede ser la reunión de los conjugados de un subgrupo propio (cf. el lema 3.6.2.), luego $A = L = K$. El lema que sigue concluye la demostración del teorema de Wedderburn:

Lema 3.6.2. *Sean G un grupo finito y H un subgrupo propio de G. Entonces G no puede escribirse como la reunión de los conjugados de H.*

Si $h = \text{card}(H)$ y $n = (G : H)$ es el índice de H en G, entonces $nh = \text{card}(G)$. Por otra parte, cada conjugado de H se escribe de la forma $a_iHa_i^{-1} (i = 1, \ldots, n)$ y cada conjugado tiene como cardinal a h. Luego $\text{card}(\bigcup_{i=1}^{n} a_iHa_i^{-1}) \leq (h - 1)n + 1$, pues el elemento neutro de G está contenido en todos los conjugados. Como $n \geq 2$, necesariamente $(h - 1)n + 1 < hn$, y esto muestra que existen elementos de G que no están en $\bigcup_{i=1}^{n} a_iHa_i^{-1}$.

Podemos ahora enunciar la siguiente consecuencia del teorema de Wedderburn (cf. el teorema 3.6.1.):

Corolario 3.6.3. *Si K es un cuerpo finito, entonces* $\text{Br}(K) = 0$.

Como caso particular de este corolario resulta que para todo número primo $p \geq 2$, se tiene $\text{Br}(\mathbb{Z}/(p)) = 0$.

3.7. GRUPO DE BRAUER DE LOS NÚMEROS REALES Y CARACTERIZACIONES DEL CUERPO DE LOS CUATERNIOS

Se sabe (cf. el teorema 2.3.1.) que, salvo isomorfismos, las únicas álgebras con división, de dimensión finita y asociativas son $\mathbb{R}$, $\mathbb{C}$ y $\mathbb{H}$, o sea los reales, los complejos y los cuaternios. Además, de estas tres álgebras, las únicas que son centrales son $\mathbb{R}$ y $\mathbb{H}$. Luego, el grupo de Brauer $\text{Br}(\mathbb{R})$ sólo tiene un elemento distinto del elemento neutro, a saber la clase de $\mathbb{H}$. Esto demuestra el siguiente teorema:

Teorema 3.7.1. *El grupo de Brauer del cuerpo $\mathbb{R}$ de los números reales es un grupo de orden 2 o, precisando aún más,* $\text{Br}(\mathbb{R}) \approx \mathbb{Z}/(2)$, *isomorfismo de grupos abelianos.*

Pero, cabría preguntarse aquí lo que ocurre con un cuerpo ordenado maximal (cf. [8], § 2) que, hasta cierto punto, es una generalización natural del cuerpo de los números reales. Para esto, conviene examinar ante todo algunos de los resultados que caracterizan el cuerpo de los cuaternios.

Proposición 3.7.2. *Si K es un cuerpo conmutativo de característica $\neq 2$, toda K-álgebra con división D no conmutativa cuyo centro contiene a K y de dimensión 4 sobre K es un cuerpo de cuaternios sobre K.*

Como $\dim_{Z_K(D)}(D)$ es un cuadrado (cf. el corolario 2.6.9.) y $\dim_K(D) = 4$, necesariamente $Z_K(D) = K$. Si L es un subcuerpo conmutativo maximal de D, entonces $\dim_K(L) = 2$ (cf. el corolario 3.3.5.) y, por lo tanto, L es una extensión cuadrática de K de la forma $K(x)$ con $x^2 \in K$, puesto que K es de característica $\neq 2$. Por el teorema de Skolem-Noether (cf. el teorema 3.3.1.), el K-automorfismo $K(x) \to K(x)$, definido por $\lambda + \mu x \mapsto \lambda - \mu x$ $(\lambda, \mu \in K)$, es la restricción a $K(x)$ de un automorfismo interior $\theta : D \to D$, $z \mapsto yzy^{-1}$ de D. Por consiguiente, $y \notin L = K(x)$, pues la restricción de θ a L no es el automorfismo identidad, pero como θ^2 restringido a L es la identidad, entonces $y^2 \in C_D(L) = L$. Por otra parte, $y^2 \in K$, pues si $y^2 \notin K$ se tendría $L = K(y^2)$ y θ restringido a L sería la identidad, lo que no es posible. Se escribe $x^2 = a$, $y^2 = b$, donde $a, b \in K$ y como $yxy^{-1} = \theta(x) = -x$, entonces $xy = -yx$. Se tiene así la siguiente tabla de multiplicación:

	1	x	y	xy
1	1	x	y	xy
x	x	a	xy	ay
y	y	$-xy$	b	$-bx$
xy	xy	$-ay$	bx	$-ab$

Finalmente, se va a demostrar que $\{1, x, y, xy\}$ es una base de D sobre K. Si así no fuera, existirían elementos α, β y γ en K, no todos nulos, tales que $xy = \alpha + \beta x + \gamma y$, y por tanto $(x - \gamma)y = \alpha + \beta x \in K(x)$. Multiplicando tal relación por $x + \gamma$ a la izquierda, se obtiene $(a - \gamma^2)y \in K(x)$ y si fuera $a - \gamma^2 \neq 0$, se tendría $y \in K(x)$, lo que es absurdo. Luego $a = \gamma^2$, pero esta relación también conduce fácilmente a un absurdo. Se ha demostrado que $\{1, x, y, xy\}$ es una base de D sobre K.

El álgebra D es el cuerpo de cuaternios sobre K correspondiente al par (a, b).

Corolario 3.7.3. *Sean K un cuerpo conmutativo de característica $\neq 2$ y D una K-álgebra central con división, no conmutativa y de dimensión finita sobre K. Si, para todo $x \in D$, $K(x)$ es de dimensión ≤ 2 sobre K, entonces D es un cuerpo de cuaternios sobre K.*

En efecto, se sabe ya (cf. el teorema 3.5.2.) que existe un subcuerpo conmutativo maximal L de D tal que L es una extensión separable de K. Pero, entonces, L es una extensión monógena de K (cf. [7], § 11, n° 4, proposición 4) y, por lo tanto, $\dim_K(L) \leq 2$, luego $\dim_K(D) = (\dim_K(L))^2 \leq 4$ (cf. el corolario 3.2.3.). Necesariamente, $\dim_K(D) = 1$ o $\dim_K(D) = 4$. En el primer caso, se tendría $D = K$, lo que es absurdo, pues D no es conmutativo. Luego, $\dim_K(D) = 4$ y la proposición 3.7.2. indica que D es un cuerpo de cuaternios sobre K.

Nótese que si K es un cuerpo ordenado, el álgebra de cuaternios sobre K correspondiente al par $(-1, -1)$ es un cuerpo, pues la relación $\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = 0$, con α, β, γ y δ en K, implica $\alpha = \beta = \gamma = \delta = 0$ (cf. la proposición 2.4.2.). Recíprocamente, se tiene el siguiente resultado:

Teorema 3.7.4. (Teorema de Frobenius). *Sean K un cuerpo ordenado maximal, D una K-álgebra no conmutativa con división, de dimen-*

sión finita sobre K y cuyo centro contiene a K. Entonces D es isomorfa, como K-álgebra, al álgebra de cuaternios sobre K correspondiente al par $(-1, -1)$.

Como K es un cuerpo ordenado maximal, toda extensión algebraica L de K (L cuerpo conmutativo) verifica $\dim_K(L) = 1$ o $\dim_K(L) = 2$ (cf. [8], § 2, n° 6, proposición 9). Luego, en virtud del corolario 3.7.3., D es un álgebra de cuaternios sobre su centro $Z_K(D)$. Por la proposición 2.4.1., el cuerpo $Z_K(D)$ no puede ser algebraicamente cerrado, luego $Z_K(D) = K$. Pero, todo elemento de K es de la forma x^2 o $-x^2$ con $x \in K$ (cf. [8], § 2, n° 5, proposición 6), luego el álgebra de cuaternios D sobre K correspondiente al par (a, b) es un cuerpo si, sólo si, $a = -\lambda^2$ y $b = -\mu^2$ (cf. la proposición 2.4.2.), ya que en este caso, la relación $\alpha^2 + (\beta\lambda)^2 + (\gamma\mu)^2 + \delta^2 = 0$ con α, β, γ y δ en K implica $\alpha = \beta = \gamma = \delta = 0$, por el hecho de ser K un cuerpo ordenado. Esto implica que D, como K-álgebra, es isomorfa al álgebra de cuaternios sobre K correspondiente al par $(-1, -1)$.

Corolario 3.7.5. *El grupo de Brauer de un cuerpo ordenado maximal es un grupo étalico de orden* 2.

3.8. ALGUNAS INFORMACIONES COMPLEMENTARIAS

Los ejemplos dados muestran cuan difícil es calcular el grupo de Brauer de un cuerpo. Ante todo, se requiere conocer la estructura de las álgebras centrales simples sobre tal cuerpo, problema que no siempre se puede resolver. Pero igual, si se conociera la respuesta a este último problema, bien puede ocurrir que el grupo de Brauer no se preste a ser descrito de manera sencilla.

Así, por ejemplo, si K es un cuerpo de números algebraicos y K_p es su completación p-ádica, existe una sucesión exacta de grupos abelianos $0 \to \mathrm{Br}(K) \to \bigoplus_p \mathrm{Br}(K_p) \to \mathbb{Q}/\mathbb{Z} \to 0$ (cf. [23]).

Sea K un cuerpo conmutativo completo para una valorización discreta, cuyo cuerpo residual es finito. Un ejemplo de tal cuerpo es el cuerpo $\mathbb{Q}_p$ de números p-ádicos. Entonces $\mathrm{Br}(K) \approx \mathbb{Q}/\mathbb{Z}$, isomorfismo de grupos abelianos (cf. [11], § 10.8).

Se dice que un cuerpo conmutativo K tiene la *propiedad* C_1 si todo polinomio homogéneo $f \in K[X_1, \ldots, X_n]$ de grado $d < n$ tiene un cero no trivial en K, o sea existe un elemento $(a_1, \ldots, a_n) \in K^n$, donde los a_i son no todos nulos, tal que $f(a_1, \ldots, a_n) = 0$. Por ejemplo, todo cuerpo algebraicamente cerrado tiene la propiedad C_1, pero hay otros ejemplos de tales cuerpos. Así, toda extensión finita de un cuerpo con la propiedad C_1 tiene aún la propiedad C_1. Todo cuerpo finito tiene la propiedad C_1. Todo cuerpo completo para una valorización discreta, cuyo cuerpo residual es algebraicamente cerrado, tiene la propiedad C_1 (Teorema de Lang). Sea K un cuerpo algebraicamente cerrado y sea L una extensión (de cuerpos conmutativos) de K, cuyo grado de transcendencia sobre K es 1. Entonces L tiene la propiedad C_1 (Teorema de Tsen). Si K es un cuerpo con la propiedad C_1, se puede mostrar, mediante la norma reducida, que $\mathrm{Br}(K) = 0$ (cf. [11], § 10.8).

Se podría decir mucho más sobre el grupo de Brauer y, muy particularmente, sobre el grupo de Brauer de un anillo. Pero, en este caso,

la teoría de álgebras centrales simples (sobre un cuerpo conmutativo K) debe ser reemplazada por la teoría de álgebras centrales separables (sobre un anillo K, conmutativo con elemento unidad) o álgebras de Azumaya. Para una lectura más a fondo se recomienda la obra citada en [11], § 10.10., o la citada en [12].

3.9. EJERCICIOS Y COMPLEMENTOS

Se darán aquí no sólo ejercicios, sino también resultados que complementan la teoría.

3.9.1. Sea D una R-álgebra con división de dimensión finita que contiene a R como subcuerpo. Muestre que, o bien D es central y en este caso $\dim_R(D) = n^2$, donde n es un entero conveniente, o bien el centro $Z_R(D)$ es distinto de R, luego $Z_R(D)$ es una extensión finita de R y, por lo tanto, $Z_R(D) = \mathbb{C}$, cuerpo de los complejos. De este modo, D es una $\mathbb{C}$-álgebra central con división de dimensión finita y demuestre que necesariamente $D = \mathbb{C}$. Aplique el Teorema de Frobenius y muestre que $n = 2$, luego D es el cuerpo de los cuaternios sobre R relativo al par $(-1, -1)$.

3.9.2. Sean $\mathbb{Q}$ el cuerpo de los números racionales y A una $\mathbb{Q}$-álgebra asociativa no conmutativa con elemento unidad generada por x e y. Si $x^3 = -x^2 + 2x + 1$, $xy = y(x^2 - 2)$ e $y^3 = \gamma$, donde γ es un entero par no divisible por 8, pruebe que $\dim_{\mathbb{Q}}(A) = 9$ y que A es una $\mathbb{Q}$-álgebra con división (cf. [12], cap. V, § 48).

3.9.3. Sean K un cuerpo conmutativo, L una extensión (de cuerpos conmutativos) finita de K y A una K-álgebra central simple. Si $\dim_K(L) = r$ y si A y $A \otimes_K L$ son de índices m y n, respectivamente, entonces $n \mid m \mid nr$.

3.9.4. Sean K un cuerpo conmutativo y A una K-álgebra central simple. Muestre que si el grado de A es igual al índice de A, entonces A es una K-álgebra con división.

3.9.5. Muestre que el producto tensorial de dos álgebras con división no es necesariamente un álgebra con división. Dé un ejemplo.

3.9.6. Sean K un cuerpo conmutativo y A y B dos K-álgebras centrales con división. Muestre que si los grados de A y B son primos entre sí, entonces $A \otimes_K B$ es una K-álgebra central con división.

3.9.7. Muestre que si K es un cuerpo conmutativo y si D es una K-álgebra central con división de grado $m = p_1^{a_1} \dots p_r^{a_r}$, entonces $D \approx D_1 \otimes_K \otimes_K \dots \otimes_K D_r$, isomorfismo de K-álgebras, donde D_i es una K-álgebra central con división de grado $p_i^{a_i}$ $(i = 1, \dots, r)$ y donde los p_i son los factores primos distintos de m.

3.9.8. Sean K un cuerpo conmutativo y A una K-álgebra central simple. Se dice que el álgebra A es *primaria* si $A \neq K$ y si A no contiene K-subálgebras centrales simples propias. Muestre, a partir del teorema 2.7.3., que toda K-álgebra central simple de dimensión finita es un producto tensorial finito de álgebras primarias.

3. 9. 9. **Productos cruzados.** Sean K un cuerpo conmutativo y A una K-álgebra central simple. Se dice que A es un *producto cruzado* si A contiene a un subcuerpo conmutativo maximal L tal que L/K sea una extensión de Galois. Sea G el grupo de Galois de L sobre K. Se sabe que si $\dim_K(L) = n$, entonces $\dim_K(A) = n^2$ y el orden de G es n. Muestre que para todo $\sigma \in G$, existe un elemento inversible $x_\sigma \in A$ tal que $\sigma(y) = x_\sigma y x_\sigma^{-1}$ para todo $y \in L$. Muestre que el conjunto $\{x_\sigma\}_{\sigma \in G}$ es una base de A sobre L; para esto basta mostrar que los x_σ son L-linealmente independientes, pues el orden de G es $n = \dim_L(A)$. Cualesquiera que sean $\sigma, \tau \in G$, $x_\sigma x_\tau y x_\tau^{-1} x_\sigma^{-1} = x_{\sigma\tau} y x_{\sigma\tau}^{-1}$, o sea $x_{\sigma\tau}^{-1} x_\sigma x_\tau y = y x_{\sigma\tau}^{-1} x_\sigma x_\tau$, para todo $y \in L$, luego $x_{\sigma\tau}^{-1} x_\sigma x_\tau \in C_A(L) = L$. Si se denota $h(\sigma, \tau) = x_{\sigma\tau}^{-1} x_\sigma x_\tau$ y $f(\sigma, \tau) = x_{\sigma\tau} h(\sigma, \tau) x_{\sigma\tau}^{-1}$, pruebe que $f(\sigma, \tau) \in L$, $f(\sigma, \tau) \neq 0$ cualesquiera que sean $\sigma, \tau \in G$. Además, cualesquiera que sean $\sigma, \tau, \nu \in G$, muestre que $f(\sigma, \tau) f(\sigma\tau, \nu) = \sigma(f(\tau, \nu)) f(\sigma, \tau\nu)$. Así, la estructura del álgebra A queda completamente definida por L, K y el *conjunto de factores* $\{f(\sigma, \tau)\}_{(\sigma, \tau) \in G \times G}$ de L sobre K. En efecto, dos elementos de la base x_σ y x_τ se multiplican mediante la fórmula $x_\sigma x_\tau = f(\sigma, \tau) x_{\sigma\tau}$.

Recíprocamente, muestre que dados un cuerpo conmutativo K y una extensión de Galois L de K de grupo de Galois G y si $f : G \times G \to L^*$ es un conjunto de factores de L sobre K, o sea f es una aplicación de conjuntos que verifica $f(\sigma, \tau) f(\sigma\tau, \nu) = \sigma(f(\tau, \nu)) f(\sigma, \tau\nu)$, cualesquiera que sean $\sigma, \tau, \nu \in G$, existe una K-álgebra A que contiene a L como subcuerpo conmutativo maximal. Muestre que A es una K-álgebra simple con elemento unidad. Determine el centro de A.

3. 9. 10. Sean K un cuerpo conmutativo y A una K-álgebra central simple. Muestre que si B_1 es una K-subálgebra simple de A, entonces existe una K-subálgebra simple B_2 de A tal que $A \approx B_1 \underset{K}{\otimes} B_2$, isomorfismo de K-álgebras, $B_1 = C_A(B_2)$ y $B_2 = C_A(B_1)$.

3. 9. 11. **Algebras cíclicas.** Sean K un cuerpo conmutativo y $f \in K[X]$ un polinomio de grado n, f irreductible. Se dice que f es un *polinomio cíclico* sobre K si existen una extensión (de cuerpos conmutativos) L de K, un polinomio $\theta \in K[X]$ y una raíz $x \in L$ de f tales que todas las raíces de f en L se escriben x, $\theta(x)$, $\theta^2(x)$, ..., $\theta^{n-2}(x)$ y $\theta^n(x) = x$, donde $\theta^k(x) = \theta(\theta^{k-1}(x))$ $(k = 1, 2, \ldots)$. Así, en el anillo $L[X]$, el polinomio f se escribe $f = (X - x)(X - \theta(x)) \ldots (X - \theta^{n-1}(x))$. Si, como polinomio de $K[X]$, f se escribe $f = X^n + a_1 X^{n-1} + \ldots + a_{n-1} X + a_n$, donde los a_i están en K, escriba las relaciones entre los coeficientes a_i y las raíces $\theta^i(x)$ del polinomio f. Por ejemplo, el polinomio $f = X^2 + 1 \in \mathbb{R}[X]$ es cíclico sobre $\mathbb{R}$ y escriba el polinomio θ correspondiente. Dé otros ejemplos de polinomios cíclicos.

Sean ahora $f \in K[X]$ un polinomio cíclico sobre K de grado n y veamos cómo se puede asociar a f una K-álgebra, que se denominará *álgebra cíclica* (noción que se debe a L. E. Dickson[12]; consúltese también (1) para un estudio exhaustivo del problema). En efecto, sea $X^n - c$ un polinomio irreductible de $K[X]$ y sea y una raíz de este polinomio en una extensión conveniente de K, que puede suponerse sea L. Los elementos $y^i x^j (0 \leq i, j \leq n - 1)$ son K-linealmente independientes y sea A el K-espacio vectorial de base $\{y^i x^j\}_{0 \leq i, j \leq n-1}$.

La tabla de multiplicación de A relativamente a la base dada es $(y^i x^j)(y^k x^l) = y^{i+k} (\theta^k(x))^j x^l$, para $0 \leq i, j, k, l \leq n - 1$. Muestre que se

obtiene así sobre A una estructura de K-álgebra asociativa con elemento unidad. Dé un ejemplo de álgebra cíclica con división. Muestre que las álgebras cíclicas son un caso particular de producto cruzado.

Los trabajos de Albert y otros, alrededor de 1930, llevaron a la conclusión de que toda $\mathbb{Q}$-álgebra central con división es un producto cruzado. Sin embargo, en 1972, Amitsur[2] dio ejemplos de álgebras centrales con división que no son productos cruzados.

3.9.12. **Algebras separables.** La extensión de la teoría de álgebras centrales simples al caso de álgebras sobre un anillo dio origen a la noción de álgebra central separable. Así, si K es un anillo conmutativo (y asociativo) con elemento unidad y A es una K-álgebra asociativa con elemento unidad, se considera el álgebra opuesta A^0 y sobre el K-módulo $A \otimes_K A^0$ se define, de manera natural, una estructura de K-álgebra asociativa con elemento unidad. La ley de composición $(a \otimes b^0)z = azb$, cualesquiera que sean $a \in A$, $b^0 \in A^0$ y $z \in A$, define sobre A una estructura de $A \otimes_K A^0$-módulo a la izquierda y se dice que A es una *K-álgebra separable* si A es un $A \otimes_K A^0$-módulo proyectivo, necesariamente de tipo finito, pues la multiplicación $\mu : A \otimes_K A^0 \to A, a \otimes b^0 \mapsto ab$ es una aplicación $A \otimes_K A^0$-lineal sobreyectiva. Si $J(A)$ es el núcleo de la multiplicación, se tiene una sucesión exacta de $A \otimes_K A^0$-módulos a la izquierda

$$0 \to J(A) \to A \otimes_K A^0 \xrightarrow{\mu} A \to 0.$$

Se dice que A es un *álgebra de Azumaya* si A es un álgebra central separable y son las álgebras de Azumaya las que reemplazan las álgebras centrales simples en la construcción del grupo de Brauer de un anillo.[16]

(i) Muestre que si P es un K-módulo proyectivo de tipo finito y fiel, entonces la K-álgebra $A = \mathrm{End}_K(P)$ de los K-endomorfismos (lineales) de P es un álgebra de Azumaya.

(ii) En particular, para todo entero $n \geq 1$, la K-álgebra $M_n(K)$ de las matrices cuadradas $n \times n$ con coeficientes en K es un álgebra de Azumaya.

(iii) Sea $(e_{ij})_{1 \leq i,j \leq n}$ la base canónica del álgebra de matrices $A = M_n(K)$ y considérese el elemento $e = \sum_{i=1}^{n} e_{1i} \otimes e_{i1}$ del álgebra $A \otimes_K A^0$. Muestre que si $\mu : A \otimes_K A^0 \to A$ es la multiplicación de A y si $J(A) = \mathrm{Ker}(\mu)$, entonces $e^2 = e$, $\mu(e) = 1$ y $J(A)e = 0$.

Esta última propiedad sugiere una definición equivalente de álgebra separable, a saber: Se dice que una K-álgebra A es un *álgebra separable* si existe un elemento $e \in A \otimes_K A^0$, necesariamente idempotente, tal que $\mu(e) = 1$ y $J(A)e = 0$, donde $J(A) = \mathrm{Ker}(\mu)$.

Se estudiará ahora cuál es la idea de construcción del grupo de Brauer de un anillo. Sean K un anillo conmutativo con elemento unidad y A y B dos álgebras de Azumaya sobre K. Se dice que A y B son *semejantes* si

existen dos K-módulos fielmente proyectivos P y Q tales que $A \otimes_K \mathrm{End}_K(P) \approx B \otimes_K \mathrm{End}_K(Q)$, isomorfismo de K-álgebras. Es fácil ver que se define así una relación de equivalencia entre álgebras de Azumaya y sea $\mathrm{Br}(K)$ el conjunto de las clases de equivalencia de álgebras de Azumaya semejantes. Como el producto tensorial de álgebras de Azumaya es un álgebra de Azumaya, ese mismo producto tensorial define sobre $\mathrm{Br}(K)$ una estructura de grupo abeliano llamada de *grupo de Brauer* del anillo K. Para un estudio más completo, véase la obra citada en[16] Sin embargo, se puede adelantar, para beneficio del lector interesado en la teoría, que $\mathrm{Br}(\mathbf{Z}) = 0$, o sea el grupo de Brauer del anillo de enteros es trivial.

3. 9. 13. **Sobre el grado y el índice.** Se ha visto ya que el grado $\varrho : Br(K) \to \mathbb{N}^*$ y el índice $\iota : Br(K) \to \mathbb{N}^*$ son aplicaciones definidas en el grupo de Brauer del cuerpo K con valores en el monoide multiplicativo $\mathbb{N}^*$ de los enteros ≥ 1 (cf. 3. 1.). Muestre que tales aplicaciones son morfismos para las estructuras de monoides de $Br(K)$ y de $\mathbb{N}^*$, o sea cualesquiera que sean A y B, álgebras centrales simples sobre K, $\varrho([A] + [B]) = \varrho([A])\ \varrho([B])$ e $\iota([A] + [B]) = \iota([A])\ \iota([B])$. Con las notaciones de 3. 1., tales fórmulas se escriben $\varrho(A \otimes_K B) = \varrho(A)\ \varrho(B)$ e $\iota(A \otimes_K B) = \iota(A)\ \iota(B)$, cualesquiera que sean A y B dos K-álgebras centrales simples.

ÍNDICE DE NOTACIONES

$\mathbb{N}$	:	monoide aditivo de los números enteros ≥ 0.
$\mathbb{N}^*$	:	monoide multiplicativo de los números enteros ≥ 1.
$\mathbb{Z}$	:	anillo de números enteros.
$\mathbb{Q}$	:	cuerpo de números racionales.
$\mathbb{R}$	:	cuerpo de números reales.
$\mathbb{C}$	:	cuerpo de números complejos.
C^*	:	álgebra de números complejos "torcidos".
$\mathcal{O}$	:	álgebra de Cayley.
$\mathbb{H}$	:	álgebra de cuaternios (sobre $\mathbb{R}$ correspondiente al par $(-1, -1)$).
$\left(\frac{a, b}{K}\right)$	:	álgebra de cuaternios sobre el cuerpo o anillo K correspondiente al par (a, b).
$\mathbb{Z}/_{(p)}$	:	anillo de enteros módulo p, p número entero ≥ 0.
$\mathbb{F}_p$	:	cuerpo finito de característica $p > 0$ y con p elementos.
$\oplus$	:	suma directa.
$\prod$	:	producto directo.
$\rightarrow$	:	morfismo.
$\mapsto$	:	efecto de morfismo sobre elementos.
$\approx$	:	isomorfo.
$\simeq$	:	isomorfismo.
$M_n(K)$	:	álgebra de matrices cuadradas $n \times n$ con coeficientes en el anillo conmutativo K.
$K[G]$	:	álgebra del grupo G con coeficientes en el anillo conmutativo K.
$R(M)$	:	radical del K-módulo M.

$N(A)$: nilradical del anillo A.

$\mathrm{End}_K(M)$: grupo aditivo de K-endomorfismos del K-módulo M.

$\mathrm{Aut}_K(M)$: grupo multiplicativo de K-endomorfismos del K-módulo M.

$\mathrm{Ann}(x)$: Anulador del elemento x de un K-módulo M.

$K[X_1, \ldots, X_n]$: anillo de polinomios en las variables $X_1, \ldots, X_n$ con coeficientes en K.

$K[[X_1, \ldots, X_n]]$: anillo de series formales en las variables $X_1, \ldots, X_n$ con coeficientes en K.

$\mathrm{Hom}_K(M, N)$: K-módulo de las aplicaciones K-lineales de M en N.

$\otimes_K$: producto tensorial sobre el anillo K.

$G \times H$: producto de los grupos G por H.

$\dim_K(M)$: dimensión del K-espacio vectorial M.

$Z_K(A)$: centro de la K-álgebra A.

$C_A(S)$: centralizador de S en A donde S es un subconjunto del álgebra A.

$\overline{K}$: clausura algebraica del cuerpo K.

R_x : multiplicación a la derecha definida por x.

L_x : multiplicación a la izquierda definida por x.

$\delta_{ij} = 0$, si $i \neq j$, e igual a 1, si $i = j$ (δ de Kronecker).

$x \wedge y$: producto exterior de x por y.

$(x|y)$: producto escalar de x por y.

$u(x \wedge y)$: producto vectorial de x por y.

$\mathrm{Br}(K)$: grupo de Brauer del cuerpo o anillo conmutativo K.

A° : álgebra opuesta del álgebra A.

K_p : completado p-ádico de un cuerpo de números algebraicos, p entero primo > 1.

$\binom{n}{k}$: coeficiente binomial, igual a $\dfrac{n!}{k!(n-k)!}$ si $0 \leq k \leq n$ y cero si $k > n$ o si $k < 0$.

$n|m$: el entero n divide al entero m.

L/K : el cuerpo L es una extensión del cuerpo K.

ÍNDICE ALFABÉTICO

BIBLIOGRAFÍA

(1) ALBERT, A. A. Structure of Algebras, AMS Colloquium Publications N° 24, Providence, R. I. (1939).

(2) AMITSUR, S. A. On Central Division Algebras, *Israel J. Math.*, **12**, 408-420 (1972).

(3) ARTIN, E., NESBITT, C. J. y THRALL, R. M. Rings with Minimum Condition, University of Michigan Press, Ann Arbor, Mich. (1944).

(4) ATIYAH, M. F. y MACDONNALD, I. G. Introduction to Commutative Algebra, Addison-Wesley, Reading, Mass. (1969).

(5) BOURBAKI, N. Théorie des Ensembles, Fascicule des Résultats, Hermann, París (1958).

(6) BOURBAKI, N. Algèbre, Hermann, París, Capítulo 2 (1962).

(7) BOURBAKI, N. Algèbre, Hermann, París, Capítulo 5 (1950).

(8) BOURBAKI, N. Algèbre, Hermann, París, Capítulo 6 (1964).

(9) BOURBAKI, N. Algèbre, Hermann, París, Capítulo 8 (1958).

(10) CÁRDENAS, H. y LLUIS, E. Módulos Semisimples y Representación de Grupos Finitos, Editorial F. Trillas S. A., México (1970).

(11) COHN, P. M. Algebra, Wiley, Nueva York, N. Y., Vol. 2 (1979).

(12) DICKSON, L. E. Algebras and Their Arithmetics, University of Chicago Press, Chicago, Ill. (1923).

(13) FELZENSZWALB, B. Álgebras de Dimensão Finita, IMPA, Río de Janeiro (1979).

(14) GENTILE, E. R. Notas de Álgebra, Álgebras Asociativas (Notas no Publicadas).

(15) HERSTEIN, I. N. Noncommutative Rings, The Carus Mathematical Monographs N° 15, The Mathematical Association of America (1968).

(16) KNUS, M. A. y OJANGUREN, M. Théorie de la Descente et Algèbres d'Azumaya, Lecture Notes in Mathematics N° 389, Springer-Verlag, Berlín (1974).

(17) KUZMIN, E.N. Malcev Algebras of Dimension Five over a Field of Characteristic Zero, *Alg. Log.*, 9, 691-700 (1971).

(18) EL MALLAH, M. L. y MICALI, A. Sur les Dimensions de Algèbres absolument valuées, *J. Alg.*, 68, 237-246 (1981).

(19) EL MALLAH, M. L. y MICALI, A. Sur les Algebres normées sans Diviseurs topologiques de Zéro, *Bol. Soc. Mex. Mat.*, 25, 23-28 (1980).

(20) MICALI, A. y VILLAMAYOR, O. E. Estructuras Algebraicas IV (Álgebra Multilineal), Monografía N° 16, Serie de Matemática, OEA, Washington, D. C. (1976).

(21) RENAULT, G. Algèbre non commutative, Gauthier-Villars, París (1975).

(22) RIEFFEL, M. A. A General Wedderburn Theorem, *Proc. Nat. Acad. Sc.*, 54, 1513 (1965).

(23) WEIL, A. Basic Number Theory, Springer-Verlag, Berlín (1967).

COLECCIÓN DE MONOGRAFÍAS CIENTÍFICAS

Publicadas

Serie de matemática

N° 1. La Revolución en las Matemáticas Escolares, por el Consejo Nacional de Maestros de Matemáticas de los Estados Unidos de América.
N° 2. Espacios Vectoriales y Geometría Analítica, por Luis A. Santaló.
N° 3. Estructuras Algebraicas I, por Enzo R. Gentile.
N° 4. Historia de las Ideas Modernas en la Matemática, por José Babini.
N° 5. Álgebra Lineal, por Orlando E. Villamayor.
N° 6. Álgebra Linear e Geometria Euclidiana, por Alexandre Augusto Martins Rodrigues.
N° 7. El Concepto de Número, por César A. Trejo.
N° 8. Funciones de Variable Compleja, por José I. Nieto.
N° 9. Introducción a la Topología General, por Juan Horváth.
N° 10. Funções Reais, por Djairo G. de Figueiredo.
N° 11. Probabilidad e Inferencia Estadística, por Luis A. Santaló.
N° 12. Estructuras Algebraicas II (Álgebra Lineal), por Enzo R. Gentile.
N° 13. La Revolución en las Matemáticas Escolares (Segunda Fase), por Howard F. Fehr, John Camp y Howard Kellog.
N° 14. Estructuras Algebraicas III (Grupos Finitos), por Horacio H. O'Brien.
N° 15. Introducción a la Teoría de Grafos, por Fausto A. Toranzos.
N° 16. Estructuras Algebraicas IV (Álgebra Multilineal), por Artibano Micali y Orlando E. Villamayor.
N° 17. Introdução à Análise Funcional: Espaços de Banach e Cálculo Diferencial, por Leopoldo Nachbin.
N° 18. Introducción a la Integral de Lebesgue en la Recta, por Juan Antonio Gatica.
N° 19. Introducción a los Espacios de Hilbert, por José I. Nieto.
N° 20. Elementos de Biomatemática, por Alejandro B. Engel.
N° 21. Introducción a la Computación, por Jaime Michelow.
N° 22. Estructuras Algebraicas V (Teoría de Cuerpos), por Héctor A. Merklen.
N° 23. Estructuras Algebraicas VI (Formas Cuadráticas), por Francisco M. Piscoya.
N° 24. Estructuras Algebraicas VII (Estructuras de Álgebras), por Artibano Micali.

Serie de física

N° 1. Concepto Moderno del Núcleo, por D. Allan Bromley.
N° 2. Panorama de la Astronomía Moderna, por Félix Cernuschi y Sayd Codina.
N° 3. La Estructura Electrónica de los Sólidos, por Leopoldo M. Falicov.
N° 4. Física de Partículas, por Igor Saavedra.

N° 5. Experimento, Razonamiento y Creación en Física, por Félix Cernuschi.
N° 6. Semiconductores, por George Bemski.
N° 7. Aceleradores de Partículas, por Fernando Alva Andrade.
N° 8. Física Cuántica, por Onofre Rojo y Harold V. McIntosh.
N° 9. La Radiación Cósmica, por Gastón R. Mejía y Carlos Aguirre.
N° 10. Astrofísica, por Carlos Jaschek y Mercedes C. de Jaschek.
N° 11. Ondas, por Oscar J. Bressan y Enrique Gaviola.
N° 12. El Láser, por Mario Garavaglia.
N° 13. Teoría Estadística de la Materia, por Antonio E. Rodríguez y Roberto E. Caligaris.
N° 14. Aplicações da Teoria de Grupos na Espectroscopia Raman e do Infra-Vermelho, por Jorge Humberto Nicola y Anildo Bristoti.

Serie de química

N° 1. Cinética Química Elemental, por Harold Behrens LeBas.
N° 2. Bioenergética, por Isaías Raw y Walter Colli.
N° 3. Macromoléculas, por Alejandro Paladini y Moisés Burachik.
N° 4. Mecanismo de las Reacciones Orgánicas, por Jorge A. Brieux.
N° 5. Elementos Encadenados, por Jacobo Gómez Lara.
N° 6. Enseñanza de la Química Experimental, por Francisco Giral.
N° 7. Fotoquímica de Gases, por Ralf-Dieter Penzhorn.
N° 8. Introducción a la Geoquímica, por Félix González-Bonorino.
N° 9. Resonancia Magnética Nuclear de Hidrógeno-1 y de Carbono-13, por Pedro Joseph-Nathan.
N° 10. Cromatografía Líquida de Alta Presión, por Harold M. McNair y Benjamín Esquivel H.
N° 11. Actividad Óptica, Dispersión Rotatoria Óptica y Dicroísmo Circular en Química Orgánica, por Pierre Crabbé.
N° 12. Espectroscopia Infrarroja, por Jesús Morcillo Rubio.
N° 13. Polarografía, por Alejandro J. Arvía y Jorge A. Bolzan.
N° 14. Paramagnetismo Electrónico, por Juan A. McMillan.
N° 15. Introducción a la Estereoquímica, por Juan A. Garbarino.
N° 16. Cromatografía en Papel y en Capa Delgada, por Xorge A. Domínguez.
N° 17. Introducción a la Espectrometría de Masa de Sustancias Orgánicas, por Otto R. Gottlieb y Raimundo Braz Filho.
N° 18. Cinética Química, por Rodolfo V. Caneda.
N° 19. Fuerzas Intermoleculares, por Mateo Díaz Peña.
N° 20. Físico-Química de Superficies, por Tibor Rabockai.
N° 21. Corrosión, por José R. Galvele.
N° 22. Introducción a la Electroquímica, por Dionisio Posadas.
N° 23. Cromatografía de Gases, por Harold M. McNair.
N° 24. Cinética de Disolución de Medicamentos, por Edison Cid Cárcamo.
N° 25. Introducción a la Química de Suelos, por Elemer Bornemisza.
N° 26. Elementos de Catálisis Heterogénea, por Sergio E. Droguett.

N° 27. Introducción a la Electrocatálisis, por Alejandro J. Arvía y María Cristina Giordano.

Serie de biología

N° 1. La Genética y la Revolución en las Ciencias Biológicas, por José Luis Reissig.
N° 2. Bases Ecológicas de la Explotación Agropecuaria en la América Latina, por Guillermo Mann F.
N° 3. La Taxonomía y la Revolución en las Ciencias Biológicas, por Elías R. de la Sota.
N° 4. Principios Básicos para la Enseñanza de la Biología, por Oswaldo Frota-Pessoa.
N° 5. A Vida da Célula, por Renato Basile.
N° 6. Microorganismos, por J. M. Gutiérrez-Vázquez.
N° 7. Principios Generales de Microbiología, por Norberto J. Palleroni.
N° 8. Los Virus, por Enriqueta Pizarro-Suárez y Gamba.
N° 9. Introducción a la Ecología del Bentos Marino, por Manuel Vegas Vélez.
N° 10. Biosíntesis de Proteínas y el Código Genético, por Jorge E. Allende.
N° 11. Fundamentos de Inmunología e Inmunoquímica, por Félix Córdoba Alva y Sergio Estrada-Parra.
N° 12. Bacteriófagos, por Romilio Espejo T.
N° 13. Biogeografía de América Latina, por Angel L. Cabrera y Abraham Willink.
N° 14. Relación Hospedante-Parásito. Mecanismo de Patogenicidad de los Microorganismos, por Manuel Rodríguez-Leiva.
N° 15. Genética de Poblaciones Humanas, por Francisco Rothhammer.
N° 16. Introducción a la Ecofisiología Vegetal, por Ernesto Medina.
N° 17. Aspectos de Biología Celular y la Transformación Maligna, por Manuel Rieber.
N° 18. Transporte a Través de la Membrana Celular, por P. J. Garrahan y A. F. Rega.
N° 19. Duplicación Cromosómica y Heterocromatina a Nivel Molecular y Citológico, por Néstor O. Bianchi.
N° 20. Citogenética Básica y Biología de los Cromosomas, por Francisco A. Sáez y Horacio Cardoso.
N° 21. Ecología de Poblaciones Animales, por Jorge E. Rabinovich.
N° 22. Metodología para el Estudio de la Vegetación, por Silvia D. Matteucci y Aída Colma.
N° 23. Los Sistemas Ecológicos y la Humanidad, por Ariel E. Lugo y Gregory L. Morris.
N° 24. A Germinação das Sementes, por Luiz Gouvêa Labouriau.
N° 25. Introducción a la Farmacocinética, por Edison Cid Cárcamo.
N° 26. Introducción a la Teoría y Práctica de la Taxonomía Numérica, por Jorge V. Crisci y María Fernanda López Armengol.
N° 27. ¿Qué es la Diferenciación Celular?, por Roberto B. García y Susana Pereyra-Alfonso.

En preparación

Serie de matemática

Ecuaciones en Derivadas Parciales, por Lorenzo Lara-Carrero.
Geometrías Finitas, por Oscar Barriga.
Álgebra Elemental, por Leopoldo Nachbin.

Serie de física

Teoría de Fluidos en Equilibrio, por Antonio E. Rodríguez y Roberto E. Caligaris.
Fundamentos de Cristalografía Física, por Jaime Rodríguez Lara.
Teoría Cuántica del Impulso Angular, por Manuel de Llano y Mauricio Fortes.

Serie de química

Fisicoquímica de Interfases, por Francisco Javier Garfias.
Química de Sólidos, por Julio César Bazán.
Química Bioinorgánica, por Henrique E. Toma.
Introducción al Estudio de los Productos Naturales, por Eduardo G. Gros.

Serie de biología

Etología: El Estudio del Comportamiento Animal, por Raúl Vaz-Ferreira.
Fotosíntesis, por Rubén H. Vallejos.
Cromosomas Humanos y de Primates, por Máximo E. Drets y Héctor Seuanez.
Limnología Sanitaria. Estudio de la Polución de Aguas Continentales, por Samuel Murgel Branco.
Aprovechamiento de Aguas Dulces y el Cultivo de Peces, por Argentino Boneto y Hugo P. Castillo.

Nota: Las personas interesadas en adquirir estas obras deben dirigirse a la Unidad de Ventas y Promoción, Organización de los Estados Americanos, Washington, D. C., 20006 - 4499 o a las Oficinas de la OEA en el país respectivo.