USC UNIVERSIDADE DE SANTIAGO DE COMPOSTELA
FACULTADE DE MATEMÁTICAS

Traballo Fin de Grao

Grupo de Brauer de un cuerpo

Andrés Siaba Rodríguez

2021/2022

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

GRAO DE MATEMÁTICAS

Traballo Fin de Grao

Grupo de Brauer de un cuerpo

Andrés Siaba Rodríguez

Septiembre, 2022

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

Trabajo propuesto

Área de Coñecemento: Álxebra
Título: Grupo de Brauer dun corpo.
Breve descrición do contido
O teorema de Frobenius afirma que o corpo dos números reais, o dos números complexos e o anel dos cuaternios, son as únicas álxebras de división de dimensión finita sobre $\mathbb{R}$ e as únicas centrais son $\mathbb{R}$ e $\mathbb{H}$. Clasificar as álxebras de división de dimensión finita e centrais sobre outros corpos é moito máis difícil. Neste traballo xustificarase que a clasificación de estas redúcese á clasificación das álxebras centrais e simples de dimensión finita. Así, introducirase unha relación de equivalencia no conxunto das K-álxebras centrais e simple de dimensión finita e probarase que o conxunto das clases de equivalencia de tales álxebras é un grupo, denominado o Grupo de Brauer do corpo K. Este grupo actúa como "clasificador" de álxebras de división centrais.
Recomendacións
Ë recomendable cursar as materias de Estruturas Alxébricas e Ecuacións Alxébricas.
Outras observacións

Índice

Resumen

Con la finalidad de dar una clasificación de las álgebras de división centrales de dimensión finita sobre un cuerpo K, en este trabajo se estudia la noción de álgebra central simple de dimensión finita sobre K y se define una relación de equivalencia en el conjunto de estas álgebras, lo que permite construir el grupo de Brauer del cuerpo K, $\mathrm{Br}(K)$. Se finaliza la memoria definiendo el grupo de Brauer relativo, $\mathrm{Br}(E/K)$, que además de ser útil para el estudio de $\mathrm{Br}(K)$, ya que simplifica cuestiones a cerca del grupo de Brauer de K a cuestiones en $\mathrm{Br}(E/K)$ para un cierto cuerpo E, permite dar una definición alternativa del grupo de Brauer del cuerpo K considerando extensiones de Galois finitas de K.

Abstract

With the aim of providing a classification of finite dimensional central division algebras over a field K, in this work we deal with the notion of finite dimensional central simple algebras over K and we define an equivalence relation in the set of these algebras, which allow us to construct the Brauer group of the field K, $\mathrm{Br}(K)$. The memoir ends defining the relative Brauer group, $\mathrm{Br}(E/K)$, that will also be useful for the study of $\mathrm{Br}(K)$, since it simplifies questions about the Brauer group of K to questions on $\mathrm{Br}(E/K)$ for a certain field E, allow us to give an alternative definition of the Brauer group of the field K by considering finite Galois extensions of K.

Introducción

En 1877, Ferdinand Georg Frobenius demostró que las únicas álgebras de división de dimensión finita sobre los números reales son: los propios reales, los números complejos y los cuaternios de Hamilton. Buscando generalizar este concepto, es decir, dar las posibles álgebras de división sobre un cuerpo determinado, nace la idea del grupo de Brauer, que es el objeto de estudio de este trabajo.

Treinta años más tarde, en 1907, Joseph Wedderburn (1882-1948) publica un artículo en Proceedings on the London Mathematical Society donde demuestra un Teorema, el *Teorema de Estructura de Wedderburn*, que caracteriza las álgebras de dimensión finitas centrales y simples sobre un cuerpo K como un anillo de matrices sobre un anillo de división. Este anillo, si se considera como álgebra sobre el mismo cuerpo, también es central. De esta manera, se plantea por primera vez el problema de clasificar, de manera general, estas álgebras centrales de división.

El grupo de Brauer fue definido en 1929 por Richard Brauer (1901-1977). Brauer fue un matemático alemán con importantes resultados en diversos ámbitos de las matemáticas, en especial el Álgebra Abstracta y la Teoría de Números. Ahora, gracias a las investigaciones de Brauer y de otros importantes matemáticos de la época, como Hasse y Noether, el problema planteado por Wedderburn en 1907 comienza a estar un paso más cerca de ser resuelto, al menos parcialmente. Estos trabajos concluyen que se puede obtener esta clasificación asociando al cuerpo un grupo abeliano, cuyos elementos son álgebras centrales simples de dimensión finita cocientadas por una relación de equivalencia.

Una vez caracterizado el grupo, Brauer aprovechó el trabajo existente sobre las extensiones de Galois para definir el grupo de Brauer relativo, dando una manera alternativa de construir este grupo.

Después, Brauer y Noether investigaron los conjuntos factores y su trabajo se incorporó a la moderna rama de las matemáticas que cogía fuerza en la época, conocida como el Álgebra

Homológica. De hecho, las interpretaciones homológicas del grupo de Brauer cobran una gran importancia, así por ejemplo el grupo de Brauer relativo es isomorfo al grupo de cohomología de Amitsur ([6]) .

A la hora de estudiar el grupo de Brauer de un cuerpo, la continuación natural es intentar estudiar el grupo de Brauer de un anillo conmutativo. Este estudio no solamente es interesante como generalización, si no porque ofrece la posibilidad de facilitar la construcción del grupo de Brauer clásico, ya que es habitual encontrar cuerpos con anillos asociados. Un ejemplo de esta situación es el anillo de polinomios con coeficientes en un cuerpo.

La memoria está organizada en tres Capítulos. En un primer Capítulo, se dan los conceptos necesarios para seguir el desarrollo del trabajo, es decir, nociones de álgebras, homomorfismos,... además de definir y caracterizar el producto tensor.

Después, se concentra el estudio en las álgebras centrales simples. Se definen los conceptos de simplicidad y centralidad en álgebras y se relacionan con las álgebras de matrices, además de estudiar su comportamiento bajo la actuación del producto tensor. Se sigue con el *Teorema de Estructura de Wedderburn* y las nociones de simplicidad y semisimplicidad necesarias para llegar a él. También se definen las extensiones de escalares, haciendo uso de las extensiones de cuerpos y se define el cuerpo de descomposición de un álgebra.

Por último, en el tercer Capítulo, se utilizarán todos los conceptos desarrollados anteriormente para construir finalmente el grupo de Brauer y se exponen algunos ejemplos de ciertas condiciones que se pueden imponer sobre los cuerpos de forma que se extraigan conclusiones inmediatas sobre su grupo de Brauer. Además, se definirá el grupo de Brauer relativo a una extensión de cuerpos y se justificará su utilidad para construir el grupo de Brauer clásico a partir de unas extensiones de cuerpos determinadas, las extensiones de Galois.

Para la realización de esta memoria se han seguido fundamentalmente los libros *Nonconmutative algebras* ([5]) y *Ring Theory*([11]).

Capítulo 1

Preliminares

En este Capítulo 1 se expondrán los conceptos básicos necesarios para seguir el desarrollo general del trabajo. Se comenzará definiendo las diferentes estructuras algebraicas sobre las que se trabajará y enunciando resultados básicos relacionados con ellas.

Además, en la Sección 1.2 se estudiará el producto tensor y sus características y diferencias según la estructura sobre la que se establezca.

El objetivo de este estudio es la construcción del grupo de Brauer de un cuerpo, así que las álgebras que se estudiarán están definidas sobre cuerpos. Por lo tanto, salvo que se especifique lo contrario, a lo largo de la memoria se entenderá que las álgebras son sobre un cuerpo. Además, también durante todo el trabajo, K denotará un cuerpo.

1.1. Conceptos básicos

En este trabajo, se utilizarán fundamentalmente álgebras. Un álgebra no es más que un anillo R dotado de una estructura de módulo sobre otro anillo (o sobre sí mismo). Por lo tanto es importante recordar los términos de anillo, módulo y álgebra, así como los conceptos relacionados con ellos. En esta Sección 1.1 se sentarán las bases para el resto del estudio, a la vez que se introducirá la notación.

Definición 1.1. Un **anillo**, $(R, +, \cdot)$, es un conjunto R no vacío con dos operaciones internas,

$$\begin{array}{rcl} + : R \times R & \longrightarrow & R \\ (x, y) & \longmapsto & x + y \end{array} \qquad \begin{array}{rcl} \cdot : R \times R & \longrightarrow & R \\ (x, y) & \longmapsto & x \cdot y \end{array}$$

verificando:

- $(R, +)$ es un grupo abeliano.
- $(R, \cdot)$ es un monoide (el producto es asociativo y tiene elemento neutro 1) y además el producto es distributivo con respecto a la suma, es decir, $x \cdot (y + z) = x \cdot y + x \cdot z$ y $(x + y) \cdot z = x \cdot z + y \cdot z$ para cualesquiera $x, y, z \in R$.

Si el producto también es conmutativo ($x \cdot y = y \cdot x \ \forall x, y \in R$) se dice que el anillo R es **conmutativo**.

Definición 1.2. Sean R y S dos anillos. Una aplicación $f : R \to S$ es un **homomorfismo de anillos** si $\forall x, y \in R$ se verifican las siguientes dos condiciones:

i. $f(a + b) = f(a) + f(b)$.

ii. $f(a \cdot b) = f(a) \cdot f(b)$.

Definición 1.3. Sea R un anillo. Un subconjunto $I \subseteq R$ es un **ideal por la izquierda** de R si verifica:

i. I es subgrupo de R con respecto a la suma ($(I, +) < (R, +)$).

ii. $r \cdot i \in I \ \ \forall r \in R, \forall i \in I$.

Análogamente, se define ideal por la derecha si I es subgrupo con respecto a la suma y si $i \cdot r \in I \ \forall r \in R, \forall i \in I$.

Si $I \subset R$ es ideal por la izquierda y por la derecha, se dice que es un **ideal bilátero**.

Definición 1.4. Un anillo se dice que es **simple** si no tiene ideales biláteros propios, es decir, si sus únicos ideales biláteros son $\{0\}$ y R.

Observación 1.5. Más adelante, se trabajará sobre un cuerpo. Nótese que un cuerpo no es más que un anillo conmutativo simple, ya que en un cuerpo todos sus elementos son unidades, por lo tanto sus únicos ideales son los triviales, es decir, el nulo y el total.

Sea R un anillo y n un entero positivo. Se denota por $M_n(R)$ el anillo de matrices $n \times n$ con coeficientes en el anillo R. Es muy interesante la relación entre los ideales de R y los de $M_n(R)$. Si I es un ideal por la izquierda de R entonces $M_n(I)$ es un ideal por la izquierda de $M_n(R)$, ya que el elemento a_{ij} de la matriz resultado de multiplicar una matriz con coeficientes en R por una con coeficientes en I será una suma de la forma $r_1 \cdot i_1 + r_2 \cdot i_2 + \cdots + r_n \cdot i_n$ que pertenece a I por ser suma de elementos de I ($r_j \cdot i_j \in I$ ya que I es ideal por la izquierda de R).

Este resultado se verifica análogamente para ideales derechos o biláteros, lo cual se resume en la siguiente proposición:

Proposición 1.6. *Sea R un anillo y n un entero positivo. Entonces existe una biyección entre los ideales de R y los de $M_n(R)$, de forma que:*

$$\begin{array}{rcl} R & \longrightarrow & M_n(R) \\ I & \longmapsto & M_n(I) \text{ ideal de } M_n(R). \end{array}$$

Corolario 1.7. *Sea n un entero positivo. Si R es un anillo simple. Entonces $M_n(R)$ también lo es.*

Definición 1.8. Sea R un anillo (no necesariamente conmutativo). Un **R-módulo por la izquierda** es un grupo abeliano $(M, +)$ con una operación externa:

$$\begin{array}{rcl} R \times M & \longrightarrow & M \\ (r, x) & \longmapsto & r \cdot x \end{array}$$

que para cualesquiera $r, s \in R$ y $x, y \in M$ verifica las siguientes propiedades:

i. $r \cdot (s \cdot x) = (r \cdot s) \cdot x$.

ii. $(r + s) \cdot x = r \cdot x + s \cdot x$.

iii. $r \cdot (x + y) = r \cdot x + r \cdot y$.

iv. $1_R \cdot x = x$.

Análogamente, se puede definir el concepto de R-módulo por la derecha.

Observación 1.9. Nótese que si R es conmutativo no es necesario diferenciar entre R-módulo por la derecha y R-módulo por la izquierda.

Definición 1.10. Dado un anillo $(R, +, \cdot)$, se define su **anillo opuesto** como el anillo $(R, +, *)$ cuya multiplicación está definida como $x * y = y \cdot x$, $\forall x, y \in R$. Lo denotaremos por R^{op}.

Si el anillo R es conmutativo, $R = R^{op}$ $(x * y = y \cdot x = x \cdot y)$.

El concepto de anillo opuesto se ve de forma muy clara con un ejemplo:

Ejemplo 1.11. Consideremos el anillo $\mathbb{Z}[x, y]$. Sean $f(x, y) = 2x^2yx + 3yxy$ y $g(x, y) = xyxy + 1$ dos polinomios en $\mathbb{Z}[X, Y]$. Su multiplicación sería:

$$f \cdot g = (2x^2yx + 3yxy) \cdot (xyxy + 1) = 2x^2yx^2yx + 2x^2yx + 3yxyxyxy + 3yxy.$$

Entonces su anillo opuesto, $(Z[x, y])^{op}$, tendrá los mismos elementos pero su multiplicación vendrá dada por:

$$\begin{aligned} f * g &= (2x^2yx + 3yxy) * (xyxy + 1) = (xyxy + 1) \cdot (2x^2yx + 3yxy) = \\ &= 2xyxyx^2yx + 3xyx^2xy + 2x^2yx + 3yxy. \end{aligned}$$

Observación 1.12. En el caso del anillo de matrices sobre un cuerpo $(M_n(K))$ existe un isomorfismo entre el propio anillo y su opuesto:

$$\begin{array}{ccc} M_n(K) & \longrightarrow & M_n(K)^{op} \\ B & \longmapsto & B^t \end{array}$$

que envía cada matriz en su traspuesta.

Proposición 1.13. *Todo R-módulo por la derecha es un R^{op}-módulo por la izquierda y viceversa.*

Definición 1.14. Un **álgebra** sobre un anillo conmutativo R es un anillo A que es a su vez un R-módulo y que satisface que la multiplicación de A como anillo y la que le viene dada por la estructura R-módulo son compatibles, es decir:

$$x \cdot (a \cdot b) = (x \cdot a) \cdot b = a \cdot (x \cdot b) \ \ \forall x \in R, a, b \in A.$$

Se dice que A es una R-álgebra.

El álgebra A se dice que es **conmutativa** si lo es como anillo.

Definición 1.15. Una **base** del R-álgebra A es una base de A como R-módulo.

Si la base de A es **finita** se dice que el R-álgebra A es de dimensión finita.

Definición 1.16. Sean A y B dos R-álgebras. Una aplicación $f : A \to B$ es un **homomorfismo de R-álgebras** si $\forall a, b \in A$, $\forall x \in R$ verifica las siguientes propiedades:

i. $f(a+b) = f(a) + f(b)$.

ii. $f(x \cdot a) = x \cdot f(a)$.

iii. $f(a \cdot b) = f(a) \cdot f(b)$.

iv. $f(1) = 1$.

Es decir, f es homomorfismo de anillos y de R-módulos a la vez.

Ejemplo 1.17. Sea M un grupo abeliano, se define su conjunto de endomorfismos:

$$\mathrm{End}(M) := \big\{ f : M \longrightarrow M \text{ tal que } f \text{ es homomorfismo} \big\}.$$

Si $f \in \mathrm{End}(M)$ entonces $f(0) = 0$ (por ser f homomorfismo). Además, la composición de endomorfismos de M es endomorfismo de M. Como consecuencia, están bien definidas las siguientes operaciones en $\mathrm{End}(M)$. Sean $\rho, \phi \in \mathrm{End}(M)$:

- $(\rho + \phi)(m) := \rho(m) + \phi(m), \ \forall m \in M.$
- $(\rho \cdot \phi)(m) := (\rho \circ \phi)(m) = \rho\big(\phi(m)\big), \ \forall m \in M.$

De esta manera, $\mathrm{End}(M)$ es un anillo.

Si en lugar de ser M un grupo abeliano, se considera M un R-módulo (para cierto anillo R), denotamos el conjunto de los endomorfismos de R-módulos $\mathrm{End}_R(M)$. Análogamente, $\mathrm{End}_R(M)$ es un anillo y, para $r \in R$ y $\phi \in \mathrm{End}_R(M)$, es un R-módulo mediante la operación:

$$(r\phi)(m) := r \cdot \phi(m), \quad \forall m \in M.$$

Si R es un anillo conmutativo, la operación externa se hace compatible con el producto de $\mathrm{End}_R(M)$ como anillo. De este modo, si M es un R-módulo y R es un anillo conmutativo, $\mathrm{End}_R(M)$ es una R-álgebra. Se puede ver sin dificultad que si M es libre de rango n, $\mathrm{End}_R(M) \approx M_n(R)$.

Definición 1.18. Cuaternios, $\mathbb{H}$.

Los cuaternios son espacios vectoriales de dimensión cuatro sobre los números reales dotados con una estructura de álgebra no conmutativa. Se denotan por $\mathbb{H}$ en honor a Hamilton, el matemático que los inventó. Su base, $\{1, i, j, k\}$, satisface las siguientes propiedades multiplicativas:

$$\begin{aligned} i^2 = j^2 = k^2 = -1, \\ ij = -ji = k, \\ jk = -kj = i, \\ ki = -ik = j. \end{aligned}$$

La siguiente tabla muestra todos los productos entre elementos básicos.

$\cdot$	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

Los cuaternios son una generalización (a dimensión 4) de los números complejos ($\mathbb{C}$). Ciertas definiciones y propiedades de $\mathbb{C}$ se generalizan a $\mathbb{H}$. Por ejemplo, sea $q = a + bi + cj + dk \in \mathbb{H}$ se define su **conjugado**:

$$\overline{q} := a - bi - cj - dk \in \mathbb{H}.$$

Es fácil comprobar que $\mathbb{H}$ (al igual que $\mathbb{C}$) cumple que $\overline{q} \cdot \overline{q} = \overline{qq}$.

Si $|q|$ denota la norma usual en $\mathbb{R}^4$, se cumple que $|q|^2 := q \cdot \overline{q} = \overline{q} \cdot q = a^2 + b^2 + c^2 + d^2 \in \mathbb{R}$. Así, sea $q \in \mathbb{H}$, $q \neq 0$ se tiene:

$$q \cdot \frac{\overline{q}}{|q|^2} = \frac{1}{|q|^2} \cdot (q \cdot \overline{q}) = \frac{1}{|q|^2} \cdot |q|^2 = 1.$$

En resumen, para todo $q \in \mathbb{H}$ no nulo existe $q^{-1} := \dfrac{\overline{q}}{|q|^2}$. Por tanto, se ha visto que $\mathbb{H}$ es una $\mathbb{R}$-álgebra de división.

1.2. Producto tensor

Durante esta sección se introduce el concepto de producto tensor, que se utilizará en el Capítulo 3 para la construcción del grupo de Brauer. Se empleará como base de la operación

del grupo. Este concepto como tal se puede aplicar a diversos contextos en el campo de las matemáticas. En este trabajo, se utilizará como la operación del grupo para el grupo de Brauer que se quiere construir.

Definición 1.19. Sea R un anillo y sean M,N y P tres R-módulos. Una aplicación R-**bilineal** es una aplicación

$$\begin{array}{rcl} f : M \times N & \longrightarrow & P \\ (x, y) & \longmapsto & f(x, y) \end{array}$$

que cumple que para cada $x_0 \in M$ y cada $y_0 \in N$ fijados se tiene que las aplicaciones:

$$\begin{array}{rcl} f_{x_0} : N & \longrightarrow & P \\ y & \longmapsto & f_{x_0}(y) := f(x_0, y) \end{array} \qquad \begin{array}{rcl} f_{y_0} : M & \longrightarrow & P \\ x & \longmapsto & f_{y_0}(x) := f(x, y_0) \end{array}$$

son aplicaciones R-lineales.

El conjunto de las aplicaciones R-bilineales de $M \times N$ en P se denota por $\mathrm{Bil}_R(M, N; P)$.

Observación 1.20. Se puede demostrar sin dificultad que $\mathrm{Bil}_R(M, N; P)$ es un R-módulo, ya que al ser aplicaciones bilineales verifican trivialmente las condiciones de R-módulo (Definición 1.8).

En este trabajo interesa estudiar las propiedades del producto tensor de álgebras sobre un cuerpo. Para ello, será suficiente definir el producto tensor de módulos sobre anillos conmutativos.

Definición 1.21. Sea R un anillo conmutativo y M y N dos R-módulos. Se considera el R-módulo libre $R^{M\times N}$ definido como conjunto de las combinaciones lineales de elementos de $M \times N$ con coeficientes en R. Sea ahora V el R-submódulo de $R^{M\times N}$ generado por los elementos de la forma:

$$\begin{gathered} (m + m', n) - (m, n) - (m', n), \\ (m, n + n') - (m, n) - (m, n'), \\ (r \cdot m, n) - r \cdot (m, n), \\ (m, r \cdot n) - r \cdot (m, n), \end{gathered}$$

$\forall m, m' \in M$, $\forall n, n' \in N$ y $\forall r \in R$.

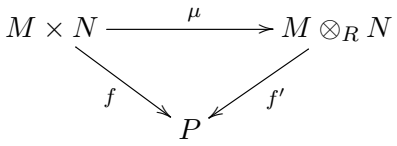
Se denomina **producto tensor** de M y N al cociente de $R^{M\times N}$ por el submódulo V. Se denota $M \otimes_R N$.

Esta definición da lugar a una aplicación bilineal canónica:

$$\begin{array}{rcl} \mu : \ M \times N & \longrightarrow & M \otimes_R N \\ (m, n) & \longmapsto & [(m, n)] := m \otimes n. \end{array}$$

Al fin y al cabo, el producto tensor de dos R-módulos M y N es el único R-módulo que se puede construir a partir de $M \times N$ de modo que se respete la bilinealidad. De esta manera, muchas veces se define el producto tensor por el siguiente teorema que lo caracteriza, conocido como la *Propiedad Universal del Producto tensor*:

Teorema 1.22. *Dado cualquier R-módulo P y una aplicación bilineal $f : M \times N \to P$ arbitraria, existe una única aplicación lineal $f' : M \otimes_R N \to P$ tal que $f = f' \circ \mu$. Dicho de otro modo, existe un único homomorfismo de R-módulos f' que hace que el siguiente diagrama sea conmutativo:*



Demostración. Basta con probar que la aplicación definida a continuación como Λ es un isomorfismo.

$$\begin{array}{rccc} \Lambda: & \mathrm{Hom}_R(M \otimes_R N, P) & \longrightarrow & \mathrm{Bil}_R(M, N; P) \\ & g & \longmapsto & \Lambda(g) \end{array}$$

donde $\Lambda(g)$ es una aplicación bilineal de $M \times N$ en P construida del siguiente modo:

$$\begin{array}{rccc} \Lambda(g): & M \times N & \longrightarrow & P \\ & (m, n) & \longmapsto & g(\mu(m, n)) = g(m \otimes n). \end{array}$$

Véase que efectivamente es isomorfismo:

- En primer lugar se comprueba que $\Lambda(g)$ es **bilineal** para todo $g \in \mathrm{Hom}_R(M \otimes_R N, P)$. Sean $r \in R$, $m, m' \in M$, $n \in N$ arbitrarios; se tiene:

$$\begin{aligned} \Lambda(g)(m + m', n) &= (g \circ \mu)(m + m', n) = g((m + m') \otimes n) \\ &= g(m \otimes n + m' \otimes n) = g(m \otimes n) + g(m' \otimes n) \\ &= \Lambda(g)(m, n) + \Lambda(g)(m', n). \\ \Lambda(g)(rm, n) &= (g \circ \mu)(rm, n) = g((rm) \otimes n) = g(r \cdot (m \otimes n)) \\ &= = r \cdot g(m \otimes n) = r \cdot \Lambda(g)(m, n). \end{aligned}$$

  Análogamente se puede comprobar que $\Lambda(g)(m, n + n') = \Lambda(g)(m, n) + \Lambda(g)(m, n')$ y que $\Lambda(g)(m, rn) = r \cdot \Lambda(g)(m, n)$, por lo que $\Lambda(g)$ es bilineal.

- Ahora, es necesario comprobar que Λ es una aplicación **lineal**.

$$\begin{aligned} \Lambda(g + g')(m, n) &= ((g + g') \circ \mu)(m, n) = (g \circ \mu)(m, n) + (g' \circ \mu)(m, n) \\ &= \Lambda(g)(m, n) + \Lambda(g')(m, n). \\ \Lambda(rg)(m, n) &= (rg \circ \mu)(m, n) = (rg)(m \otimes n) = r \cdot g(m \otimes n) = r \cdot \Lambda(g)(m, n). \end{aligned}$$

  Por lo tanto, Λ es lineal.

- Se continúa probando la **inyectividad** de Λ. Tomando una f del núcleo de Λ, es decir, tal que $\Lambda(f) = 0$, se tiene que $\Lambda(f)(m, n) = 0$ para cualesquiera $m \in M$ y $n \in N$. Además,

$$0 = \Lambda(f)(m, n) = f(m \otimes n)$$
$$\forall m \in M,\, \forall n \in N$$

  por lo que $f = 0$ y, por tanto, Λ es inyectiva.

- Por último, se ve que Λ es **sobreyectiva**. Sea $g \in \mathrm{Bil}_R(M, N; P)$, y $\mathcal{G}$ la aplicación $\mathcal{G} : R^{M\times N} \to P$ obtenida extendiendo g por linealidad. Al ser R-bilineal, $\mathcal{G}$ se anula en todos los generadores del R-submódulo de $R^{M\times N}$ que previamente fue denotado por V. Por lo tanto, $V \subseteq \ker \mathcal{G}$ y entonces existe un homomorfismo de R-módulos:

$$h : \quad M \otimes_R N = R^{M\times N} \,/\, V \quad \longrightarrow \quad P$$

  tal que $\Lambda(h) = h \circ \mu = g$. Es decir, para una $g \in \mathrm{Bil}_R(M, N; P)$ se ha encontrado una $h \in \mathrm{Hom}_R(M \otimes_R N, P)$ tal que $\Lambda(h) = f$. Por tanto, Λ es sobreyectiva.

Con todo esto, se concluye que Λ es isomorfismo. □

Se ha visto que, para dos módulos M y N sobre un anillo conmutativo R, $M \otimes_R N$ tiene estructura también de R-módulo. Como se ha indicado con anterioridad, se busca generalizar esta condición a dos álgebras sobre un cuerpo.

Proposición 1.23. *Sea K un cuerpo. Si R y S son dos K-álgebras, entonces $R \otimes_K S$ tiene estructura de K-álgebra con la operación:*

$$(r \otimes s) \cdot (r' \otimes s') = r \cdot r' \otimes s \cdot s',$$
$$\forall r, r' \in R,\, \forall s, s' \in S.$$

Las álgebras son, en particular, módulos. Se ha visto en la Definición 1.8 que el producto tensor de dos módulos es un módulo, por tanto, las operaciones suma y producto de un elemento de $R \otimes_K S$ por un elemento de K ya están definidas en $R \otimes_K S$ como K-módulo.

Observación 1.24. El elemento $1 \otimes 1$ es el elemento identidad (elemento neutro para el producto). Se pueden definir las inclusiones:

$$\begin{array}{rcl} i : R & \longrightarrow & R \otimes S \\ r & \longmapsto & r \otimes 1, \end{array} \qquad \begin{array}{rcl} j : S & \longrightarrow & R \otimes S \\ s & \longmapsto & 1 \otimes s. \end{array}$$

Si $\{e_\alpha\}$ es una base de S sobre K, todo elemento $x \in R \otimes S$ tiene una única expresión de la forma:

$$x = \sum r_\alpha \otimes e_\alpha = \sum (r_\alpha \otimes 1) \cdot (1 \otimes e_\alpha) = \sum i(r_\alpha) \cdot j(e_\alpha).$$

Si se considera $R \otimes S$ como R-módulo, $R \otimes S$ es libre con base $\{j(e_\alpha)\}$.

Si se tiene una base de R, análogamente $R \otimes S$ es libre como S-módulo y tiene una base inducida por la base de R. Por tanto, se puede identificar:

$$r \otimes s = (r \otimes 1) \cdot (1 \otimes s) = (1 \otimes s) \cdot (r \otimes 1)$$
$$\forall r \in R,\ \forall s \in S.$$

$R \otimes S$ contiene a R y a S como subálgebras conmutativas. Cabe destacar que aquí se hace referencia a que $(r \otimes 1) \cdot (1 \otimes s) = (1 \otimes s) \cdot (r \otimes 1)$, no se debe confundir con $r \otimes s = s \otimes r$, que no es cierto.

Se hará a $R \otimes_K S$ como el **producto tensor de** las **álgebras** S y R.

Como ya se ha comentado, las álgebras de matrices tendrán suma importancia en la construcción del grupo de Brauer. Por tanto, es importante estudiar su comportamiento con el producto tensor que, como también se ha mencionado previamente, será esencial también para la construcción del grupo.

Proposición 1.25. *Sea K un cuerpo, R una K-álgebra y $m, n \in \mathbb{N}$. Se tiene:*

(i) $M_n(R) \approx R \otimes_K M_n(K)$.

(ii) $M_m(K) \otimes_K M_n(K) \approx M_{mn}(K)$.

Demostración. Se tiene la inclusión natural $i : M_n(K) \hookrightarrow M_n(R)$ y además, siendo I la matriz identidad $n \times n$ en $M_n(R)$, existe una aplicación:

$$\begin{array}{ccc} R & \longrightarrow & M_n(R) \\ r & \longmapsto & rI. \end{array}$$

Entonces, si $A \in \mathrm{Im}(i) = M_n(K)$ y $r \in R$, se tiene:

$$(rI)A \;=\; rA \;=\; Ar \;=\; A(rI).$$

Por tanto, como las imágenes de ambas aplicaciones conmutan, existe un homomorfismo de anillos:

$$\begin{array}{ccc} R \otimes M_n(K) & \longrightarrow & M_n(R) \\ 1 \otimes e_{ij} & \longmapsto & e_{ij} \end{array}$$

donde e_{ij} denota la matriz con un 1 en la posición i, j y ceros en todas las demás entradas. Por tanto, esta aplicación lleva una base en una base, y así es un isomorfismo.

Para probar (ii) basta con aplicar lo anterior tomando $M_m(K)$ como R:

$$M_m(K) \otimes M_n(K) \underset{(i)}{\approx} M_n(M_m(K)) \approx M_{nm}(K).$$

□

Capítulo 2

Álgebras centrales simples

El objetivo de este trabajo es la construcción del grupo de Brauer. Es sabido que el fin de la construcción del grupo es la clasificación de las álgebras de división de dimensión finita sobre un cuerpo K dado. Para ello, será útil definir y caracterizar los conceptos de álgebra central y de álgebra simple. Debido al hecho de que el producto tensor de álgebras de división no es, en general, de división, la clasificación de este tipo de álgebras se reducirá a la de las álgebras centrales y simples.

Además, durante este Capítulo 2 se verán también (en las Secciones 2.3 y 2.4) los términos y resultados que se utilizarán para la construcción del grupo de Brauer relativo y para ser capaces de extraer conclusiones aplicables al grupo de Brauer a partir del grupo de Brauer relativo.

Todas las álgebras que se trabajarán son de dimensión finita. De esta forma, se dirá álgebra central simple para hacer referencia a álgebras centrales simples de dimensión finita sobre un cuerpo K.

2.1. Centralidad y simplicidad

Las álgebras centrales simples, como se ha mencionado, son los elementos fundamentales en el estudio del grupo de Brauer. Los conceptos y resultados vistos en esta Sección (2.1) y en la siguiente (Sección 2.2) serán suficientes para la construcción natural del grupo de Brauer que se verá en el Capítulo 3 (Sección 3.1).

Definición 2.1. Se denomina **centro** de la K-álgebra S al centro de S como anillo.

$$Z(S) := \left\{x \in S\colon\ s \cdot x = x \cdot s\ \forall s \in S\right\} \subset S.$$

Nótese que $K \subseteq Z(S)$.

Si $Z(S) = K$ se dice que S es una K-álgebra **central**.

Ejemplo 2.2. Los cuaternios son un ejemplo de álgebra central de división de dimensión finita.

- Claramente son un álgebra sobre $\mathbb{R}$.
- $\dim_{\mathbb{R}} \mathbb{H} = 4$, por lo que es de dimensión finita.
- Sólo los elementos de $\mathbb{R} \subsetneq \mathbb{H}$ conmutan con el resto, ya que los elementos básicos no conmutan ($i \cdot j = k \neq -k = j \cdot i$). Por tanto, $Z(\mathbb{H}) = \mathbb{R}$ y entonces es central.
- Ya se ha visto que para cualquier elemento $q \in \mathbb{H}$ no nulo, $\exists q^{-1} \in \mathbb{H}$, por lo que es de división.

Definición 2.3. Un álgebra A se dice que es **simple** si lo es como anillo (es decir, si no tiene ideales biláteros propios).

Proposición 2.4. *El centro de un anillo simple es un cuerpo. Por tanto, el centro de un álgebra simple es también un cuerpo.*

Demostración. Un cuerpo no es más que un anillo conmutativo simple. Si S es simple, $Z(S)$ es simple por ser subanillo de S, y es conmutativo porque los elementos del centro conmutan con todos los de S por lo que, en particular, conmutan entre ellos. □

Ejemplo 2.5. Cualquier cuerpo es un álgebra central simple de dimensión finita sobre sí mismo.

Para construir el grupo de Brauer de un cuerpo, es interesante estudiar las álgebras de matrices, ya que la relación de equivalencia que se definirá más adelante está directamente relacionada con este tipo de álgebras.

Proposición 2.6. *Sea R un anillo. Si A es una R-álgebra central, la R-álgebra de matrices $M_n(A)$ también lo es. En particular, si K es un cuerpo, $M_n(K)$ es central.*

Demostración. A excepción de la matriz identidad y la matriz nula, no existe ninguna matriz en $M_n(A)$ que conmute con todas las demás. Por tanto, $Z(M_n(A))$ contiene, como mucho, a los elementos de R. Claramente, para que un elemento de R conmute con cualquier matriz de $M_n(A)$, tiene que conmutar con todos los elementos de A (ya que las entradas de la matriz son elementos de A). Por tanto, los elementos del centro de $M_n(A)$ pertenecen todos a R y además conmutan con todos los elementos de A, es decir, $Z(M_n(A)) = Z(A)$. Como A es central por hipótesis, $Z(M_n(A)) = R$. □

Un álgebra es en esencia un anillo. Por lo tanto se puede ver fácilmente la validez de un análogo al Corolario 1.7 aplicado sobre álgebras:

Proposición 2.7. *Sea R un anillo y n un entero positivo. Si A es una R-álgebra simple, entonces $M_n(A)$ también lo es.*

Demostración. Se sigue de la Proposición 1.6 y del hecho de que un álgebra es simple si lo es como anillo (Definición 2.3). □

Estas definiciones llevan, de forma natural, a buscar ejemplos cómodos de este tipo de álgebras. La forma más sencilla de ejemplificar estas características (tanto la centralidad como la simplicidad) es a través de las álgebras de matrices, ya que imponiendo ciertas condiciones a los anillos a los que pertenecen los coeficientes de estas matrices, se pueden extraer conclusiones interesantes sobre la centralidad y la simplicidad de este tipo de álgebras.

Ejemplo 2.8. Para cualquier n entero positivo fijado, si K es un cuerpo, $M_n(K)$ es un álgebra central simple y de dimensión n (finita). Cabe destacar que si $n \geqq 2$, $M_n(K)$ no es un álgebra de división, ya que las matrices con rango menor o igual que $n-1$ no tienen inversa.

Ejemplo 2.9. Sea R un anillo simple. Entonces es un álgebra central y simple sobre su centro, $Z(R)$. Por tanto, $M_n(R)$ es un álgebra central y simple también sobre $Z(R)$.

Si además la dimensión de R sobre $Z(R)$ es finita, $M_n(R)$ es una $Z(R)$-álgebra simple central de dimensión finita.

En el Capítulo 3, será necesario utilizar el producto tensor como operación entre álgebras centrales simples. Por tanto, interesa estudiar el comportamiento de la centralidad y la simplicidad de las álgebras de dimensión finitas bajo la actuación del producto tensor.

Es obvio que si A y B son K-álgebras de dimensión finita, $A \otimes B$ será también de dimensión finita sobre K.

Los siguientes resultados aseguran el buen comportamiento de la centralidad y la simplicidad con este producto tensor. De hecho, el motivo de que se recurra a las álgebras centrales simples para clasificar las de división es, precisamente, el hecho de que el producto tensor de dos álgebras de división no es un álgebra de división en general.

Proposición 2.10. *Sean A y B dos álgebras sobre un cuerpo K. Si B es central, para cada $a \in A$ existe un isomorfismo de álgebras:*

$$\begin{array}{rccc} f: & Z(A) & \longrightarrow & Z(A \otimes B) \\ & a & \longmapsto & f(a) := a \otimes 1_B. \end{array}$$

Demostración. Debido a la bilinealidad del producto tensor, la aplicación f es lineal.
Sean $a \in Z(A)$, $a' \in A$ y $b' \in B$, entonces:

$$(a' \otimes b') \cdot f(a) = (a' \otimes b') \cdot (a \otimes 1_B) = a'a \otimes b \underset{a \in Z(A)}{=} aa' \otimes b = f(a) \cdot (a' \otimes b'),$$

y como los elementos de la forma $a' \otimes b'$ generan $A \otimes B$, se concluye que $f(a) \in Z(A \otimes B)$. Además, f es inyectiva por definición.

Falta comprobar la sobreyectividad de f. Para todo $x \in Z(A \otimes B)$, existen un n entero positivo, un conjunto $\{a_1, \ldots, a_n\}$ linealmente independiente en A y $b_1, \ldots, b_n \in B$ tales que $x = \sum_{i=1}^{n} a_i \otimes b_i$. Sea $b \in B$, como $x \in Z(A \otimes B)$, se tiene:

$$0 = (1 \otimes b) \cdot x - x \cdot (1 \otimes b) = \sum_{i=1}^{n} a_i \otimes (bb_i - b_i b).$$

Al ser $\{a_1, \ldots, a_n\}$ linealmente independiente, $bb_i = b_i b \ \forall i = 1, \ldots, n$. Como b es arbitrario, se deduce que $b_1, \ldots, b_n \in Z(B)$. Por hipótesis B es central, por lo que $Z(B) = K$, es decir, $b_1, \ldots, b_n \in K$. Por comodidad, para que sea más sencillo visualizar que son escalares (elementos de K), ahora se denotarán por $\lambda_1, \ldots, \lambda_n$. Entonces,

$$x = \sum_{i=1}^{n} a_i \otimes b_i = \sum_{i=1}^{n} a_i \otimes \lambda_i = \sum_{i=1}^{n} \lambda_i a_i \otimes 1_B = \left(\sum_{i=1}^{n} \lambda_i a_i \right) \otimes 1_B.$$

Por tanto, existe un elemento $a \in A$ tal que $x = a \otimes 1_B$ $(a = \sum \lambda_i a_i)$.
Para acabar, sea $a' \in A$ arbitrario, como x es central en $A \otimes B$:

$$0 = (a' \otimes 1_B) \cdot x - x \cdot (a' \otimes 1_B) = (a'a - aa') \otimes 1_B.$$

Entonces, $a'a = aa'$ y, al ser a' un elemento arbitrario de A, entonces $a \in Z(A)$. Por tanto, $x = f(a)$ y queda probada la sobreyectividad de f. □

Corolario 2.11. *Sea K un cuerpo y R y S dos K-álgebras centrales. Entonces $R \otimes_K S$ es una K-álgebra central.*

Es fácil comprobar que si K es un cuerpo, R una K-álgebra central simple y S una K-álgebra simple, entonces los ideales biláteros de $R \otimes S$ son de la forma $I \otimes S$, siendo I ideal bilátero de R. Por tanto, $R \otimes_K S$ es una K-álgebra simple, y así si R y S son álgebras centrales simples sobre K, entonces $S \otimes_K R$ también es central simple.

El recíproco también se tiene, es decir, si $R \otimes S$ es central simple se puede concluir que tanto R como S serán también centrales simples.

Proposición 2.12. *Sea K un cuerpo y S un álgebra central simple de dimensión finita sobre K. Entonces existe n entero positivo tal que $S \otimes S^o \approx M_n(K)$.*

2.2. Teorema de Wedderburn

En esta sección se introducirán los conceptos y resultados necesarios sobre semisimplicidad de modo que se llegue al Teorema de Wedderburn (Teorema 2.23) y sus conclusiones, que permitirán relacionar de forma directa las álgebras centrales simples de dimensión finita y las álgebras centrales de división de dimensión finita. De este modo, en el Capítulo 3 se define una relación de equivalencia entre álgebras centrales simples que permitirá clasificar las álgebras de división.

Definición 2.13. Sea R un anillo arbitrario. Un R-módulo por la izquierda M no nulo se dice **simple** si no contiene ningún submódulo propio no nulo.

Proposición 2.14. *Sean R un anillo y M un R-módulo por la izquierda. Equivalen:*

(i) M es un R-módulo simple.

(ii) *M es cíclico y cualquier elemento no nulo de M genera M, es decir, $\forall m \in M$ se tiene que $M = Rm$.*

(iii) *Existe un ideal maximal por la izquierda I de R tal que $M \approx R/I$.*

Demostración. $(i) \Rightarrow (ii)$
Sea $m \neq 0$ un elemento de M, entonces Rm es un submódulo de M distinto de cero, y por tanto (al ser M simple) $Rm = M$.

$(ii) \Rightarrow (iii)$
La aplicación: $\phi : R \to Rm = M$ es un homomorfismo sobreyectivo de R-módulos (ya que M es cíclico generado por m). El núcleo de esta aplicación será el aniquilador de m, es decir, $\ker \phi = (0 : m)$, un ideal maximal de R. Por tanto, denotando por I al aniquilador de m, por el *Primer Teorema de Isomorfía de Módulos* se tiene::

$$R/I \approx Rm.$$

$(iii) \Rightarrow (i)$
Por ser I ideal maximal, R/I es un R-módulo simple. □

Lema 2.15. *[12]* ***Schur.***
Sea R un anillo y M y N dos R-módulos simples por la izquierda. Entonces cualquier homomorfismo $f : M \to N$ es, o bien un isomorfismo, o bien el homomorfismo nulo. Por tanto el anillo de endomorfismos, $\mathrm{End}_R(M)$*, es un anillo de división.*

Demostración. Por ser f homomorfismo, $\ker f$ es un ideal de M e $\mathrm{Im}f$ es un ideal de N. Al ser M y N simples, $\ker f$ es o 0 o M e $\mathrm{Im}f$ es o 0 o N.

Si $\ker f = M$, entonces $\mathrm{Im}f = 0$ y f es el homomorfismo nulo. Si $\ker f = 0$, entonces $\mathrm{Im}f = N$ y f es un isomorfismo. □

Definición 2.16. Sea R un anillo y M un R-módulo por la izquierda. Se dice que M es **semisimple** si es suma directa de una familia de R-submódulos simples.

Ejemplo 2.17. Un $\mathbb{Z}$-módulo es semisimple si y sólo si es suma directa de módulos cíclicos de primer orden, es decir, si y sólo si cada elemento tiene un orden libre de cuadrados.

Ejemplo 2.18. Todos los módulos sobre un anillo de división son libres, es decir, tienen una base. Análogamente a los cuerpos, los módulos sobre anillos de división se denominan frecuentemente espacios vectoriales. Como toda sucesión exacta de módulos libres se descompone en módulos simples, cualquier módulo sobre un anillo de división es semisimple.

Definición 2.19. Un anillo R se dice que es **semisimple** si lo es como módulo sobre sí mismo (como R-módulo).

Observación 2.20. A priori, se debería diferenciar un anillo semisimple por la derecha y por la izquierda (según por dónde se considere el R-módulo). Se puede probar que ser semisimple por la derecha es equivalentes a ser semisimple por la izquierda, por tanto se dirá simplemente anillo semisimple.

Proposición 2.21. *Un anillo R es semisimple si y sólo si cualquier R-módulo es semisimple.*

Demostración. Sea M un R-módulo por la izquierda. Al ser R semisimple, Rm también lo es para cualquier elemento $m \in M$.
Entonces $M = \sum_{m \in M} Rm$ es semisimple.

Además, si M es un R-módulo semisimple, toda sucesión exacta corta de homomorfismos de R-módulos por la izquierda rompe. En particular, si I es un submódulo de M, la sucesión exacta $I \to R \to R/I$ rompe, y por tanto I es sumando directo de R. Así, R es semisimple. □

Ejemplo 2.22. Se sigue del Ejemplo 2.18 que todo anillo de división es semisimple.

Teorema 2.23. ***Wedderburn.***
Un anillo R es semisimple si y sólo si $R \approx M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)$ donde D_i es un anillo de división y n_i un entero positivo $\forall i \in \{1, \ldots, r\}$.

Demostración. Es consecuencia de que R como R-módulo es semisimple de longitud finita y de que $R^{op} \approx \mathrm{End}_R(R)$ es isomorfo a un producto finito $\prod M_{n_i}(D_i)$ de anillos de matrices sobre anillos de división D_i. Así,

$$R \approx (R^{op})^{op} \approx \prod \left(M_{n_i}(D_i)\right)^{op} \approx \prod M_{n_i}(D_i^{op}).$$

□

Este teorema se empleará para relacionar las álgebras centrales simples con las de división. El siguiente resultado recoge el contenido del Teorema de Wedderburn (Teorema 2.23) de una manera más directa. Para ello es necesario recurrir a la definición de anillo artiniano.

Definición 2.24. Un anillo R se dice que es **artiniano por la izquierda** si sus ideales por la izquierda satisfacen la condición de cadena descendente, es decir, cualquier conjunto de ideales por la izquierda de R admite un elemento mínimo para la relación de inclusión (estricta). Dicho de otra forma, R es un anillo para el cual no existe una cadena infinita estrictamente descendiente de ideales de R.

Análogamente se define anillo artiniano por la derecha. Se dirá que un anillo **es artiniano** si lo es por la derecha y por la izquierda.

Observación 2.25. Nótese que un anillo puede ser simple y no artiniano, ya que la noción de simplicidad hace referencia a ideales biláteros, mientras que el ser artiniano depende de ideales por la izquierda o por la derecha, no necesariamente biláteros.

Por ejemplo, el **álgebra de Weyl** sobre un cuerpo K: $A_1 = \{x, y \in K : xy - yx = 1\}$ es simple cuando la característica de K es cero, pero no es artiniano, ya que los ideales por la izquierda $A_1 x^i$ forman una sucesión infinita decreciente de ideales decrecientes que no se estabiliza nunca.

Teorema 2.26. *Sea R un anillo. Son equivalentes:*

(i) *R es un anillo artiniano simple.*

(ii) *R es semisimple y todos los R-módulos simples son isomorfos.*

(iii) *Existe n entero positivo y un anillo de división D tales que $R \approx M_n(D)$ como anillos.*

Demostración. $(i) \Rightarrow (ii)$
Para cualquier R-módulo M no vacío su aniquilador, que se denota por $(0 : M)$, es un ideal bilátero de R. Además, como M es no vacío, $1 \notin (0 : M)$, por tanto $(0 : M) = 0$ ya que R es simple. Entonces cualquier R-módulo es fiel. Además, al ser R artiniano, existe un R-módulo simple. Entonces R tiene un módulo fiel simple, M. Además, si se consideran todos los R-homomorfismos $f : R \to M^n$ y se escoge uno con núcleo mínimo (se puede hacer ya que R es artiniano), f es inyectivo. Esto se debe a que al ser M fiel, $\exists m \in M$ tal que $rm \neq 0$ $\forall r \in R$ y entonces si f no fuese inyectivo la aplicación:

$$\begin{array}{ccc} R & \longrightarrow & M^n \oplus M \\ x & \longmapsto & (f(x), xm) \end{array}$$

tendría un núcleo más pequeño que f, dando una contradicción. Entonces R es submódulo de M^n, por lo que R es semisimple y homogéneo.

$(ii) \Rightarrow (iii)$
Si R es semisimple es suma directa de módulos simples. Cada módulo simple es isomorfo por el *Teorema de Wedderburn* (Teorema 2.23) a un anillo de matrices sobre un anillo de división D. Como todos los sumandos directos son isomorfos, el anillo de división D es el mismo en todos los sumandos. Entonces, R es isomorfo a un anillo de matrices sobre D.

$(iii) \Rightarrow (i)$
Es conclusión de que un anillo de matrices sobre un anillo de división es simple y artiniano. □

Corolario 2.27. *Sea R un anillo artiniano simple. Entonces existe un entero positivo n y un anillo de división D (único salvo isomorfismo) tal que $R \approx M_n(D)$ como anillos.*

El siguiente resultado permite aplicar el Teorema 2.26 a las álgebras centrales simples, ya que estas son finitas.

Proposición 2.28. *Sea K un cuerpo y R una K-álgebra de dimensión finita. Entonces R es un anillo artiniano.*

Demostración. Sea R un álgebra de dimensión finita sobre K y suponiendo que existe una cadena estrictamente decreciente de ideales por la izquierda de R:

$$I_1 \supsetneq I_2 \supsetneq \dots$$

Cada ideal I_i es un K-submódulo de R, por tanto (al ser R un álgebra de dimensión finita) es de dimensión finita sobre K. Como la cadena es estrictamente descendiente, se tiene $\dim_K(I_1) > \dim_K(I_2)$... y por tanto, al estar los enteros bien ordenados y siendo $\dim_K(I_1)$ (la mayor de todas) finita, se tiene que la cadena no puede ser estrictamente descendiente. Por tanto, R es artiniano por la izquierda. Con un razonamiento análogo, se concluye R es artiniano por la derecha y por tanto, es artiniano. □

Si K es un cuerpo y R una K-álgebra de dimensión finita, por la Proposición 2.28, se tiene que R es un anillo artiniano. Además, por el Teorema 2.26, es simple si y sólo si existe un entero

positivo n y una K-álgebra de división D tales que $R \approx M_n(D)$. Además, si R es central entonces D también, ya que $Z(M_n(D)) = Z(D)$ y si R y $M_n(D)$ son isomorfas tienen el mismo centro.

De esta manera, un álgebra de dimensión finita R, será un álgebra central simple siempre que sea isomorfa a $M_n(D)$, siendo n un entero positivo y D un álgebra de división.

Proposición 2.29. *Sea K un cuerpo algebraicamente cerrado, es decir, tal que todo polinomio de $K[X]$ (de grado al menos 1) tiene un cero en K. Cualquier álgebra de división de dimensión finita sobre K es isomorfa a K como K-álgebra.*

Demostración. Si D es un álgebra de división de dimensión finita sobre K y x un elemento de D. Entonces x genera la extensión $K(x)$ de K, que es finita porque D es de dimensión finita sobre K. Como las extensiones finitas son algebraicas y K es algebraicamente cerrado, es decir, no tiene extensiones algebraicas propias, entonces se tiene que $K(x) = K$. Así, $x \in K$ y entonces $D = K$. □

Corolario 2.30. *Sea K un cuerpo algebraicamente cerrado. Entonces cualquier K-álgebra central simple es isomorfa a $M_n(K)$ como K-álgebra para algún entero positivo n.*

2.3. Extensión de escalares

Si S es una K-álgebra a los elementos de K se les denomina **escalares**. Una extensión de un cuerpo K es otro cuerpo E tal que $K \subseteq E$ y se denota $E|K$. Aplicando este concepto, dada una extensión $E|K$, interesa extender los escalares del álgebra S (es decir, los elementos de K) a todo E. Visto de otro modo, se trata de construir, a partir de S, una E-álgebra.

Para lograrlo, se empleará el producto tensor. De hecho, la construcción de los números complejos a partir de $\mathbb{R}$ es un caso particular de este concepto.

Observación 2.31. Dada una extensión de cuerpos $E|K$, es habitual considerar E como un espacio vectorial sobre K. Claramente la multiplicación interna de E como anillo (un cuerpo es en particular un anillo) y la externa como K-módulo son compatibles. Por tanto, E es una álgebra sobre K.

Además, E es un cuerpo y por tanto es conmutativo, es decir, E es una K-álgebra conmutativa.

Observación 2.32. Nótese que cualquier extensión de cuerpos propia ($E \supsetneq K$) nunca será central como K-álgebra, ya que E es un cuerpo, es decir, $Z(E) = E \neq K$. El ejemplo más claro es el caso de $\mathbb{C}|\mathbb{R}$, que, como se ha comentado previamente, es una $\mathbb{R}$-álgebra simple pero no es central.

Definición 2.33. Sea S una K-álgebra y $E|K$ una extensión de cuerpos. Se dice que S_E es la E-álgebra obtenida a partir de S por extensión de escalares:

$$S_E := E \otimes_K S.$$

Observación 2.34. El conjunto S_E (Definición 2.33) es una E-álgebra:
S como K-álgebra está descrita por una base $\{e_i\}$ de S y una forma de multiplicar los elementos básicos:

$$e_i \cdot e_j = \textstyle\sum_k c_{ijk} e_k \quad \text{donde} \quad c_{ijk} \in K.$$

S_E como anillo, se define a partir la misma base que S y la misma regla multiplicativa. Para concluir que S_E es una E-álgebra, hace falta dotarlo de estructura de E-módulo.

En la Observación 1.24 se deduce que se puede considerar $\{e_i\}$, denotando como $\{e_i\}$ al conjunto $\{1_E \otimes e_i\}$, como base de S_E como E-módulo (ya que $S_E = E \otimes S$). Por tanto, la dimensión de S_E sobre E es la misma que la dimensión de S sobre K:

$$[S_E : E] \quad = \quad [S : K].$$

$[S : K]$ denota la dimensión de S sobre K, es decir, la dimensión de S como K-espacio vectorial ($\dim_K(S)$).

Además, la operación externa por elementos de E es compatible con el producto interno de S_E (como anillo), al ser $K \subset E$. De este modo, S_E es una E-álgebra y el siguiente diagrama es conmutativo:

$$\begin{array}{ccc} K & \longrightarrow & S \\ \downarrow & & \downarrow \\ E & \longrightarrow & S_E \end{array}$$

Ejemplo 2.35. El ejemplo más habitual que se puede encontrar de extensión de escalares es la **complexificación** de una $\mathbb{R}$-álgebra S ([10]). Se construye a partir de S la $\mathbb{C}$-álgebra denotada por $S_{\mathbb{C}}$. Nótese que si tomamos $S = \mathbb{R}$, entonces $S_{\mathbb{C}} = \mathbb{C}$.

Un caso particular a destacar es la complexificación de $\mathbb{H}$:

$$\mathbb{H}_{\mathbb{C}} = \mathbb{C} \otimes_{\mathbb{R}} \mathbb{H},$$

que es un álgebra de dimensión 4 sobre $\mathbb{C}$. De hecho, se puede ver que es una $\mathbb{C}$-álgebra simple e isomorfa a $M_2(\mathbb{C})$.

Proposición 2.36. *Si S es un álgebra central y simple sobre K, entonces S_E es un álgebra central y simple sobre E.*

Demostración. S es un una K-álgebra central simple y E también es un álgebra simple sobre K. Por tanto, por lo visto previamente, se tiene que $S_E = E \otimes S$ es una K-álgebra simple y en conclusión, un álgebra simple sobre E.

Por otro lado, S es un álgebra central, por tanto, por la Proposición 2.10, existe un isomorfismo entre $Z(E)$ y $Z(E \otimes S)$, que es precisamente el centro de S_E. Por tanto, $Z(S_E) = E$ y S_E es central. □

Observación 2.37. El recíproco de la Proposición 2.36 también se tiene.

La extensión de escalares se puede aplicar también a las funciones lineales y se comportan con las propiedades esperables:

Proposición 2.38. *Sea $E|K$ una extensión de cuerpos, S una K-álgebra y R una E-álgebra. Si $f : S \to R$ es una aplicación K-lineal, entonces existe una única aplicación E-lineal de S_E en R:*

$$\begin{array}{rccc} \overline{f}: & S_E & \longrightarrow & R \\ & 1_E \otimes s & \longmapsto & \overline{f}(1_E \otimes s) := f(s). \end{array}$$

Demostración. La existencia es consecuencia de que $(e, s) \in E \times S \mapsto e \cdot f(s) \in R$ es una función bilineal.

Como el conjunto $\{1_E \otimes s\}$ genera a S_E como E-álgebra, $\overline{f}$ es la única aplicación que satisface las condiciones. □

Por otro lado, en el Capítulo 3 se exigirá a las álgebras que sean centrales y simples, por lo que es interesante estudiar el comportamiento de las extensiones de escalares respecto a su simplicidad

y a su centralidad. Al fin y al cabo, esto no es más que un caso particular de dos resultados vistos en la Sección 2.1, estudiando la evolución de estas características bajo la actuación del producto tensor (ya que una extensión de escalares es, en esencia, un producto tensor).

Proposición 2.39. *Sea S una K-álgebra central simple y $E|K$ una extensión de cuerpos.*

(i) *S_E es una E-álgebra central.*

(ii) *S_E es un álgebra simple.*

Demostración. Si se aplica la Proposición 2.10 a este contexto se concluye que:

$$Z(S_E) = Z(E) \otimes Z(S) = E \otimes K \approx E.$$

Por tanto, S_E es un álgebra central sobre E.

Análogamente, para probar (ii), basta con aplicar un resultado visto en la Sección 2.1. Al ser S simple y central y E simple (es un cuerpo), se tiene que S_E es simple. □

Corolario 2.40. *Si S es un álgebra central simple sobre K y $E|K$ es una extensión de cuerpos, S_E es un álgebra central simple sobre E.*

Demostración. Se sigue directamente de la Proposición 2.39 y del hecho de que si S es finita sobre K entonces S_E es finita sobre E (Observación 2.34). □

Teorema 2.41. *Sea D un álgebra de división finita sobre su centro K, entonces $[D : K]$ es un cuadrado.*

2.4. Cuerpos de descomposición

En la Proposición 2.30 se ha visto que cualquier álgebra central simple de dimensión finita sobre un cuerpo algebraicamente cerrado es isomorfa a un álgebra de matrices sobre ese mismo cuerpo. En particular, si se considera un álgebra central simple de dimensión finita sobre un cuerpo K, la extensión de escalares $S_{\overline{K}}$ (siendo $\overline{K}$ la clausura algebraica de K) es un álgebra

de dimensión finita central y simple sobre $\overline{K}$, que es algebraicamente cerrado. Por tanto, $S_{\overline{K}} \approx M_n(\overline{K})$ para algún n entero positivo.

En general, si $E|K$ es una extensión arbitraria, se tiene que $E \otimes_K M_m(K) \approx M_m(E)$, $\forall m \in \mathbb{Z}_{>0}$ (Proposición 1.25).

Proposición 2.42. *Sea S una K-álgebra central simple de dimensión finita. Entonces el rango de S sobre K es n^2 para algún n entero positivo, es decir, es un cuadrado.*

Demostración. Existe $n \in \mathbb{Z}_{>0}$ tal que $S_{\overline{K}} \approx M_n(\overline{K})$ en donde $\overline{K}$ la clausura algebraica de K. Entonces:

$$[S : K] = [S_{\overline{K}} : \overline{K}] = [M_n(\overline{K}) : \overline{K}] = n^2.$$

□

Definición 2.43. Sea S un álgebra central simple de dimensión finita sobre K. Se le llama **grado** de S sobre K al entero $\sqrt{[S : K]}$.

Ahora, se define cuerpo de descomposición de un álgebra:

Definición 2.44. Se dice que una K-álgebra central simple de dimensión finita, S, **se descompone** sobre E si existe n entero positivo tal que S_E es isomorfa a $M_n(E)$ como E-álgebras ($S_E \approx M_n(E)$).

También es habitual decir que E es un **cuerpo de descomposición** para el álgebra S.

Proposición 2.45. *Sea S una K-álgebra central simple de dimensión finita, sea n el grado de S (sobre K) y $E|K$ una extensión que descomponga a S. Entonces $S_E \approx M_n(E)$.*

Demostración. Por definición, $S_E \approx M_i(E)$ para algún i entero positivo, se tiene:

$$i^2 \;=\; [S_E : E] \;=\; [S : K] \;=\; n^2.$$

Al ser i y n enteros positivos, se concluye que $i = n$. □

Observación 2.46. La Proposición 2.45 indica que el entero n de la Definición 2.44 no es arbitrario, sino que es el grado de S.

El estudio que se hará en el Capítulo 3 sobre el grupo de Brauer relativo estará basado en las extensiones de escalares y en los cuerpos de descomposición. De hecho, por razones que se harán evidentes más adelante, interesa especialmente un tipo de cuerpos de descomposición para un álgebra simple y central. Para poder definir este tipo de cuerpos es necesario recurrir a las subálgebras centralizadoras y al *Teorema Centralizador* (Teorema 2.49):

Definición 2.47. Sea S un álgebra y D un subconjunto de S. Se define el **centralizador** de D en S como:

$$C_S(D) := \{s \in S \colon sx = xs \ \forall x \in D\}.$$

Observación 2.48. Se puede comprobar que $C_S(D)$ es una subálgebra de S para cualquier subconjunto $D \subseteq S$.

Teorema 2.49. ***Centralizador.***
Sea S un álgebra central simple de dimensión finita sobre K y R una K-subálgebra simple de S. Entonces:

(i) $C_S(R)$ *es simple.*

(ii) $[S : K] = [R : K] \cdot [C_S(R) : K]$.

Demostración. Por el Teorema 2.26, se tiene que $S \approx M_n(D^{op}) \approx \mathrm{End}_D(V)$ donde D es un álgebra de división con centro Ky V es un D-módulo de dimensión finita. Además, V es también un $(R \otimes D)$-módulo y $C(R) = \mathrm{End}_{R\otimes D}(V)$.

Como $R \otimes D$ es simple, $R \otimes D \approx \mathrm{End}_E(W)$ siendo W el único $(R \otimes D)$-módulo simple y y $E = \mathrm{End}_{R\otimes D}(W)$ es el álgebra de división asociada. Entonces, $V \approx W^m$ como $(R \otimes D)$-módulos. Entonces,

$$C(R) \ \approx \ \mathrm{End}_{R\otimes D}(V) \ \approx \ M_m(\mathrm{End}_{R\otimes D}(W)) \ \approx \ M_m(E).$$

Por tanto, $C(R)$ es simple.

Para probar (ii), como $C(R) \approx M_n(E)$, se tiene que $[C(R) : K] = n^2 \cdot [E : K]$. Además, $V \approx W^n$ y por tanto $[V : K] = n \cdot [W : K] = n \cdot [W : E] \cdot [E : K]$. Despejando en esta igualdad y sustituyendo en la primera, se tiene que:

$$[C(R) : K] \ = \frac{[V : K]^2}{[W : E]^2[E : K]^2}[E : K] = \frac{[V : K]^2}{[W : E]^2[E : K]}$$

$$= \frac{[V : K]^2}{\dim_K(End_E(W))} = \frac{[V : K]^2}{[R : K][D : K]}.$$

Por lo tanto,

$$[R:K][C(R):K] = \frac{[V:K]^2}{[D:K]} = \frac{[V:D]^2[D:K]^2}{[D:K]} = [S:K].$$

□

Corolario 2.50. *Sea S un álgebra central simple de dimensión finita sobre K y R una K-subálgebra simple de S. Entonces $C_S(C_S(R)) = R$*

A este Corolario se le conoce frecuentemente como el Doble Teorema Centralizador.

Demostración. Aplicando la parte (ii) del Teorema 2.49 se tiene que:

$$[S:K] = [R:K] \cdot [C_S(R):K].$$

Por otro lado, al ser $C_S(R)$ simple (parte (i)), se puede aplicar de nuevo la parte (ii) tomando $C_S(R)$ como R. De este modo:

$$[S:K] = [C_S(R):K] \cdot [C_S(C_S(R)):K].$$

Juntando ambas expresiones, se sigue trivialmente que $[C_S(C_S(R)):K] = [R:K]$. Por definición, $R \subset C_S(C_S(R))$, y por tanto, $R = C_S(C_S(R))$ (ya que tienen la misma dimensión). □

Corolario 2.51. *Sea D es un álgebra de división central sobre un cuerpo K y $[D:K] = n^2$. Si E es un subcuerpo maximal de D, entonces $[D:E] = n$.*

Demostración. La primera parte es consecuencia de la parte (ii) del *Teorema Centralizador* (Teorema 2.49) y del Corolario 2.50: $n^2 = [D:K] = [E:K] \cdot [C(E):K]$ Al ser E un cuerpo, $C(E) = E$ y por tanto $[E:K] = n$.

Como $n^2 = [D:K] = [D:E] \cdot [E:K]$, se concluye que $[D:E] = n$. □

Ahora, se da una definición alternativa de subcuerpo maximal, más fuerte que la definición usual, es decir, que la maximalidad con respecto a la inclusión. Estos cuerpos (que más adelante se verá que son, en efecto, cuerpos de descomposición para el álgebra al que pertenecen) serán muy útiles para extraer consecuencias del grupo de Brauer relativo.

Definición 2.52. Sea S una K-álgebra simple. Se dirá que E es un **subcuerpo estrictamente maximal** de S si $K \subseteq E \subseteq S$ y es su propio centralizador ($C(E) = E$).

Observación 2.53. Si E es subcuerpo estrictamente maximal de S también es maximal con la definición usual (respecto a la inclusión). En efecto, sea E un subcuerpo de S que es igual a su centralizador y sea $\mathcal{F}$ una extensión de E en A. Entonces $\mathcal{F} \subset C_S(E)$ (por ser $\mathcal{F}$ un cuerpo que está contenido en S). Pero $C_S(E) = E$, por lo tanto, $\mathcal{F} \subset E$. Se concluye que E es subcuerpo maximal de S.

Por tanto, efectivamente la definición de cuerpo estrictamente maximal es más fuerte que la noción de maximalida con respecto a la inclusión.

El recíproco no se tiene, es decir, no todos los subcuerpos maximales son estrictamente maximales, y puede verse de forma sencilla con un ejemplo:

Ejemplo 2.54. Sea el anillo $M_{2n}(K)$ sobre un cuerpo K. Por el *Teorema Centralizador* (Teorema 2.49) y su Corolario (2.50), cualquier subcuerpo estrictamente maximal de $M_{2n}(K)$ tiene dimensión $2n$ (ya que la dimensión de $M_{2n}(K)$ es $4n^2$).

Considérese ahora el subanillo $S \subset M_{2n}(K)$ de las matrices de la forma:

$$\begin{pmatrix} aI & B \\ 0 & aI \end{pmatrix}$$

siendo $a \in K$, I la matriz identidad $(n \times n)$ y $B \in M_n(K)$ arbitraria.

S es un subanillo conmutativo de dimensión $n^2 + 1$. Por tanto, la dimensión de un subanillo conmutativo maximal es, como mínimo, $n^2 + 1$.

Por tanto, se evidencia que ambas definiciones no siempre coinciden.

Proposición 2.55. *Sea S un álgebra central simple de dimensión finita sobre K, n el grado de S y $E|K$ una extensión contenida en S. Entonces, los siguientes enunciados son equivalentes:*

(i) E es un subcuerpo estrictamente maximal de S.

(ii) E es de grado n sobre K.

(iii) E es una K-subálgebra conmutativa maximal de S.

Observación 2.56. Nótese que si D es una K-álgebra de división, cualquier K-subálgebra conmutativa de D es un cuerpo y, por tanto, cualquier subcuerpo maximal de D es estrictamente maximal.

Claramente, esto no se cumple en general para álgebras centrales simples. De hecho, en las álgebras centrales simples no siempre existen subcuerpos estrictamente maximales.

Lo que se acaba de ver en la Observación 2.56 se puede ver con un ejemplo:

Ejemplo 2.57. Se considera la $\mathbb{R}$-álgebra simple $M_n(\mathbb{H})$, de dimensión $4n^2$. De nuevo por el *Teorema Centralizador* y su Corolario, cualquier subcuerpo estrictamente maximal de $M_n(\mathbb{H})$ tiene que tener dimensión $2n$ sobre $\mathbb{R}$. Pero es sabido que las únicas extensiones finitas de $\mathbb{R}$ son $\mathbb{R}$ y $\mathbb{C}$ ([1]).

Por tanto, si $n > 1$, no existen subcuerpos estrictamente maximales de $M_n(\mathbb{H})$.

Como se ha mencionado al comienzo de la Sección 2.1, el objetivo es la clasificación de las álgebras centrales de división sobre un cuerpo dado. Sobre este punto en concreto y años antes de la definición del grupo, Frobenius demostró cuáles son las únicas álgebras de división sobre el cuerpo de los números reales. Este resultado es clave y se aprovechará para ejemplos y cálculos concretos.

Teorema 2.58. ***Frobenius.***
Sea D una $\mathbb{R}$-álgebra de división con $\mathbb{R} \subset Z(D)$ y $[D : \mathbb{R}] < \infty$. Entonces $D = \mathbb{R}$, $D = \mathbb{C}$ o $D = \mathbb{H}$.

Demostración. Sea E un sbcuerpo maximal de D. Entonces $[E : \mathbb{R}] < \infty$. Las únicas extensiones de cuerpos finitas de $\mathbb{R}$ son $\mathbb{R}$ y $\mathbb{C}$. Por tanto, $[E : \mathbb{R}] = 1$ o $[E : \mathbb{R}] = 2$.

Si $[E : \mathbb{R}] = 1$, entonces por el Corolario 2.51, $[D : \mathbb{R}] = 1$ y por tanto, $D = \mathbb{R}$.

En cambio, si $[E : \mathbb{R}] = 2$, entonces $[D : E] = 1$ o $[D : E] = 2$. Si $[D : E] = 1$, se concluye que $D = \mathbb{C}$, ya que $[D : \mathbb{R}] = [D : E] \cdot [E : \mathbb{R}] = 1 \cdot 2 = 2$.
Si $[D : E] = 2$, entonces $E \approx \mathbb{C}$ y la aplicación:

$$\begin{array}{rccc} f: & K & \longrightarrow & K \\ & a+bi & \longmapsto & a-bi \end{array}$$

es un $\mathbb{R}$-isomorfismo. Por tanto, $\forall a, b \in \mathbb{R}$ existe un elemento $x \in D$ tal que $x \cdot (a+bi)x^{-1} = a-bi$. Está claro que $f(f(a+bi))$, por tanto la conjugación por x^2 es la identidad, es decir:

$$x \cdot \left(x \cdot (a+bi) \cdot x^{-1}\right) \cdot x^{-1} = x^2 \cdot (a+bi) \cdot (x^{-1})^2 = a+bi.$$

Por tanto, los elementos de la forma x^2 conmutan con todos los de E, es decir, $x^2 \in C(E) = E$, $\forall x \in D$. Además, $f(x^2) = x^2$, por tanto, $x^2 \in \mathbb{R}$.

Si $x^2 > 0$ se tiene que $x^2 = r^2$ para algún $r \in \mathbb{R}$ y entonces $x = \pm r$ lo cual es una contradicción.

Si $x^2 < 0$ se tiene que $x^2 = -s^2$ para algún $s \in \mathbb{R}$. Denotando $j := x/y$ y $k := ij$, se comprueban las ecuaciones multiplicativas de $\mathbb{H}$ dadas en la Definición 1.18. Es fácil comprobar que es una base. □

Corolario 2.59. *Las únicas álgebras de división centrales de dimensión finita que existen sobre* $\mathbb{R}$ *son* $\mathbb{R}$ *y* $\mathbb{H}$*.*

Observación 2.60. La $\mathbb{R}$-álgebra de los números complejos $\mathbb{C}$ no es un álgebra central, ya que al ser conmutativa, $Z(\mathbb{C}) = \mathbb{C}$, por lo tanto no es central (el centro es distinto de $\mathbb{R}$). Por este motivo no se hace mención a $\mathbb{C}$ en el Corolario 2.59.

Del mismo modo, si se elimina la hipótesis de la asociatividad del álgebra (impuesta en la Definición 1.14), aparece una $\mathbb{R}$-álgebra de dimensión 8 con $\mathbb{R}$ contenido en el centro y de división, conocida como los Octonios de Cayley ($\mathbb{O}$). Existe una generalización del teorema de Frobenius que concluye que las únicas álgebras de división de dimensión finita sobre $\mathbb{R}$ son $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ y $\mathbb{O}$.

Capítulo 3

Grupo de Brauer de un cuerpo

Con la construcción de este grupo se busca obtener información para clasificar álgebras centrales de división de dimensión finita sobre un cuerpo K dado.

Una forma de abordar este problema es tratar de clasificar las álgebras centrales simples de dimensión finita sobre el cuerpo K, ya que se ha visto que para cada una de estas (S) corresponde una única K-álgebra de división de dimensión finita, D (aquella tal que $S \approx M_n(D)$).

Este Capítulo 3 se comienza dando una construcción natural de este grupo, definiendo el conjunto y la operación que los caracteriza y se finaliza definiendo el grupo de Brauer relativo de una extensión de cuerpos $E|K$ que será útil para el estudio del grupo de Brauer del cuerpo K.

3.1. Grupo de Brauer

Si $K = \mathbb{R}$ el teorema de Frobenius afirma que $\mathbb{R}$ y $\mathbb{H}$ son las únicas álgebras centrales de división de dimensión finita. Por tanto, el grupo de Brauer de $\mathbb{R}$ solamente tendrá dos elementos, uno representando a $\mathbb{R}$ y otro a $\mathbb{H}$, que serán distintos ya que $\mathbb{R} \not\approx \mathbb{H}$.

No siempre se podrá obtener la lista de elementos del grupo de Brauer (como en $\mathbb{R}$). Es decir, no siempre se podrá identificar explícitamente cada una de las posibles K-álgebras centrales de división de dimensión finita sobre un cuerpo arbitrario K.

Se trata de clasificar álgebras de dimensión finita. Por tanto, a partir de aquí, salvo que se indique lo contrario, se supondrá que las álgebras son de dimensión finita sobre un cuerpo, K.

Definición 3.1. Sean R y S álgebras centrales centrales simples de dimensión finita sobre K. Se dice que S es **similar** a R, y se denota $S \sim R$, si se verifica alguna de las siguientes condiciones:

i. Existen m y n dos enteros positivos tales que $M_m(S) \approx M_n(R)$.

ii. Si $S \approx M_n(C)$ y $R \approx M_m(D)$ para ciertos anillos de división D y E, entonces $D \approx E$.

iii. Existen $m, n \in \mathbb{N}$ tales que $S \otimes_K M_m(K) \approx R \otimes_K M_n(K)$.

iv. Si M es el único S-módulo simple y N es el único R-módulo simple, entonces $\mathrm{End}_S(M) \approx \mathrm{End}_R(N)$.

A esta relación, se le conoce como **relación de similaridad**.

Observación 3.2. Se puede probar sin dificultad que esta relación es de equivalencia. Que es reflexiva y simétrica es evidente. La transitividad es consecuencia de la Proposición 1.25.

Por tanto se tiene una relación de equivalencia en el conjunto de K-álgebras centrales simples de dimensión finita bien definida. La **clase de equivalencia** de una K-álgebra central simple de dimensión finita S se denotará como $[S]$. Al conjunto de estas clases de equivalencia, se le denotará por $\mathrm{Br}(K)$.

Observación 3.3. Cada elemento de $\mathrm{Br}(K)$ se corresponde con una K-álgebra central simple de dimensión finita no similar al resto, de ahí su utilidad para clasificar este tipo de álgebras bajo el criterio de similaridad definido previamente. De la misma manera, cada elemento de $\mathrm{Br}(K)$ se identifica también con un álgebra de división concreta.

Si $\mathrm{Br}(K) = 0$ entonces K es la única K-álgebra central simple de dimensión finita que existe sobre K.

Se busca darle a $\mathrm{Br}(K)$ estructura de grupo utilizando el producto tensor como base para la operación del grupo y la clase de equivalencia de K como K-álgebra central simple de dimensión finita actuando como el elemento neutro del grupo.

Lema 3.4. *Sean S, S', T y T' K-álgebras centrales simples de dimensión finita. Se tiene que si $S \sim S'$ y $T \sim T'$ entonces $S \otimes T \sim S' \otimes T'$.*

Demostración. Si dos álgebras centrales simples son similares tienen asociada la misma álgebra de división, así que, para ciertos enteros positivos m, n, m', n' y para ciertas álgebras de división

D y E, se tiene:

$$\begin{array}{cc} S \approx M_n(D) & T \approx M_m(E) \\ S' \approx M_{n'}(D) & T' \approx M_{m'}(E). \end{array}$$

Entonces, aplicando la Proposición 1.25:

$$\begin{aligned} S \otimes T &\approx M_n(D) \otimes M_m(E) \approx D \otimes M_n(K) \otimes E \otimes M_m(K) \\ &\approx D \otimes E \otimes M_{nm}(K) \approx M_{nm}(D \otimes E). \end{aligned}$$

Análogamente, $S' \otimes T' \approx M_{n'm'}(D \otimes E)$ y, por tanto, $S \otimes T \sim S' \otimes T'$. □

Proposición 3.5. $\mathrm{Br}(K)$ *con la operación* $S \bullet T = [S \otimes T]$ *es un grupo abeliano.*

Demostración. La operación está bien definida ya que si S y T son dos K-álgebras centrales simples de dimensión finita, entonces $S \otimes T$ es de dimensión finita. Además, al ser S y T centrales y simples, $S \otimes T$ también lo es y, por el Lema 3.4, si $S \sim S'$ y $T \sim T'$ se tiene que $S \otimes T \sim S' \otimes T'$.

La asociatividad de la operación es consecuencia directa de la asociatividad del producto tensor. $[K]$ es el elemento neutro del grupo y además, todo elemento tiene simétrico, ya que si S es un álgebra central simple de dimensión finita sobre K se tiene que $S \otimes S^o \approx M_n(K)$ (Proposición 2.12) y por lo tanto:

$$[S] \bullet [S^o] = [S \otimes S^o] = [M_n(K)] = [K].$$

Además, $\mathrm{Br}(K)$ es abeliano ya que para cualesquiera K-álgebras centrales simples de dimensión finita S y T, se tiene que $S \otimes T \approx T \otimes S$. □

Observación 3.6. A $\big(\mathrm{Br}(K), \bullet\big)$ se le denomina el **grupo de Brauer** del cuerpo K.

Ejemplo 3.7. Estudiando en particular $\mathrm{Br}(\mathbb{R})$, se tiene como consecuencia del *Teorema de Frobenius* (Corolario 2.59) que sólo tiene dos elementos. Por otro lado, $\mathrm{Br}(\mathbb{R})$ es un grupo y, por tanto, $\mathrm{Br}(\mathbb{R}) \approx \mathbb{Z}_2$.
De hecho, se puede identificar cada elemento de $\mathrm{Br}(\mathbb{R})$ con un elemento de $\mathbb{Z}_2$:

$$\begin{array}{ccc} \mathrm{Br}(\mathbb{R}) & \longrightarrow & \mathbb{Z}_2 \\ [\mathbb{R}] & \longmapsto & \overline{0} \\ [\mathbb{H}] & \longmapsto & \overline{1}. \end{array}$$

Proposición 3.8. *El grupo de Brauer de un cuerpo finito es trivial.*

Demostración. Es consecuencia de que cualquier dominio finito es un cuerpo(Pequeño Teorema de Wedderburn, 1905). Un anillo de división es, en particular, un dominio, por tanto todo anillo de división finito es un cuerpo.
Si D es una K-álgebra de división de dimensión finita (siendo K finito). Entonces D es un anillo de división finito (ya que tiene dimensión finita sobre K y K es finito). Por tanto D es un cuerpo y $Z(D) = D$. Entonces la única álgebra de división de dimensión finita y central es K. □

Proposición 3.9. *El grupo de Brauer de un cuerpo algebraicamente cerrado es trivial.*

Demostración. En el Corolario 2.30 se ha visto que no hay álgebras de división no triviales sobre un cuerpo algebraicamente cerrado. □

Tanto los cuerpos algebraicamente cerrados como los cuerpos finitos pertenecen a una familia más grande de cuerpos que tienen grupo de Brauer trivial, llamados los **cuerpos quasi-algebraicamente cerrados** ([13]).

Definición 3.10. Sea i un entero positivo. Se dice que un cuerpo K es C_i si para cualquier entero positivo n todo polinomio homogéneo (todos los monomios tienen el mismo grado) no constante $f \in K[X_1, \ldots, X_n]$ con $(\partial f)^i < n$ tiene un cero no trivial, donde ∂f denota el grado del polinomio f.

En particular, se dice que K es un **cuerpo quasi-algebraicamente cerrado** si es C_1, es decir, si cumple la propiedad que se acaba de enunciar para $i = 1$.

Observación 3.11. Un cuerpo K es quasi-algebraicamente cerrado si $\forall n \in \mathbb{Z}_{>0}$ cualquier polinomio $f \in K[X_1, \ldots, X_n]$ no constante y homogéneo con $\partial f < n$ tiene un cero no trivial, es decir, existen $x_i \in K$ no todos cero de modo que $f(x_1, \ldots, x_n) = 0$.

Observación 3.12. Si un cuerpo es C_i también es C_j $\forall j \in \mathbb{Z}_{\geq i}$.

Se considera K un cuerpo C_i. Sea $j \geq i$ y sea un n entero positivo fijado arbitrariamente. Se toma un $f \in K[X_1, \ldots, X_n]$ homogéneo no constante tal que $(\partial f)^j < n$.

Claramente $(\partial f)^i \leq (\partial f)^j$, por tanto $(\partial f)^i < n$ y, por ser K un cuerpo C_i, f tiene un cero no trivial en K.

Se concluye que K es un cuerpo C_j.

Teorema 3.13. *El grupo de Brauer de un cuerpo C_1 es trivial.*

Un cuerpo algebraicamente cerrado verifica la condición de ser C_0. Por tanto, es también C_1 (3.12) y entonces su grupo de Brauer será trivial.

Por otro lado, se ha probado en la Proposición 3.8 que el grupo de Brauer de un cuerpo finito es trivial. Resulta que un cuerpo finito es, en particular, un cuerpo C_1.

Esta conclusión se deduce del Teorema de Chevalley-Warning que afirma que si K es un cuerpo finito y n, m enteros positivos. Sean $f_1, \ldots, f_m \in K[X1, \ldots, X_n]$ polinomios no constantes verificando $\sum_{i=1}^{m} \partial f_i < n$. Entonces su lugar cero,

$$Z(f_1, \ldots, f_m) = \left\{x \in K^n \ / \ f_i(x) = 0 \ \forall i = 1, \ldots, m\right\} \subset K^n,$$

tiene un cardinal divisible por p.

Proposición 3.14. *Un cuerpo finito es C_1.*

Demostración. Es consecuencia directa del *Teorema de Chevalley-Warning.* □

Proposición 3.15. *Cualquier cuerpo algebraicamente cerrado es C_0.*

3.2. Grupo de Brauer relativo

Durante esta sección, se estudiará el grupo de Brauer relativo. Para ello, y durante todo el capítulo, se considerará una extensión de cuerpos $E|K$ y una K-álgebra central y simple de dimensión finita, S. Se ha visto en la Sección 2.3 que la extensión de escalares S_E es una E-álgebra. También se ha visto, en la Proposición 2.36 que si S es central y simple sobre K, S_E también lo es (pero sobre E, ya que es una E álgebra).

La extensión de escalares es la base de la construcción del grupo de Brauer relativo, por lo que es necesario conocer cómo se comporta la extensión de escalares con la relación de similaridad y con la operación definida en el grupo.

Dada una extensión de cuerpos $E|K$ se define la aplicación:

$$\begin{array}{rccc} \varphi_{_{E|K}}: & \mathrm{Br}(K) & \longrightarrow & \mathrm{Br}(E) \\ & [S] & \longmapsto & [S_E]\,, \end{array}$$

siendo S_E la extensión de escalares del álgebra S al cuerpo E, es decir $S_E = E \otimes_K S$. La aplicación $\varphi_{_{E|K}}$ está bien definida ya que si S es un álgebra sobre K y n un entero mayor que 1, existe un isomorfismo de E-álgebras:

$$(M_n(S))_E \;\approx\; M_n(S_E).$$

De esta manera, si S y S' son dos álgebras centrales simples similares, las E-álgebras S_E y S'_E también lo son.

Además, es un homomorfismo, ya que si S y S' son dos álgebras centrales simples sobre K, existe un isomorfismo de E-álgebras:

$$\begin{array}{rccc} \eta: & S_E \otimes_E S'_E & \longrightarrow & (S \otimes_K S')_E \\ & (1_E \otimes x) \otimes (1_E \otimes x') & \longmapsto & 1_E \otimes (x \otimes x'). \end{array}$$

El homomorfismo $\varphi_{_{E|K}}$ permite extraer información de $\mathrm{Br}(K)$ a partir de $\mathrm{Br}(E)$, con el que suele ser más fácil trabajar (por ejemplo, si se escoge una extensión algebraicamente cerrada).

Además, si se tiene una torre de cuerpos $F|E|K$, es decir, dos extensiones ($E|K$ y $F|E$) y si S es una K-álgebra, entonces existe un isomorfismo de F-álgebras:

$$(S_E)_F \;\approx\; S_F$$

y el siguiente diagrama es conmutativo:

$$\begin{array}{ccc} \mathrm{Br}(K) & \xrightarrow{\varphi_{_{E|K}}} & \mathrm{Br}(E) \\ & \searrow^{\varphi_{_{F|K}}} & \downarrow{\scriptstyle \varphi_{_{F|E}}} \\ & & \mathrm{Br}(F) \end{array}$$

Definición 3.16. Se llama **grupo de Brauer relativo** de la extensión $E|K$, y se denota $\mathrm{Br}(E/K)$ al núcleo de φ:

$$\mathrm{Br}(E/K) := \ker(\varphi : \mathrm{Br}(K) \to \mathrm{Br}(E)).$$

Dicho de otro modo, $\mathrm{Br}(E/K)$ es el conjunto de las clases de equivalencia de álgebras centrales simples cuyas extensiones de escalares al cuerpo E coinciden con la clase de equivalencia de E en $\mathrm{Br}(E)$. Es decir, son elementos $[S] \in \mathrm{Br}(K)$ tales que $[S_E] = [E \otimes S] = [E]$.

Observación 3.17. $\mathrm{Br}(E/K)$ es subgrupo de $\mathrm{Br}(K)$, ya que el núcleo de un homomorfismo es, por definición, subgrupo del grupo de partida del homomorfismo.

El objetivo de esta Sección 3.2 es buscar apoyo en el grupo de Brauer relativo para acabar construyendo (mediante los grupos de Brauer relativos de un tipo de extensiones determinadas) el grupo de Brauer del cuerpo K en sí, es decir, todas las clases de equivalencia de álgebras centrales simples sobre ese cuerpo dado.

Ahora, que se tiene la definición de este grupo, se busca la relación entre los cuerpos de descomposición y el grupo en sí. Este núcleo, $\mathrm{Br}(E/K)$, contiene todas las clases de K-álgebras centrales simples de dimensión finita que se descomponen sobre E, como se puede ver en el siguiente resultado.

Lema 3.18. *Sea K un cuerpo, S una K-álgebra central simple, n el grado de S y una extensión de cuerpos $E|K$. Entonces E es un cuerpo de descomposición para S si y sólo si $[S]$ es un elemento de* $\mathrm{Br}(E/K)$.

Demostración. Si E es un cuerpo de descomposición para S y S' una K-álgebra central simple similar a S. Entonces, existen i, j enteros positivos tales que $M_i(S) \approx M_j(S')$.

Por otro lado, como S se descompone sobre E, se tiene que: $S_E = E \otimes S \approx M_n(E)$. Además,

$$M_i(S_E) \approx E \otimes M_i(S) \approx M_i(M_n(E)) \approx M_{in}(E).$$

Como se ha visto que $M_i(S) \approx M_j(S')$:

$$E \otimes M_j(S') \approx M_j(S'_E) \approx M_{in}(E).$$

Por tanto, E y S'_E son álgebras similares como E-álgebras centrales simples (es decir, en $\mathrm{Br}(E)$), entonces S' también se descompone sobre E y ambas pertenecen a $\mathrm{Br}(E/K)$.

El recíproco se sigue directamente de la definición. □

Para profundizar en la utilidad de este grupo, se utilizará la noción de extensión de cuerpos de Galois.

Definición 3.19. Sea una extensión de cuerpos $E|K$. Se dice que $f \in K[X]$ es el **polinomio irreducible** de $\alpha \in E$ si es mónico, $f(\alpha) = 0$ y si, en caso de haber otro $g \in K[X]$ tal que $g(\alpha) = 0$ entonces f divide a g.

Definición 3.20. Una extensión de cuerpos $E|K$ se dice **normal** si para cualquier elemento $\alpha \in E$ el polinomio irreducible de α en K tiene todas sus raíces en E.

Definición 3.21. Una extensión $E|K$ se dice **separable** si todo elemento $\alpha \in E$ es separable sobre K, es decir, si es algebraico y si su polinomio irreducible sobre K tiene todas las raíces distintas sobre una clausura algebraica de K.

Observación 3.22. La condición de que los elementos sean algebraicos no afecta a este estudio, ya que se están considerando extensiones de cuerpos finitas y toda extensión de cuerpos finita es algebraica, es decir, todos sus elementos son algebraicos.

Definición 3.23. Sea una extensión de cuerpos $E|K$, se dice que es **de Galois** si es una extensión normal y separable.

Ahora se verá que para cualquier K-álgebra central simple S existe una extensión de Galois de K que es cuerpo de descomposición para S. De esta manera, se obtendrá una manera alternativa de construir el grupo de Brauer a partir del grupo de Brauer relativo.

Teorema 3.24. *Si S es un álgebra central simple de dimensión n^2, entonces cualquier subcuerpo estrictamente maximal E de S es un cuerpo de descomposición para S. Además, $[E : K] = [S : E] = n$.*

Demostración. Por el *Teorema Centralizador* (Teorema 2.49), se tiene que $[S : K] = [E : K] \cdot [C(E) : K]$. Al ser E un cuerpo, $C(E) = E$ y entonces $[S : K] = [E : K]^2$. Como por hipótesis $[S : K] = n^2$, entonces $[E : K] = n$.

Los eementos de E actúan en S por la izquierda y los elementos de S Por la derecha, y estas dos acciones conmutan. Así, se construye una aplicación:

$$\begin{array}{rccc} f: & E \otimes S & \longrightarrow & \mathrm{End}_E(S) \approx M_n(E) \\ & x \otimes s & \longmapsto & f(x \otimes s) \end{array}$$

de modo que que, para un $s' \in S$ arbitrario, $f(x \otimes s)(s') = xss'$. Como S es central y simple y E es simple (es un cuerpo) entonces $E \otimes S$ es simple. Por tanto f es inyectiva, al tener un dominio no vacío simple. Además, $[S_E : K] = [S_E : E] \cdot [E : K] = n^2 \cdot n = n^3$. Lo mismo pasa con $M_n(E)$, de este modo, al tener ambos dimensión n^3 sobre K, se tiene que f es isomorfismo. Por tanto, S se descompone sobre E. □

Teorema 3.25. ***Jacobson-Noether.***
Sea K un cuerpo y D una K-álgebra no conmutativa central de división. Entonces, existe un elemento $x \in D \backslash Z(D)$ que es separable sobre K.

Demostración. [9] □

Teorema 3.26. *Sea K un cuerpo y x un elemento de* $\mathrm{Br}(K)$. *Entonces, existe una extensión separable $E|K$ tal que $x \in \mathrm{Br}(E/K)$.*

Demostración. Si $[x] = [K]$ se tiene trivialmente.

Se asume, entonces, que $[x] \neq [K]$. Sea D un álgebra de división en $[x]$. Por el Teorema 3.25 existen subcuerpos separables de D que contienen a K. Sea E un subcuerpo de D que contenga a K y que sea maximal con respecto a la condición de ser separable como extensión de K. Se puede observar que la K-subálgebra $C_D(E)$ es de división y contiene a E. Por el Corolario 2.50: $E = C_D(C_D(E))$, por lo que E es el centro de $C_D(E)$. Por lo tanto, $C_D(E)$ es un álgebra de división central sobre E.

Si $E \neq C_D(E)$, por el Teorema 3.25, existe $y \in C_D(E) \backslash E$ tal que la extensión $E(y)|E$ es no trivial y separable. Entonces $E(y)$ es un subcuerpo de D separable sobre K y más grande que E, lo que contradice la maximalidad de E. Por tanto se concluye que $E = C_D(E)$.

Así, se tiene que E es cuerpo de descomposición para D. Entonces, $[x]$ es un elemento de $\mathrm{Br}(E/K)$. □

Corolario 3.27. *Sea K un cuerpo y* $[x] \in \mathrm{Br}(K)$. *Entonces existe una extensión de Galois E de K tal que $[x]$ es un elemento de* $\mathrm{Br}(E/K)$.

Corolario 3.28. *Sea K un cuerpo. Se tiene:*

$$\mathrm{Br}(K) = \bigcup_{E|K \text{ de Galois finitas}} \mathrm{Br}(E/K).$$

Demostración. La inclusión $\mathrm{Br}(K) \subset \bigcup_{E|K} \mathrm{Br}(E/K)$ es consecuencia directa del Corolario anterior.

Por otro lado, por definición de grupo de Brauer relativo, $\mathrm{Br}(E/K) \subset \mathrm{Br}(K)$ (para cualquier extensión $E|K$), por lo tanto, la otra inclusión se tiene inmediatamente. □

Bibliografía

[1] R. B. J. T. Allenby, *Rings, Fields and Groups*, Butterworth-Heinemann (1991).

[2] M. Auslander y O. Goldman, The Brauer Group of a Conmutative Ring, *American Mathematical Society* (2015).

[3] N. Bourbaki, *Elements of mathematics-Algebra*, Springer-Verlag (1973).

[4] P. L. Clark, *Nonconmutative Algebra*, Lecture Notes (2012).

[5] B. Farb y K. R. Dennis, *Nonconmutative algebra*, Springer-Verlag (1993).

[6] P. Guille y T. Szamuely, *Central simple algebras and Galois cohomology*, Cambridge Universuty Press (1983).

[7] N. Jacobson, *Finite-dimensional division algebras over fields*, Springer-Verlag (2010).

[8] A. Javanpeykar, *The Brauer Group of a Field*, Bachelor's thesis (2011).

[9] I. Kersten, *Brauergruppen*, Universitätsverlag Göttingen (1990).

[10] S. Roman, *Advanced Linear Algebra*, Springer-Verlag (2007).

[11] L. Rowen, *Ring Theory Volume 1*, Academic Press (1988).

[12] I. Schur, *Sitzungsberichte der Königlich Preußischen*, Akademie der Wissenschaften zu Berlin (1882).

[13] C. Tsen, *Zur Stufentheorie der Quasi-algebraisch-Abgeschlossenheit kommutativer Körper*, J. Chinese Mathematical Society 171 (1936), 81–92.