Álgebras no asociativas

Cándido Martín González
Departamento de Álgebra, Geometría y Topología.
Universidad de Málaga, 29080 Málaga

19 de febrero de 2008

Índice general

Capítulo 1

Preliminares

En este primer apartado trataremos de hacer una introducción con conceptos muy básicos de álgebras no necesariamente asociativas. Así, los conceptos de álgebra, subálgebra, ideales, cocientes, propiedad universal del mismo, tablas de multiplicar y otros, serán los que nos sirvan para adentrarnos en futuros capítulos de mayor profundida.

1.1. La categoría de las álgebras sobre un cuerpo

A lo largo de este libro trabajaremos con álgebras sobre cuerpos. El concepto de cuerpo hay que entenderlo en el sentido de anillo asociativo y conmutativo con unidad en el que todo elemento no nulo posee inverso. Así consideraremos un cuerpo fijo F y definiremos una *F-álgebra* como un espacio vectorial A sobre F provisto de una aplicación bilineal (llamado producto)

$$A \times A \to A$$

que asigna a cada pareja de elementos $(a, b) \in A \times A$ un nuevo elemento de A (denominado producto de a y b) que será denotado normalmente mediante la simple yuxtaposición ab de dichos elementos. El sentido que tiene la bilinealidad de la operación es desde luego que debe ser distributiva a derecha y a izquierda respecto a la suma, y que los escalares se comportan del siguiente modo

$$\lambda(ab) = (\lambda a)b = a(\lambda b), \forall a, b \in A, \forall \lambda \in F.$$

Si A es una F-álgebra , lo mismo podemos decir del álgebra opuesta A^{op} cuyo espacio vectorial subyacente es el mismo que el de A pero cuyo producto esta dado por la operación $a \cdot b := ba$ para cualesquiera $a, b \in A$. Si A y B son F-álgebras, una aplicación lineal $f : A \to B$ entre los espacios vectoriales subyacentes se dirá que es un *homomorfismo* de F-álgebras cuando $f(ab) = f(a)f(b)$ para cualesquiera $a, b \in A$. El conjunto de todos los homomorfismos de F-álgebras de A en B se denotará por $\hom_F(A, B)$. Los homomorfismos sobreyectivos se llaman *epimorfismos* y los inyectivos *monomorfismos*. Los que son a la vez monomorfismo y epimorfismo se llaman isomorfismos. Para denotar que dos álgebras A y B son isomorfas utilizaremos la notación $A \cong B$. Los homomorfismos de una F-álgebra en

sí misma se llamarán endomorfismos y utilizaremos la notación $\mathrm{End}_F(A) := \hom_F(A, A)$. Los isomorfismos de un álgebra en sí misma se llamaran automorfismos. Al conjunto de todos ellos lo denotaremos por $\mathrm{Aut}_F(A)$.

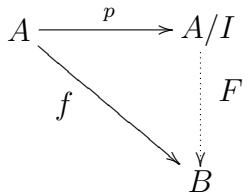
Diremos que B es una *subálgebra* de la F-álgebra A cuando B es un subespacio tal que las operaciones de A restringidas a B, dotan a esta de una estructura de F-álgebra. En este caso la inclusión $i : B \to A$ es un homomorfismo de F-álgebras. Un subespacio I de una F-álgebra A diremos que es un *ideal por la izquierda* cuando $\forall a \in A$, $\forall x \in I$, se tiene $ax \in I$ (usaremos la notación $I \lhd_i A$). Diremos que I es un *ideal por la derecha* cuando es un ideal por la izquierda del álgebra opuesta. En este caso usaremos la notación $I \lhd_d A$. Diremos que I es un *ideal bilátero* (o simplemente un *ideal*) de A cuando es un ideal por ambos lados. Esto lo denotaremos mediante $I \lhd A$.

Dado un homomorfismo de F-álgebras $f : A \to B$ se define el núcleo de f (denotado $\ker(f)$) como el conjunto de elementos cuya imagen por f es nula. Es trivial comprobar que $\ker(f)$ es un ideal de A.

Cuando I es un ideal de la F-álgebra A podemos considerar el espacio vectorial cociente A/I. Sus elementos son las clases de equivalencia de elementos $a \in A$. Denotaremos la clase de equivalencia de $a \in A$ mediante $[a]$. Sabemos que dicha clase consiste en el conjunto de todos los elementos de A que se relacionan con a. El espacio cociente A/I es por lo tanto $A/I := \{[a] : a \in A\}$. Este espacio lo podemos convertir en una F-álgebra definiendo el producto de clases mediante:

$$[a][b] := [ab] \tag{1.1}$$

La buena definición de esta operación es algo que queda como ejercicio al lector (se plantea en el problema 6). Esta estructura de álgebra definida en A/I es lo que llamaremos el álgebra cociente de A por el ideal I. Dicha álgebra cociente tiene una propiedad universal para describir la cual necesitaremos la definición de la proyección canónica $p : A \to A/I$ que asocia a cada elemento de A, su clase de equivalencia. Es decir, para cada $a \in A$ se tiene $p(a) = [a]$. Se demuestra sin dificultad que p es un epimorfismo de álgebras y que para cada homomorfismos de F-álgebras $f : A \to B$ tal que $I \subset \ker(f)$, existe un único homomorfismo de F-álgebras $F : A/I \to B$ haciendo conmutativo el diagrama:



es decir, tal que $F \circ p = f$. La demostración de esta propiedad se pide en el problema 7.

1.2. Constantes de estructura, tablas de multiplicar

Supongamos en esta sección que A es una F-álgebra de dimensión finita y fijemos una base $B = \{e_1, \ldots, e_n\}$ de A. Entonces el producto de cualesquiera dos elementos e_i y e_j de

A será una combinación lineal de los elementos de B:

$$e_i e_j = \sum_{k=1}^{n} \Gamma_{ijk} e_k, \ (\Gamma_{ijk} \in F).$$

Los escalares Γ_{ijk} se llaman *constantes de estructura* del álgebra relativas a B. Conocidos estos escalares podemos hacer virtualmente cualquier cálculo en A. Si tomamos dos elementos cualesquiera $a, b \in A$ y lo expresamos como combinación lineal de los elementos de la base $a = \sum_i \lambda_i e_i$, $b = \sum_j \mu_j e_j$, entonces

$$ab = (\sum_i \lambda_i e_i)(\sum_j \mu_j e_j) = \sum_{ij} \lambda_i \mu_j e_i e_j = \sum_{ijk} \lambda_i \mu_j \Gamma_{ijk} e_k,$$

y por lo tanto conocidas las constantes de estructura podemos multiplicar elementos cualesquiera del álgebra.

A veces se arregla el producto de elementos básicos en forma de tabla de doble entrada:

$\cdot$	e_1	$\cdots$	e_j	$\cdots$	e_n
e_1					
$\vdots$					
e_i			$\sum_k \Gamma_{ijk} e_k$		
$\vdots$					
e_n					

donde se escribe en el lugar (i, j) de la table el producto $e_i e_j$. Veamos algún ejemplo de interés. Vamos a introducir primero lo que se llama en la literatura matemática la función antisimétrica de orden tres. Tomemos el conjunto $I = \{1, 2, 3\}$ y la función

$$\epsilon : I \times I \times I \to \{0, 1\}$$

tal que $(i, j, k) \mapsto \epsilon_{ijk}$ de modo que

$$\epsilon_{ijk} = -\epsilon_{jik} = -\epsilon_{kji} = -\epsilon_{ikj}, \text{ siendo } \ \epsilon_{123} = 1.$$

A partir de la definición de ϵ se deduce que $\epsilon_{iij} = \epsilon_{jii} = \epsilon_{iji} = 0$. Pues bien, habiendo definido la función ϵ, definamos ahora una estructura de $\mathbb{R}$-álgebra cuyo espacio vectorial subyacente sea $\mathbb{R}^4$. Tomemos por ejemplo la base canónica

$$e_0 = (1, 0, 0, 0), e_1 = (0, 1, 0, 0), e_2 = (0, 0, 1, 0), e_3 = (0, 0, 0, 1).$$

Definamos una estructura de $\mathbb{R}$-álgebra en $\mathbb{R}^4$ mediante las relaciones

$$e_0 e_i = e_i e_0 = e_i, (i = 0, 1, 2, 3),$$

$$e_i e_j = -\delta_{ij} e_0 + \sum_{k=1}^{3} \epsilon_{ijk} e_k, \ (i, j \in \{1, 2, 3\})$$

donde δ_{ij} es la delta de Kronecker. De este modo tenemos definida una estructura de $\mathbb{R}$-álgebra, habiendo dado las constantes de estructura del álgebra. Si ahora nos molestamos en determinar los productos de los elementos básicos tenemos la table de multiplicar del álgebra respecto a la base canónica:

$\cdot$	e_0	e_1	e_2	e_3
e_0	e_0	e_1	e_2	e_3
e_1	e_1	$-e_0$	e_3	$-e_2$
e_2	e_2	$-e_3$	$-e_0$	e_1
e_3	e_3	e_2	$-e_1$	$-e_0$

.

Este álgebra recibe el nombre de *álgebra de cuaterniones reales de división*. Se suele denotar por $\mathbb{H}$. En capítulos que están por venir la definiremos de una forma más intrínseca. Por ahora, podemos conformarnos con comprobar que este álgebra tiene alguna de las propiedades que le dan su nombre. Por ejemplo $\mathbb{H}$ es un *álgebra de división*. Esto quiere decir que todo elemento no nulo posee inverso: $\forall x \in \mathbb{H}, \exists y \in \mathbb{H}$ tal que $xy = yx = 1$. Para demostrar esto usaremos la identificación natural que se suele hacer en toda álgebra con unidad, del cuerpo base con los múltiplos escalares de la unidad del álgebra. En nuestro caso identificaremos el cuerpo base $\mathbb{R}$ con $\mathbb{R}e_0$ (múltiplos escalares de la unidad) mediante la aplicación $r \mapsto re_0$. Ahora definiremos la *involución estandar* también conocida como involución de Cayley como la aplicación $n : \mathbb{H} \to \mathbb{H}$ tal que $x \mapsto \bar{x}$ donde para $x = x_0e_0 + x_1e_1 + x_2e_2 + x_3e_3$, se define $\bar{x} := x_0e_0 - x_1e_1 - x_2e_2 - x_3e_3$. Se comprueba que esta aplicación es lineal y verifica $\overline{xy} = \bar{y}\bar{x}$ y $\bar{\bar{x}} = x$ para todos $x, y \in \mathbb{H}$ (este es el objeto del problema 11). Ahora es fácil comprobar que para cada cuaternión $x \in \mathbb{H}$ se tiene $x\bar{x} \in \mathbb{R}e_0$ por lo cual podemos definir una aplicación llamada *norma cuaterniónica* $n : \mathbb{H} \to \mathbb{R}$ tal que $x\bar{x} = n(x)e_0$ para cada cuaternión x. Si calculamos $x\bar{x}$ encontraremos que para $x = x_0e_0 + x_1e_1 + x_2e_2 + x_3e_3$ se tiene $x\bar{x} = (x_0^2 + x_1^2 + x_2^2 + x_3^2)e_0$ por lo que la norma de x es $n(x) = \sum_{i=0}^{3} x_i 2$, es decir, coincide con el cuadrado de la norma euclídea. Este hecho lo podemos escribir de la forma $n(x) = x\bar{x} = \|x\|^2$. Esto implica que si $x \neq 0$ entonces $n(x) \neq 0$. En ese caso $x\bar{x} = n(x)e_0$ o bien $x\frac{\bar{x}}{n(x)} = 1$. Análogamente se demostraría que $\frac{\bar{x}}{n(x)}x = 1$ y por lo tanto todo $x \neq 0$ es inversible con inverso $x^{-1} = \frac{\bar{x}}{n(x)}$. Así el álgebra $\mathbb{H}$ es de división. Otra propiedad a destacar de $\mathbb{H}$ es que es un álgebra asociativa.

Teorema 1 *Sea A una F-álgebra con una base $B = \{e_i : i \in I\}$. Entonces A es asociativa si $(e_ie_j)e_k = e_i(e_je_k)$ para cualesquiera $i, j, k \in I$.*

Dem. Si el álgebra es asociativa, entonces necesariamente se tiene la condición del enunciado del teorema. Supongamos ahora que se satisface tal condición y veamos que el álgebra es asociativa: Sean $a, b, c \in A$ tales que se expresan como combinación lineal de los elementos de B en la forma

$$a = \sum_i \lambda_i e_i, \quad b = \sum_j \mu_j e_j, \quad c = \sum_k \gamma_k e_k.$$

Entonces $ab = \sum_{ij} \lambda_i\mu_j e_ie_j$ mientras que

$$(ab)c = (\sum_{ij} \lambda_i\mu_j e_ie_j)\sum_k \gamma_k e_k = \sum_{ijk} \lambda_i\mu_j\gamma_k(e_ie_j)e_k = \sum_{ijk} \lambda_i\mu_j\gamma_k e_i(e_je_k)$$

$$= \sum_i \lambda_i e_i (\sum_{jk} \mu_j \gamma_k e_j e_k) = a(bc),$$

lo que demuestra la asociatividad del álgebra. ■

Ahora la asociatividad de $\mathbb{H}$ se comprueba directamente sobre los elementos de la base.

1.3. Problemas

Problema 1 *En el espacio euclídeo $\mathbb{R}^3$ demuéstrese que una base $\{e_1, e_2, e_3\}$ tiene orientación positiva si y sólo si $e_3 = e_1 \wedge e_2$ donde $\wedge$ denota el producto vectorial de $\mathbb{R}^3$. Sugerencia: recuérdese que una base es positiva cuando la matriz del cambio de esa base a la canónica, tiene determinante positivo.*

Problema 2 *Sea $(\ ,\ )$ el producto escalar euclídeo de $\mathbb{R}^3$. Una isometría f de $\mathbb{R}^3$ es un isomorfismo lineal tal que $(f(x), f(y)) = (x, y)$ para todos $x, y \in \mathbb{R}^3$. El grupo de todas ellas con la composición se denota por $O(3)$. Se dice que una isometría es propia si transforma una base positiva en otra base positiva. Demuestra que el conjunto de las isometrías propias de $O(3)$ es un subgrupo normal (que se denotará por $SO(3)$ en lo sucesivo).*

Problema 3 *Demuéstrese que para una F-álgebra A, el conjunto $Aut_F(A)$ es un grupo para la composición de automorfismos.*

Problema 4 *Considérese el álgebra $\mathbb{H}$ de los cuaterniones reales de división. Fijemos la base canónica $\{1, i, j, k\}$ de dicha álgebra. Sea W el subespacio tridimensional generado por i, j y k. Se tiene entonces la descomposición $\mathbb{H} = \mathbb{R}1 \oplus W$ de modo que todo cuaternión q se puede escribir de la forma $q = \lambda 1 + w$ con $\lambda \in \mathbb{R}$ y $w \in W$. Si identificamos W con $\mathbb{R}^3$ de denotemos por (x, y) el producto escalar euclídeo y por $x \wedge y$ el producto vectorial de W. Demuéstrese que el producto de dos cuaterniones $q_1, q_2 \in \mathbb{H}$ con $q_i = \lambda_i 1 + w_i$ $(i = 1, 2)$ es precisamente:*

$$q_1 q_2 = [\lambda_1 \lambda_2 - (w_1, w_2)]1 + (\lambda_1 w_2 + \lambda_2 w_1 + w_1 \wedge w_2).$$

Sea q un cuaternión $q \in \mathbb{H}$, $q \notin \mathbb{R}1$. Demuéstrese que $q^2 \in \mathbb{R}1$ si y sólo si $q \in W$.

Problema 5 *Sea $f \in Aut(\mathbb{H})$ y consideremos en $\mathbb{H}$ la base canónica $\{1, i, j, k\}$. Sea W el subespacio de $\mathbb{H}$ generado por los vectores del conjunto $\{i, j, k\}$ (identificado con el espacio euclídeo $\mathbb{R}^3$). Demuéstrese:*

1. *Que $f(W) = W$.*
2. *Que f es una isometría del espacio euclídeo $\mathbb{R}^4$ subyacente a $\mathbb{H}$.*
3. *Que para cualesquiera $w, w' \in W$ se tiene $f(w \wedge w') = f(w) \wedge f(w')$*

Concluyase que $f|_W$ es un elemento del grupo $SO(3)$. Recíprocamente si partimos de $g \in SO(3)$, entonces la aplicación de $\mathbb{H}$ en $\mathbb{H}$ tal que $\lambda 1 + w \mapsto \lambda 1 + g(w)$ para cualesquiera $\lambda \in \mathbb{R}$, $w \in W$ es un automorfismo de $\mathbb{H}$. Conclúyase que $Aut(\mathbb{H}) \cong SO(3)$.

Problema 6 *Demuéstrese que el producto de clases de equivalencia dado en 1.1 está bien definido.*

Problema 7 *Demuéstrese la propiedad universal del álgebra cociente enunciada en este capítulo.*

Problema 8 *Supóngase que $f : A \to B$ es un epimorfismo de F-álgebras. Demuéstrese que para cada ideal $I \lhd A$ se tiene un epimorfismo de F-álgebras $A/I \to B/f(I)$ tal que $[a] \mapsto [f(a)]$ (hemos denotado las clases de equivalencia de tanto de A/I como de $B/f(I)$ del mismo modo: usando corchetes).*

Problema 9 *Demuéstrese el primer teorema de isomorfía para las F-álgebras: si $f : A \to B$ es un homomorfismo, entonces $A/\ker(f) \cong im(f)$ (imagen de f).*

Problema 10 *Demuestra que si $I, J \lhd A$ con $I \subset J$ entonces*

$$J/I \lhd A/I, \text{ y además } \frac{A/I}{J/I} \cong A/J.$$

Problema 11 *Compruébese que la involución estandar de $\mathbb{H}$ es lineal y verifica las propiedades $\overline{xy} = \bar{y}\bar{x}$ y $\bar{\bar{x}} = x$ para cualesquiera $x, y \in \mathbb{H}$.*

Problema 12 *Demuéstrese que para cada cuaternión $x \in \mathbb{H}$ se tiene $x\bar{x} \in \mathbb{R}e_0$. Justifíquese que podemos definir una aplicación llamada* norma cuaterniónica *$n : \mathbb{H} \to \mathbb{R}$ tal que $x\bar{x} = n(x)e_0$ para cada cuaternión x.*

Problema 13 *Demuéstrese que $\mathbb{H}$ es un álgebra asociativa.*

Capítulo 2

Álgebras asociativas

En este capítulo vamos a explicar en forma breve la estructura de las álgebras asociativas simples y de dimensión finita sobre un cuerpo. La técnica que se utilizará está basada en la existencia de suficientes idempotentes así como en la descomposición de Peirce y sus propiedades.

2.1. Álgebras asociativas.

Recordemos que un álgebra A (no necesariamente asociativa) se dice *simple* cuando $A^2 \neq 0$ y los únicos ideales de A son 0 y A. La teoría de estructura de las álgebras asociativas simples de dimensión finita tiene tu piedra angular en la existencia de idempotentes no nulos. Para empezar a capturar tales elementos observaremos en primer lugar que se pueden detectar idempotentes en los ideales minimales por un lado, siempre que no sean de cuadrado nulo.

Lema 1 *Sea U una K-álgebra (K un cuerpo) y J ideal derecho minimal de U. Entonces $J^2 = \{0\}$ ó existe un idempotente $e \in J$ no nulo tal que $J = eU$. (igualmente se puede demostrar para ideales a izquierda).*

Dem. Si $J^2 \neq \{0\}$, existe $b \in J$ tal que $bJ \neq \{0\}$ por tanto $J = bJ$. Sea $I := \{x \in U : bx = 0\}$, entonces I es un ideal derecho de U. Si $I \cap J \neq \{0\}$, se llega a $J \subset I$ luego $bJ = \{0\}$ una contradicción. Por tanto $I \cap J = \{0\}$, como $bJ = J$ existe $e \in J$ tal que $be = b$ (necesariamente $e \neq 0$). Entonces $be^2 = be$ luego $e^2 - e \in I \cap J$ por tanto e es un idempotente no nulo. Como $\{0\} \neq eU \subset J$ se tiene $eU = J$ por minimalidad de J. ■

Corolario 1 *En un álgebra finito-dimensional simple U (sobre un cuerpo K), cada ideal derecho no nulo posee un idempotente no nulo. (idem para ideales a izquierda).*

Dem. Sea K un ideal derecho no nulo de U. Existe un ideal derecho minimal J de U contenido en K. Veamos que $J^2 \neq \{0\}$: por ser U simple se tiene $Rann(U) := \{x \in U : Ux = \{0\}\}$ y $Lann(U) := \{x \in U : xU = \{0\}\}$ son ambos nulos, entonces no puede tenerse

$UJ = \{0\}$. Por consiguiente UJ es un ideal de U no nulo luego coincide con U. Entonces si J^2 fuese nulo se tendría $U = UJ = UJ^2 = \{0\}$ una contradicción. Ahora aplicamos el lema previo y tenemos un idempotente no nulo en J luego en K.■

Lema 2 *Sea A una K-álgebra (K un cuerpo) finito - dimensional simple y $e \in A$ un idempotente maximal (es decir que no existe otro idempotente no nulo de A, ortogonal a e). Entonces $ex = xe = x$ para todo $x \in A$, es decir A es una K-álgebra con unidad, siendo e la unidad.*

Dem. Descompongamos A en la forma $A = A_0 \oplus A_1$ donde $A_i := \{x \in A : ex = ix\}$ con $i = 0, 1$. Se tiene que A_0 es un ideal derecho de A. Hay que analizar dos casos : que $A_0 = \{0\}$ y que $A_0 \neq \{0\}$. Analicemos la posibilidad $A_0 \neq \{0\}$; como A_0 es un ideal derecho de A, tenemos un idempotente $f \neq 0$ en A_0. Por tanto $ef = 0$, descompongamos A_0 en la forma $A_0 = A_{00} \oplus A_{01}$ donde $A_{0i} := \{x \in A_0 : xe = ix\}$ $(i = 0, 1)$. Como $f \in A_0$, tenemos $f = f_{00} + f_{01}$ con $f_{0i} \in A_{0i}$. Ahora $f = f^2 = (f_{00} + f_{01})^2 = f_{00}^2 + f_{01}^2 + f_{00}f_{01} + f_{01}f_{00}$. Pero $f_{01}^2 = f_{01}ef_{01} = 0$ y por un razonamiento análogo $f_{01}f_{00} = 0$, por tanto de igualar f con f^2 se obtiene $f_{00} + f_{01} = f_{00}^2 + f_{00}f_{01}$ es decir f_{00} es un idempotente y $f_{01} = f_{00}f_{01}$. Entonces f_{00} es un idempotente ortogonal a e y por maximalidad de este, $f_{00} = 0$ pero entonces $f_{01} = 0$ lo que nos lleva a la contradicción de que $f = 0$. En consecuencia, se tiene que necesariamente $A_0 = \{0\}$ por tanto tenemos $ex = x$ para todo $x \in A$. Descomponemos $A = B_0 \oplus B_1$ con $B_i := \{x \in A : xe = ix\}$ con $i = 0, 1$. Si $B_0 \neq \{0\}$, como B_0 es un ideal a la izquierda no nulo de A, tenemos un idempotente no nulo $u \in B_0$. Se tiene entonces $eu = u$ y $ue = 0$, luego $u = u^2 = ueu = 0$, contradicción. Por tanto $B_0 = \{0\}$ y entonces $A = B_1$ es decir $xe = x$ para todo $x \in A$. ■

Definición 1 *Un idempotente no nulo e de una K-álgebra asociativa diremos que es irreducible cuando no se puede expresar como suma de idempotentes ortogonales no nulos.*

Lema 3 *Si e es un idempotente irreducible de una K-álgebra A finito-dimensional y simple, entonces el ideal derecho eA es minimal (idem para el ideal izquierdo Ae).*

Dem. Si I es un ideal a derecha no nulo de A con $I \subset eA$, tenemos un idempotente no nulo $u \in I$. Entonces $eu = u$ por pertenecer u a eA. Por otro lado $(ue)^2 = u(eu)e = ue^2 = ue$ luego ue es un idempotente. También $e - ue$ lo es ya que $(e - ue)^2 = e^2 + (ue)^2 - eue - uee = e + ue - ue - ue = e - ue$. Además ue y $e - ue$ son ortogonales : $ue(e - ue) = ue - ue = 0$, $(e - ue)ue = eue - ue = ue - ue = 0$. Como e es irreducible, $ue = 0$ ó $e = ue$. La primera posibilidad no puede darse porque $u = eu$ y $u = u^2 = eueu$, si ue fuese nulo, lo sería u. En cuanto a la segunda posibilidad, $e = ue$ implica que $e \in I$ luego $eA = I$.■

Lema 4 *Sea e un idempotente de una K-álgebra A simple. Entonces se tiene la equivalencia de las tres siguientes afirmaciones :*

a) eA es un ideal derecho minimal de A.

b) Ae es un ideal izquierdo minimal de A.

c) eAe es una K-álgebra de división (como subálgebra de A).

Dem. Demostraremos que a) es equivalente a c), y por la simetría de los razonamientos se sigue la equivalencia de b) con c). Si eA es ideal derecho minimal de A, sea exe un elemento arbitrario no nulo de eAe, vamos a demostrar que tiene inverso en eAe. Como $exeA$ es un ideal derecho de A no nulo (recordemos que $Lann(A) = \{0\}$), y $exeA \subset eA$ se tiene la igualdad $exeA = eA$, por tanto existe $y \in A$ tal que $exey = e$, luego $exeye = e$ es decir $(exe)(eye) = e$. Hemos visto que exe tiene inverso por la derecha. Como eye es no nulo, existe un $z \in A$ tal que $(eye)(eze) = e$. De aquí se sigue sin dificultad que $exe = eze$ luego exe es inversible. Supongamos ahora que eAe es una K-álgebra de división como subálgebra de A. Vamos a ver que eA es un ideal derecho minimal de A. Sea I un ideal derecho no nulo de A contenido en eA. No puede ocurrir $Ie = 0$ pues en este caso como $A = AI$ se tendría $Ae = 0$. Por tanto existe $x \in I$ tal que xe es no nulo. Como $x \in I \subset eA$ se tiene $x = ex$ luego exe es no nulo. Dado que eAe es de división, existe $y \in A$ tal que $exeye = e$, es decir $e \in exA \subset IA \subset I$ luego $eA = I$. ■

Lema 5 *Sea A una K-álgebra finito-dimensional simple (K un cuerpo), entonces la unidad 1 de A es suma de una familia ortogonal de idempotentes irreducibles.*

Dem. La unidad es un idempotente, si es irreducible, no hay nada que demostrar. En caso contrario expresemos la unidad como una suma $1 = e_1 + \ldots + e_n$ de idempotentes no nulos ortogonales dos a dos, con n máximo (la finito-dimensionalidad de A implica que n está acotado). Veamos ahora que cada idempotente e_i es irreducible. Si un idempotente dado e_i no es irreducible, $e_i = u + w$ donde u y w son idempotentes ortogonales no nulos. Entonces se tiene una familia $\{e_1, \ldots, e_{i-1}, u, w, e_{i+1}, \ldots, e_n\}$ ortogonal de idempotentes de cardinal $n + 1$ contradiciendo le carácter de máximo que tiene n.■

Teorema 2 *Sea A un álgebra finito-dimensional simple sobre un cuerpo K. Entonces existe una K-álgebra de división finito-dimensional D tal que A es isomorfa al álgebra de matrices cuadradas $\mathcal{M}_n(D)$ con coeficientes en D.*

Dem. Expresemos la unidad como suma de una familia ortogonal de idempotentes irreducibles $1 = e_1 + \ldots + e_n$. Hagamos la descomposición de Peirce de A con relación a dicha familia, es decir expresemos A en la forma

$$A = \bigoplus_{i,j=1}^{n} A_{ij}$$

donde $A_{ij} = e_i A e_j$ para cualesquiera $i, j = 1, \ldots, n$. Por los resultados anteriores sabemos que cada $e_i A e_i$ es una K-álgebra de división al ser e_i un idempotente irreducible (además $\dim_K(e_i A e_i) \leq dim_K(A) \leq \infty$). Sea x un elemento no nulo de un A_{ij}, vamos a demostrar

que existe un $y \in A_{ji}$ tal que $xy = e_i$ y $yx = e_j$. En efecto xA es un ideal derecho no nulo de A y está contenido en e_iA luego coincide con e_iA, entonces existe $z \in A$ tal que $xz = e_i$ pero $e_i = xz = xe_jz$ y multiplicando a derecha por e_i se obtiene $e_i = xe_jze_i$. Si definimos $y := e_jze_i$ tenemos un elemento de A_{ji} tal que $xy = e_i$. Para demostrar que $yx = e_j$ multipliquemos la igualdad $xy = e_i$ por x a la derecha y tenemos $xyx = e_ix = x = xe_j$ luego $x(yx - e_j) = 0$. Como $Ax = Ae_j$ resulta que $Ae_j(yx - e_j) = \{0\}$ es decir $A(yx - e_j) = \{0\}$ luego $yx - e_j \in Rann(A) = \{0\}$ es decir $yx = e_j$. A partir de lo anterior es fácil ver que la aplicación $\phi : A_{ii} \to A_{jj}$ dada por $\phi(z) := yzx$ es un isomorfismo de K-álgebras de división. En efecto se tiene por ejemplo que es homomorfismo de K-álgebras pues

$$\phi(z_1z_1) = yz_1z_2x = yz_1e_iz_2x = yz_1xyz_2x = \phi(z_1)\phi(z_2).$$

Además, si $\phi(z) = 0$ se tiene $yzx = 0$, $yzxy = 0$ por tanto $yze_i = yz = 0$ luego $xyz = 0$, es decir $e_iz = z = 0$ por tanto ϕ es un monomorfismo. Para ver que ϕ es un epimorfismo sea $t \in A_{jj}$ arbitrario, entonces $t = e_jte_j = (yx)t(yx) = y(xty)x = \phi(xty)$. Vamos ahora a fijar e_1, entonces para cada $i = 1, \ldots, n$ existe un elemento $e_{1i} \in A_{1i}$ y otro $e_{i1} \in A_{i1}$ tal que $e_{1i}e_{i1} = e_1$ y $e_{i1}e_{1i} = e_i$. Definamos ahora los elementos $e_{ij} := e_{i1}e_{1j}$ para cualesquiera i, j. Se tiene trivialmente que $e_{ii} = e_i$ para cada i. Además

$$e_{ij}e_{jk} = e_{i1}e_{1j}e_{j1}e_{1k} = e_{i1}e_{11}e_{1k} = e_{i1}e_1e_{1k} = e_{i1}e_{1k} = e_{ik}$$

para cualesquiera i, j, k. Tambien es fácil ver que si $j \neq k$ entonces $e_{ij}e_{kl} = 0$. Definamos ahora la familia de aplicaciones K-lineales $\varphi_{ij} : A_{ij} \to A_{11}$ dadas por $\varphi_{ij}(z) := e_{1i}ze_{j1}$ (con $i, j = 1, \ldots, n$). Se demuestra como antes que cada φ_{ii} es un isomorfismo de K-álgebras y que si $i \neq j$, φ_{ij} es un isomorfismo de K-espacios vectoriales. Se comprueban sin dificultad las relaciones :

$$\varphi_{ij}(x_{ik}y_{kj}) = \varphi_{ik}(x_{ik})\varphi_{kj}(y_{kj})$$

para cualesquiera i, j, k y $x_{ik} \in A_{ik}$, $y_{kj} \in A_{kj}$. Denotemos por D a A_{11} que es una K-álgebra de división y de dimensión finita como vimos antes. Por último definamos la aplicación $\varphi : A \to \mathcal{M}_n(D)$ dada por

$$\sum_{ij} x_{ij} \mapsto (\varphi_{ij}(x_{ij}))_{i,j=1}^{n}.$$

Es ahora un sencillo ejercicio el demostrar que φ es un isomorfismo de K-álgebras con unidad como queríamos demostrar. ■

2.2. Problemas

Sumas de cuatro cuadrados.

Esta relación de problemas está dedicada a las aplicaciones de los cuaterniones enteros (para ampliar conocimientos puede consultarse la referencia [1]). Sea $\mathbb{H}$ el álgebra de cuaterniones reales de división y D el conjunto de todos los cuaterniones enteros, es decir, el

conjunto formado por los $\lambda_0 + \lambda_1 i + \lambda_2 j + \lambda_3 k$ tales que o bien todos los λ_i son enteros, o bien todos ellos son de la forma $\frac{2k+1}{2}$. En los problemas sucesivos se pide demostrar que $\mathbb{Z}$ se puede considerar un subanillo de D. Supondremos pues de ahora en adelante que $\mathbb{Z}$ está contenido en D.

Problema 14 *Demuéstrese que D es un anillo no conmutativo que contiene una copia de $\mathbb{Z}$ (un subanillo isomorfo a $\mathbb{Z}$).*

Problema 15 *Demuéstrese que para cada cuaternión $q \in D$, su norma $N(q)$ es un entero. Recordemos que las 'unidades' de un anillo son por definición los elementos inversibles del mismo. Demuéstrese que $\alpha \in D$ es una unidad si y sólo si $N(\alpha) = 1$. Calcúlense explícitamente las unidades de D.*

Problema 16 *Sea $\alpha \in D$ tal que sus coordenadas respecto a la base $\{1, i, j, k\}$ no son enteras, demuéstrese que $\alpha = \beta + \gamma$ donde los coeficientes de β son pares, y $\gamma = \frac{1}{2}(\pm 1 \pm i \pm j \pm k)$. Demuéstrese que $\alpha\overline{\gamma}$ es un asociado de α que tiene coordenadas enteras.*

Problema 17 *Supóngase conocido el resultado según el cual para todo primo $p \in \mathbb{Z}$, dicho elemento nunca es primo visto como elemento de D (véase [1]). A partir de este resultado, demuéstrese que p es suma de cuatro cuadrados (se debe entender que es suma de cuatro cuadrados en $\mathbb{Z}$):*

1. *Como $p = xy$ para dos no-unidades $x, y \in D$, se tiene $p^2 = N(p) = N(x)N(y)$. Deducir que $p = N(x) = N(y)$.*

2. *Demuéstrese que en la descomposición anterior $p = xy$, alguno de los elementos x o y pueden elegirse con coordenadas enteras.*

3. *Como $p = N(x) = N(y)$ se tiene trivialmente que p es suma de cuatro cuadrados en $\mathbb{Z}$.*

4. *Demuéstrese que en $\mathbb{Z}$, todo elemento es suma de cuatro cuadrados. Para ello se puede usar la fórmula $N(xy) = N(x)N(y)$ que se puede interpretar en D diciendo que la multiplicación es operación interna en el conjunto de todas las sumas de cuatro cuadrados.*

Un plano no pappiano.

Para esta sección puede consultarse la referencia [4]. Se define un plano afín como una pareja (Π, Δ) donde Π es un conjunto cuyos elementos llamaremos 'puntos' y Δ una familia de partes de Π (a cada una de las cuales llamaremos 'recta') tales que:

1. Para cada par de puntos $P, Q \in \Pi$ distintos, existe una única recta $r \in \Delta$ tal que $P, Q \in r$.

2. Dada una recta l y un punto P que no pertenezca a l existe una única recta que pasa por P y tiene intersección vacía con l.

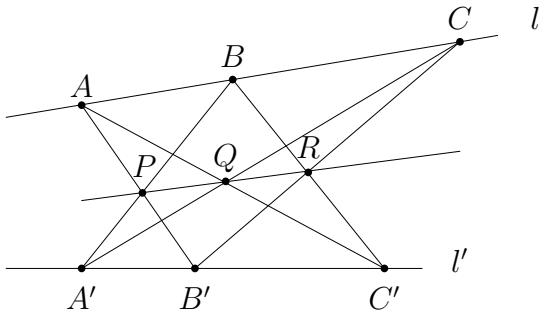
3. Existen tres puntos no alineados (es decir, no contenidos los tres en una recta).

Problema 18 *Pruébese que si D es un anillo de división, entonces definiendo $\Pi = D \times D$ y Δ como el conjunto de 'rectas'*

$$r_{abcd} := \{(x, y) \in D \times D : (x, y) = (a, b) + \lambda(c, d)\}$$

con $(a, b), (c, d) \in D \times D$,(siendo (c, d) no nulo), $\lambda \in D$, entonces la pareja (Π, Δ) es un plano afín en el sentido de la definición anterior.

Un plano afín (Π, Δ) se dice que satisface la propiedad de Pappus si dadas dos rectas $l, l' \in \Delta$ diferentes, tres puntos $A, B, C \in l - l'$, otros tres $A', B', C' \in l' - l$, entonces los puntos $P := AB' \cap A'B$, $Q = AC' \cap A'C$, y $R = BC' \cap B'C$ (en caso de existir) son colineales.



Problema 19 *Demuéstrese que el plano afín definido como en el problema anterior tomando en vez de un anillo de división, un cuerpo (por tanto conmutativo), es un plano que satisface la propiedad de Pappus.*

Problema 20 *Demuéstrese que el plano afín que se obtiene tomando $D = \mathbb{H}$ en el problema 18 es un plano afín que no satisface la propiedad de Pappus.*

Capítulo 3

Álgebras libres

En este capítulo definiremos algunos tipos de álgebras no asociativas (las más usuales e importantes: álgebras alternativas, de Lie y Jordan), y daremos un método para construir ciertos tipos de tales álgebras, que tienen determinadas propiedades universales.

3.1. Definiciones previas

Hemos introducido ya la noción de álgebra sobre un cuerpo. En realidad la restricción de considerar álgebras sobre cuerpos es innecesaria e este nivel conceptual. Podríamos definir álgebras sobre anillos conmutativos y unitarios del mismo modo: si K es un anillo conmutativo y unitario, por una *K-álgebra* entendemos un K-módulo A provisto de una aplicación (producto) $A \times A \to A$ que es bilineal en el sentido de que el producto es distributivo a derecha y a izquierda respecto a la suma, y $(ka)a' = a(ka') = k(aa')$ para cualesquiera elementos $a, a' \in A$, $k \in K$. Un tipo particular de K-álgebra se tiene cuando K es un cuerpo. En este caso A tiene una estructura subyacente de K-espacio vectorial (dado que es por definición un K-módulo). Este hecho implica la posibilidad de emplear métodos propios del álgebra lineal en la teoría de álgebras no asociativas. Nosotros nos adherimos desde este momento a ese punto de vista y trabajaremos en lo sucesivo con álgebras sobre cuerpos. Evidentemente en la definición de álgebra no se ha exigido en ningún momento el cumplimiento de la propiedad asociativa. La definición dada arriba es general y sólo en el caso particular de que se satisfaga

$$\forall a, b, c \in A, (ab)c = a(bc),$$

hablaremos de *álgebra asociativa*. Una clase algo más general de álgebras, es la dada por las *álgebras alternativas*. Éstas, son aquellas en las que se satisfacen las identidades:

$$\forall a, b \in A, a^2 b = a(ab), \qquad ba^2 = (ba)a.$$

Evidentemente toda álgebra asociativa es alternativa. Para ser coherentes con el método matemático, ahora deberíamos probar que existen álgebras alternativas no asociativas.

Esto se puede demostrar exhibiendo algún ejemplo de tales álgebras. Para ello podríamos pasar a explicar álgebras de composición hasta llegar a las álgebras de Cayley. Sin embargo retrasaremos este aspecto hasta algo más tarde ya que podemos utilizar la herramienta de las álgebras libres para exhibir los ejemplos que buscamos. Otros ejemplos de álgebras no asociativas son las álgebras de Lie que son aquellas que satisfacen las identidades:

1. $a^2 = 0$, implicando la anticonmutatividad,

2. $(ab)c + (bc)a + (ca)b = 0$, (Identidad de Jacobi),

para cualesquiera elementos $a, b, c \in A$. Toda álgebra asociativa A proporciona un ejemplo de álgebra de Lie (denotada A^-) sin más que cambiar el producto de A por el nuevo producto que vamos a denotar en forma de corchete: $A \times A \to A$ tal que $(a, a') \mapsto [a, a'] := aa' - a'a$. Este álgebra A^- se llamará en lo sucesivo, el álgebra antisimetrizada de A. Más tarde volveremos sobre esta definición ya que el proceso de antisimetrización de un álgebra no es exclusivo para las álgebras asociativas. Tendremos ocasión de aplicarlo también a las álgebras alternativas bajo ciertas condiciones especialmente provechosas. Citemos a continuación las álgebras de Jordan. Para mantenernos en un nivel elemental consideremos en todo lo que queda hasta la sección siguiente, un cuerpo K de característica distinta de dos. Diremos que una K-álgebra A es de Jordan si:

1. $ab = ba$, es decir se trata de un álgebra conmutativa, y

2. $a^2(ba) = (a^2b)a$,

para cualesquiera $a, b \in A$. Si A es un álgebra asociativa y conmutativa, entonces es de Jordan evidentemente. Otros ejemplos son las *álgebras simetrizadas* de álgebras asociativas. Así, si A es asociativa y definimos en el espacio vectorial subyacente a A el nuevo producto $a \cdot b := \frac{1}{2}(ab + ba)$, obtenemos un álgebra de Jordan denotada A^+ y llamada simetrizada de A.

3.2. Álgebras libres.

Sea K un cuerpo fijado y X un conjunto no vacío. Queremos construir una K-álgebra $\mathcal{U}(X)$ generada por X en el sentido de que los elementos de dicha álgebra sean combinaciones lineales de productos de elementos de X. Pretendemos además que exista una inyección canónica i de X en $\mathcal{U}(X)$ y que cuando tengamos una aplicación φ de X en otra K-álgebra A, se tenga automáticamente la existencia de un homomorfismo de K-álgebras $F : \mathcal{U}(X) \to A$ tal que $F \circ i = \varphi$. Intuitivamente hablando los elementos de $\mathcal{U}(X)$ son expresiones formales en los elementos del conjunto X. Podemos entender que X es un conjunto de indeterminadas y así los elementos de $\mathcal{U}(X)$ serán expresiones formales en las indeterminadas de X. Además también se podrá evaluar dichas expresiones formales en otra K-álgebra cualquiera A asignando a las indeterminadas de X valores concretos de A (esto es lo que hace la función φ). Entonces la aplicación de evaluación F que sustituye

en cualquier expresión formal de $\mathcal{U}(X)$, las indeterminadas, por los valores dados por φ, es un homomorfismo de K-álgebras. Para construir una K-álgebra con estas propiedades tenemos que definir el concepto de *palabra no asociativa* en las indeterminadas del conjunto X. Las palabras se definen en función de lo que se llama el *nivel* de las mismas. Definimos el conjunto W_1 de palabras no asociativas de nivel uno en las indeterminadas de X como el propio conjunto X. Definimos ahora el conjunto W_2 de palabras no asociativas de nivel dos como el conjunto de todas las aplicaciones $w : \{1, 2\} \to X$. Así por ejemplo si tenemos dos elementos $x_i, x_j \in X$, la aplicación tal que

$$1 \mapsto x_i, \qquad 2 \mapsto x_j$$

será denotada por $x_i x_j$, identificando la aplicación con la lista ordenada proporcionada por las imágenes. Para definir las palabras no asociativas de nivel tres tenemos que ampliar el conjunto X con dos elementos nuevos no pertenecientes a él. Podemos suponer que esos nuevos elementos son '(' y ')', es decir, apertura y cierre de paréntesis. Entonces una palabra de nivel tres es una aplicación

$$w : \{1, 2, 3, 4, 5\} \to X \cup \{(,)\}$$

tal que o bien es de la forma

$$\begin{array}{ccc} 1 & \mapsto & x_i \\ 2 & \mapsto & (\\ 3 & \mapsto & x_j \\ 4 & \mapsto & x_k \\ 5 & \mapsto &) \end{array}$$

para $x_i, x_j, x_k \in X$, o bien es de la forma

$$\begin{array}{ccc} 1 & \mapsto & (\\ 2 & \mapsto & x_i \\ 3 & \mapsto & x_j \\ 4 & \mapsto &) \\ 5 & \mapsto & x_k \end{array}$$

para $x_i, x_j, x_k \in X$. En resumen las palabras de nivel tres responden a los modelos $x_i(x_j x_k)$ o $(x_i x_j)x_k$. Supongamos entonces definidas las palabras de nivel menor que n y definamos el conjunto W_n de las palabras de nivel $n > 3$. Dichas palabras se definen como aquellas que responden a alguno de los modelos:

1. $x_i(w)$ con $w \in W_{n-1}$.

2. $(w)x_i$ con $w \in W_{n-1}$.

3. $(w)(w')$ con $w \in W_i$, $w' \in W_{n-i}$, $1 < i < n$.

Por recurrencia tenemos definidos todos los conjuntos W_n con $n \in \mathbb{N}$. Definimos entonces el conjunto de las palabras no asociativas en las indeterminadas de X como el conjunto

$$W = \cup_{n \geq 1} W_n.$$

Consideremos a continuación el K-espacio vectorial libre generado por W. Sus elementos como se sabe son las combinaciones lineales de elementos de W. Podemos denotar dicho K-espacio por $K(W)$. Vamos a definir una aplicación K-bilineal $K(W) \times K(W) \to K(W)$ de modo que tendremos dotado a $K(W)$ de una estructura de K-álgebra para el producto dado por dicha aplicación bilineal . Basta definir el producto sobre los elementos de una base de $K(W)$. En consecuencia bastaría definir el producto de los elementos de W y para ello podemos volver a emplear inducción sobre el nivel de las palabras. Por ejemplo si queremos definir el producto de dos palabras de nivel uno, a saber, x_i y x_j bastará poner (por definición)

$$x_i \cdot x_j = x_i x_j$$

resultando una palabra de nivel dos. Si ahora queremos definir el producto de una palabra de nivel uno, x_i por una w de nivel $n > 1$, bastará definir:

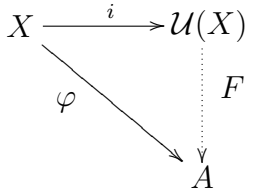
$$x_i \cdot w := x_i(w)$$

resultando una palabra de nivel $n + 1$. De forma análoga se definirá el producto de w por x_i. Por último para definir el producto de dos palabras w y w' de nivel mayor que uno bastará escribir

$$w \cdot w' := (w)(w').$$

Así dotamos a $K(W)$ de una estructura de K-álgebra, y está K-álgebra resultante vamos a denotarla por $\mathcal{U}(X)$. La llamaremos la *K-álgebra universal libre con conjunto de generadores X*. Evidentemente la aplicación $X \to \mathcal{U}(X)$ de inclusión en una inyección.

Teorema 3 Propiedad universal del álgebra no asociativa libre. *Para cualquier aplicación $\varphi : X \to A$ donde A es una K-álgebra, existe un único homomorfismo de K-álgebras $F : \mathcal{U}(X) \to A$ haciendo conmutativo el diagrama:*



Dem. Sea $w(x_1, \ldots, x_n) \in \mathcal{U}(X)$ una palabra cualquiera de nivel n. Podemos definir F por inducción sobre n. Si $n = 1$, como F debe verificar $F \circ i = \varphi$, obligatoriamente tenemos que definir $F(x_i) = \varphi(x_i)$ para todo $x_i \in X = W_1$. Para las palabras de nivel dos (todas del tipo $x_i x_j$) la definición de F es también obligatoriamente (dado su carácter de homomorfismo de álgebras) $F(x_i x_j) = \varphi(x_i)\varphi(x_j)$. Supuesto que F se ha definido para las palabras de nivel menor que n (siendo $n \geq 3$), vamos a definirla para las de nivel n. Sea pues $w \in W_n$. Entonces si

1. $w = x_i(w')$ con $w' \in W_{n-1}$, se define
   $F(w) := \varphi(x_i)F(w')$.
2. $w = (w')x_i$ con w' como antes, se define $F(w) = F(w')\varphi(x_i)$.
3. $w = (z)(z')$ siendo z y z' palabras de nivel menor que n, definiremos $F(w) = F(z)F(z')$.

Se comprueba entonces que F es el único homomorfismo de K-álgebras tal que $F \circ i = \varphi$.■

Hagamos una observación trivial en este punto: $\mathcal{U}(X)$ no es un álgebra asociativa. En efecto los elementos $x_i(x_jx_k)$ y $(x_ix_j)x_k$ son evidentemente distintos. Análogamente, éste álgebra no es alternativa ni de Lie ni Jordan. Por ejemplo $\mathcal{U}(X)$ no es conmutativa: los elementos de nivel dos x_ix_j y x_jx_i son diferentes. En consecuencia $\mathcal{U}(X)$ no es de Jordan. Tampoco se tiene $x_i^2 = 0$ toda vez que los elementos x_i^2 forman parte de la base de $\mathcal{U}(X)$ lo que les impide ser nulos. Así $\mathcal{U}(X)$ no es de Lie. Sin embargo podemos construir álgebras libres de cada una de estas clases: asociativas, alternativas, Lie y Jordan. Antes de ello tenemos que definir lo que entendemos por álgebra libre asociativa o alternativa, etc.

El lector puede comprobar sin dificultad que fijado un cuerpo K, y un conjunto no vacío, podemos definir una categoría $\mathbf{NoAss}_{X,K}$ cuyos objetos sean las parejas (A, φ) tales que A es una K-álgebra cualquiera, y

$$\varphi : X \to A$$

una aplicación arbitraria. Dados dos objetos de esta categoría (A, φ) y (A', φ'), diremos que α es un morfismo de (A, φ) en $(A'\varphi')$ para la categoría $\mathbf{NoAss}_{X,K}$, si y sólo si $\alpha : A \to A'$ es un homomorfismo de K-álgebras que hace conmutativo el diagrama

$$\begin{array}{ccc} X & \xrightarrow{\varphi} & A \\ {\scriptstyle 1_X}\downarrow & & \downarrow{\scriptstyle \alpha} \\ X & \xrightarrow[\varphi']{} & A' \end{array}$$

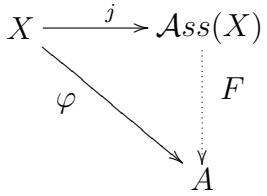
Pues bien, el lector puede comprobar sin dificultad que la propiedad universal de $\mathcal{U}(X)$ demostrada antes no es más que la afirmación de que el objeto $(\mathcal{U}(X), i)$ de $\mathbf{NoAss}_{X,K}$ es un objeto inicial en esta categoría. Como todos los objetos iniciales son únicos salvo isomorfismo, se entiende que la propiedad universal de $\mathcal{U}(X)$ implica su unicidad salvo isomorfismos.

Supongamos ahora que tenemos la intención de estudiar álgebras asociativas. Podemos considerar la subcategoría $\mathbf{Ass}_{X,K}$ de $\mathbf{NoAss}_{X,K}$ formada por aquellos objetos (A, φ) tales que A sea asociativa (los homomorfismos son los mismos). Entonces un objeto inicial para $\mathbf{Ass}_{X,K}$ (si es que existe) se llamará la K-álgebra asociativa libre con conjunto de generadores X. El hecho de poder hablar de la K-álgebra viene como siempre implicado por el hecho de que (si existe), este álgebra es única salvo isomorfismos. Vamos a denotar a nuestra K-álgebra asociativa libre por $\mathcal{A}ss(X)$. Si explicitamos las propiedades que queremos que cumpla tendremos:

1. Tener una inyección canónica $j : X \to \mathcal{A}ss(X)$.

2. La de ser una K-álgebra generada por $j(X)$.

3. La de que para cualquier aplicación $\varphi : X \to A$ siendo A una K-álgebra asociativa, exista un único homomorfismo de K-álgebras $F : \mathcal{A}ss(X) \to A$ haciendo conmutativo el triángulo:



Hay distintas maneras de construir tales álgebras asociativas $\mathcal{A}ss(X)$. Podríamos retocar nuestra construcción de $\mathcal{U}(X)$ basada en el concepto de palabra no asociativa. Para ello habría que definir las palabras de nivel uno y dos exactamente como se hizo en su momento. Pero al llegar a la definición de palabras de nivel tres, tendríamos que eliminar los paréntesis, y así una palabra de nivel tres sería cualquier aplicación $\{1, 2, 3\} \to X$ y por tanto se representarían en la forma $x_i x_j x_k$. A partir de aquí podríamos seguir definiendo las palabras de nivel superior en forma obvia. Vamos no obstante a dar una construcción del álgebra $\mathcal{A}ss(X)$ que sea más general en el sentido de que cogida la idea nos servirá para definir las álgebras alternativas, Lie o Jordan libres con conjunto de generadores X.

En el álgebra $\mathcal{U}(X)$ tomemos el ideal I generado por los elementos $(ab)c - a(bc)$ con $a, b, c \in \mathcal{U}(X)$. Definamos entonces $\mathcal{A}ss(X) := \mathcal{U}(X)/I$ y comprobemos que este álgebra satisface las propiedades 1-3 enumeradas atrás.

1. Consideremos la aplicación $j : X \to \mathcal{A}ss(X)$ definida por $j(x) = x + I$ (clase de equivalencia de x). Veamos que j es inyectiva. Si $j(x) = j(x')$ para dos elementos distintos $x, x' \in X$ entonces $x - x' \in I$ lo que implica que $x - x'$ es combinación lineal de productos tal que alguno de sus factores es del tipo $(ab)c - a(bc)$ (con $a, b, c \in \mathcal{U}(X)$). Sea $A = \mathcal{M}_n(K)$ donde $n \geq 2$. Sea $\varphi : X \to A$ tal que

   1) $\forall z \neq x, x'$, $\varphi(z) = 0$.
   2) $\varphi(x) = E_{11}$, $\varphi(x') = E_{22}$ siendo E_{ii} la matriz elemental con un 1 en la fila y columna i-ésima, y los demás coeficientes nulos.

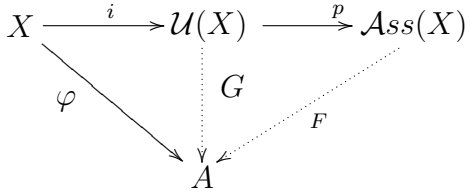
   Entonces existe un homomorfismos de K-álgebras $F : \mathcal{U}(X) \to A$ tal que $F \circ i = \varphi$. Como $x - x' \in I$ se tiene $F(x - x') = 0$ porque $x - x'$ es un producto donde alguno de los factores es del tipo $(ab)c - a(bc)$ y A es asociativa. Entonces

   $$0 = F(x - x') = F(x) - F(x') = \varphi(x) - \varphi(x') = E_{11} - E_{22}$$

   una evidente contradicción.

2. Como $\mathcal{U}(X)$ está generado por X, evidentemente $\mathcal{A}ss(X)$ está generada por $j(X)$.

3. Respecto a la propiedad universal del tercer punto de atrás, podemos demostrarla combinando dos propiedades universales:



donde en el triángulo de la izquierda, la propiedad universal de $\mathcal{U}(X)$ implica la existencia y unicidad del homomorfismo de K-álgebras G tal que $G \circ i = \varphi$. Por otra parte en el triángulo de la derecha la propiedad universal del álgebra cociente implicará la existencia del homomorfismo F siempre que podamos demostrar que el ideal I está contenido en el núcleo de G. Sin embargo esto es evidente toda vez que I está generado por productos de elementos en los que algún factor es $(ab)c - a(bc)$. Como estos elementos $(ab)c - a(bc)$ pertenecen al núcleo de G (por ser A asociativa), en definitiva, $I \subset \ker(G)$. Así se demuestra la existencia de F, la unicidad es por otra parte fácil de demostrar y la dejamos como ejercicio para el lector.

Finalmente nos queda decir que de forma totalmente análoga se construiría el álgebra alternativa libre generada por un conjunto no vacío X. Simplemente haríamos el cociente $\mathcal{U}(X)/J$ donde ahora J sería el ideal de $\mathcal{U}(X)$ generado por todos los elementos $a^2b - a(ab)$ y $ba^2 - (ba)a$ para cualesquiera $a, b \in \mathcal{U}(X)$. La propiedad universal que cumpliría este álgebra es evidente de enunciar sin más que restringir nuestra atención a álgebras alternativas. Se podría formular dicha álgebra como un objeto inicial para determinada categoría cuyos objetos fuesen las parejas (A, φ) donde A es una K-álgebra alternativa y $\varphi : X \to A$ una aplicación. El álgebra alternativa libre generada por X se suele denotar por $\mathcal{A}lt(X)$. También podrían definirse el álgebra de Lie libre con conjunto de generadores X denotada por $\mathcal{L}ie(X)$ y el álgebra de Jordan libre $\mathcal{J}or(X)$ siguiendo la filosofía descrita en esta sección.

3.3. Álgebras libres con unidad.

Finalmente dedicaremos unas líneas al estudio de las construcciones de álgebras libres con unidad.

Definición 2 *Dada una K-álgebra A definimos la* unitizada *de A (denotada A_1) como: $A_1 := A$ en caso de que A tenga unidad. En el supuesto contrario se define A_1 como el álgebra cuyo K-espacio vectorial subyacente es $A_1 := K \times A$ con la suma, el producto por escalares y el producto siguientes:*

$$\begin{aligned}
&(\alpha, a) + (\alpha', a') = (\alpha + \alpha', a + a'),\\
&\mu(\alpha, a) = (\mu\alpha, \mu a),\\
&(\alpha, a)(\alpha', a') = (\alpha\alpha', \alpha a' + \alpha' a + aa'),
\end{aligned}$$

para cualesquiera $\alpha, \alpha'\mu \in K$, $a, a' \in A$.

El lector puede comprobar que:

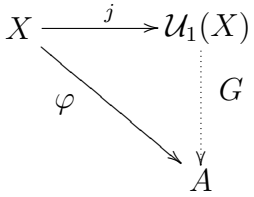
1. El elemento $(1,0)$ es la unidad de A_1 en el supuesto de que A no tenga unidad.

2. La aplicación $A \to A_1$ dada por $a \mapsto (0,a)$ es un monomorfismo de álgebras (otra vez suponiendo A no unitaria).

Resulta fácil demostrar que si $f : A \to B$ es un homomorfismo de K-álgebras (siendo A sin unidad) entonces se extiende f de forma única a un homomorfismo de K-álgebras con unidad definiendo $f_1 : A_1 \to B_1$ mediante $f_1(\alpha, a) = \alpha 1 + f(a)$. Para construir ahora el *álgebra universal libre con unidad* que denotaremos por $\mathcal{U}_1(X)$ bastará considerar entonces la unitizada del álgebra universal libre $\mathcal{U}(X)$ que es un álgebra sin unidad. Veamos que $\mathcal{U}_1(X)$ es un objeto inicial en la categoría cuyos objetos son las parejas (A, φ) donde A es una K-álgebra con unidad y $\varphi : X \to A$ una aplicación, y tal que un morfismo α de (A, φ) en (A', φ'), viene dado por un homomorfismo de K-álgebras con unidad $\alpha : A \to A'$ tal que haga conmutativo el cuadrado:

$$\begin{array}{ccc} X & \xrightarrow{\varphi} & A \\ {\scriptstyle 1_X}\downarrow & & \downarrow{\scriptstyle \alpha} \\ X & \xrightarrow[\varphi']{} & A' \end{array}$$

Esto es equivalente a demostrar la propiedad universal del álgebra libre con unidad $\mathcal{U}_1(X)$ que dice que si denotamos por $j : X \to \mathcal{U}_1(X)$ la inyección canónica composición de las inyecciones $i : X \to \mathcal{U}(x)$, y $\mathcal{U}(X) \to \mathcal{U}_1(X)$ (tal que $z \mapsto (0,z)$), entonces para cada aplicación $\varphi : X \to A$ donde A es una K-álgebra con unidad, existe un único homomorfismo G de álgebras con unidad $G : \mathcal{U}_1(X) \to A$ haciendo conmutativo el triángulo:



La demostración se apoya en la propiedad universal de $\mathcal{U}(X)$ que nos proporcionará un homomorfismo de K-álgebras de $\mathcal{U}(X) \to A$ y después extenderemos este a las unitizadas de ambas álgebras para conseguir $G : \mathcal{U}_1(X) \to A_1 = A$.

Naturalmente siguiendo la lógica de la sección precedente podemos ahora definir las álgebras asociativas, alternativas, o Jordan libres con unidad. Una de las tareas a investigar es ¿qué tipo de indentidades pasan de un álgebra sin unidad A a su unitizada? Por ejemplo el lector puede comprobar que si A es asociativa, alternativa o de Jordan, entonces A_1 lo es. Las propiedades universales que deben satisfacer estas álgebras libres deben resultar evidentes para el lector y no insistiremos más en el tema. Quizás convenga, eso si, decir que usaremos las notaciones $\mathcal{A}ss_1(X)$, $\mathcal{A}lt_1(X)$, y $\mathcal{J}or(X)$.

3.4. Problemas

Problema 21 *Compruébese que si un álgebra A es asociativa, alternativa o Jordan, entonces su unitazada A_1 lo es. ¿Qué problema hay con las álgebras de Lie?*

Problema 22 *Formalícense las definiciones de álgebra asociativa (alternativa o de Jordan) libre con unidad.*

Problema 23 *Demuéstrese que el álgebra de cuaterniones reales de división $\mathbb{H}$ es un cociente del álgebra asociativa libre con unidad, generada por un conjunto X de cardinal dos. Descríbase el ideal I tal que $\mathbb{H} \cong \mathcal{A}ss_1(X)/I$.*

Indicación. Un sistema de generadores de $\mathbb{H}$ como álgebra sobre los reales es el conjunto $\{i, j\}$. Consideremos entonces el conjunto $X = \{x, y\}$ y la aplicación $\varphi : X \to \mathbb{H}$ tal que $x \mapsto i$, $y \mapsto j$. La propiedad universal del álgebra asociativa libre con unidad nos proporciona la existencia de un único homomorfismo de $\mathbb{R}$-álgebras $F : \mathcal{A}ss_1(X) \to \mathbb{H}$ tal que $F(x) = i$, $F(y) = j$. El lector deberá demostrar que F es un epimorfismo. En consecuencia $\mathbb{H} \cong \mathcal{A}ss_1(X)/I$ donde $I := \ker(F)$. Entre los elementos de I obviamente figuran las palabras x^2+1, y^2+1, $xy+yx$ de $\mathcal{A}ss_1(X)$. El lector deberá demostrar que de hecho I es el ideal generado por estos tres elementos. Para ello podemos definir en principio I' como el ideal generado por esos tres elementos

$$I' =< x^2 + 1, y^2 + 1, xy + yx > .$$

Obviamente $I' \subset I$. Para demostrar la igualdad observaremos que I no contiene palabras en x e y de nivel uno (es decir, elementos del tipo $\alpha x + \beta y$ con $\alpha, \beta \in \mathbb{R}$). Sea entonces $w(x, y) = \alpha x^2 + \beta y^2 + \gamma xy + \delta yx$ un elemento de nivel dos de I (como siempre las letras griegas representan escalares) . Demostraremos que $w(x, y) \in I'$ del siguiente modo: dado que

$$0 = F(w(x, y)) = \alpha i^2 + \beta j^2 + \gamma ij + \delta ji = -(\alpha + \beta) + (\gamma - \delta)k$$

tendremos $\alpha = -\beta$, $\gamma = \delta$. Por tanto

$$w(x, y) = \alpha(x^2 - y^2) + \delta(xy + yx) = \alpha[(x^2 + 1) - (y^2 + 1)] + \delta(xy + yx) \in I'.$$

Finalmente supóngase que todas las palabras de nivel menor que n de I están en I' y demuéstrese para las de nivel n.

Problema 24 *Considerando $\mathbb{H}$ como el álgebra $\mathbb{H} = \mathcal{A}ss(X)/I$ del problema anterior, demuéstrese la existencia de una única involución de $\mathbb{H}$ tal que $x \mapsto \overline{x} = -x$ y $y \mapsto \overline{y} = -y$. Compruébese que esta involución satisface las condiciones $x + \overline{x}, x\overline{x} \in \mathbb{R}1$ para todo $x \in \mathbb{H}$ y que definiendo la aplicación $n : \mathbb{H} \to \mathbb{R}$ como $n(x) := x\overline{x}$, la aplicación n es una forma cuadrática que admite composición en el sentido de que es multiplicativa: $n(xy) = n(x)n(y)$, $\forall x, y \in \mathbb{H}$.*

Problema 25 *Sea ϵ_{ijk} (con $i,j,k \in \overline{3} := \{1,2,3\}$) el tensor totalmente antisimétrico de orden tres tal que $\epsilon_{123} = 1$. Esto quiere decir que ϵ es una aplicación $\epsilon : \overline{3} \times \overline{3} \times \overline{3} \to \mathbb{R}$ tal que la imagen de la terna (i,j,k) por ϵ se denota por $\epsilon_{ijk} \in \mathbb{R}$. El hecho de que ϵ_{ijk} es totalmente antisimétrico quiere decir que $\epsilon_{ijk} = -\epsilon_{jik} = -\epsilon_{kji} = -\epsilon_{ikj}$ (lo que implica que $\epsilon_{iij} = \epsilon_{jii} = \epsilon_{iji} = 0$). Compruébese que el álgebra $\mathbb{H}$ tiene una base $\{e_0, e_1, e_2, e_3\}$ con respecto a la cual, el producto viene dado por la relaciones $e_0 e_i = e_i e_0 = e_i$, para todo i, y $e_i e_j = -\delta_{ij} e_0 + \sum_{k=1}^{3} \epsilon_{ijk} e_k$ donde $i,j \neq 0$, y δ_{ij} es la delta de Kronecker ($\delta_{ii} = 1$ y $\delta_{ij} = 0$ si $i \neq j$).*

Problema 26 *Sea F un cuerpo cualquiera y X un conjunto de cardinal dos $X = \{x, y\}$. Consideremos la F-álgebra libre $\mathcal{A}ss(X)$ y definamos $A := \mathcal{A}ss(X)/I$ donde I es el ideal generado por los elementos x^2+1, y^2-1 y $xy+yx$. Demuéstrese que las clases de equivalencia de los elementos del conjunto $\{1, x, y, xy\}$ son una base de A. Encuéntrese la tabla de multiplicar de A con relación a la base anterior. Demuestrése que A es isomorfa al álgebra $\mathcal{M}_2(F)$ de la matrices 2×2 con coeficientes en F. Este álgebra se llama también al álgebra de los cuaterniones split sobre F y se suele denotar por $\mathbb{H}_s(F)$ (en el caso de que $F = \mathbb{R}$ usaremos la notación $\mathbb{H}_s$ simplemente). Compruébese que existe una involución en A (denotada por $x \mapsto \overline{x}$ tal que $x + \overline{x}, x\overline{x} \in A$,1 para todo $x \in A$. Compruébese que definiendo $n : A \to F$ por $n(x) := x\overline{x}$ se obtiene una forma cuadrática que* admite composición *(es decir, que es multiplicativa en el sentido de que $n(xy) = n(x)n(y)$ para todos $x, y \in A$).*

Problema 27 *Sea A un álgebra alternativa.*

1. *Si dos elementos $a, b \in A$ verifican $ab = -ba$, demuéstrese que entonces $(xa)b + (xb)a = 0$ para todo x. demuéstrese también que $a(bx) + b(ax) = 0$ para todo x.*

2. *Sea A como arriba y sean $x, y, z \in A$ tales que anticonmutan de dos en dos y z anticonmuta con xy. Demuéstrese que entonces x anticonmuta con yz y que y anticonmuta con xz.*

Solución. Para este problema, se autoriza al alumno a utilizar los siguientes hechos que demostraremos en el capítulo siguiente:

1. En un álgebra alternativa, el asociador (x, y, z) de tres elementos (definido por la igualdad $(x, y, z) := (xy)z - x(yz)$) es función alternada de sus argumentos. En particular un álgebra alternativa es flexible: $(xy)x = x(yx)$, $\forall x, y$.

2. En un álgebra alternativa se verifican las identidades de Moufang: $(xax)y = x(a(xy))$, $y(xax) = ((yx)a)x$, y $(xy)(ax) = x(ya)x$, $\forall x, y, a$.

Entonces la primera parte del problema se podría atacar del siguiente modo: $(xa)b+(xb)a = (x, a, b) + x(ab) + (x, b, a) + x(ba) = (x, a, b) - (x, a, b) + x(ab + ba) = 0$ y del mismo modo se obtiene la otra igualdad. Para la segunda parte hay que tener en cuenta que $x(zy) + z(xy) = 0$ de donde

$$z(xy) = -x(zy). \tag{3.1}$$

Por otra parte como

$$(xy)z + (xz)y = 0 \tag{3.2}$$

y

$$(yx)z + (yz)x = 0, \tag{3.3}$$

de esta última igualdad obtenemos $(yx)z = -(yz)x$ o bien $z(xy) = -(yz)x$ que junto con la identidad (3.1) nos da $x(zy) = (yz)x$ o lo que es lo mismo $x(zy) = -(zy)x$. Hemos demostrado pues, que x anticonmuta con zy. Para acabar, como lo papeles que juegan x e y son simétricos, intecambiando dichos elementos se tiene que y conmuta con zx.

Problema 28 *Consideremos la $\mathbb{R}$-álgebra $\mathbb{O}$ provista de una base $\{e_i\}_{i=0}^7$ en la que e_0 es la unidad del álgebra, y los elementos básicos e_i con $i \geq 1$ multiplican conforme a las reglas:*

$$e_i e_j = -\delta_{ij} e_0 + \sum_{k=1}^{7} \epsilon_{ijk} e_k$$

donde ϵ_{ijk} es el tensor totalmente antisimétrico[1] *$\epsilon : \overline{7} \times \overline{7} \times \overline{7} \to \mathbb{R}$ que vale la unidad para las siguiente ternas:*

$$(1,2,3), \quad (1,4,5), \quad (2,4,6), \quad (3,4,7), \quad (2,5,7), \quad (1,7,6), \quad (3,6,5)\,,$$

y es nulo en los demás casos. Demuéstrese que este álgebra es alternativa pero no asociativa. Compruébese que esta provista de una involución que (necesariamente) fija a e_0 mientras que cambia el signo de los demás elementos básicos. Si denotamos por $x \mapsto \bar{x}$ a dicha involución, compruébese que la aplicación $n : \mathbb{O} \to \mathbb{R}$ tal que $n(x) := x\bar{x}$ es una forma cuadrática definida positiva y multiplicativa en el sentido de que $n(xy) = n(x)n(y)$ para cualesquiera $x, y \in \mathbb{O}$. Conclúyase que $\mathbb{O}$ es un álgebra de división.

Problema 29 (Construcción libre del álgebra de octoniones reales de división). *Consideremos el conjunto $X = \{x, y, z\}$, así como la $\mathbb{R}$-álgebra alternativa libre con unidad generada por X (denotada $\mathcal{A}lt_1(X)$). Consideremos el ideal I de $\mathcal{A}lt_1(X)$ generado por los elementos $x^2 + 1$, $y^2 + 1$, $z^2 + 1$, $xy + yx$, $xz + xz$, $yz + zy$, y $(xy)z + z(xy)$. Demuéstrese que $\mathbb{O} \cong \mathcal{A}lt_1(X)/I$.*

Indicación. Consideremos la aplicación $\varphi : X \to \mathcal{A}lt_1(X)^{\mathrm{op}}$ tal que $\varphi(x) = -x$, $\varphi(y) = -y$ y $\varphi(z) = -z$. La propiedad universal de $\mathcal{A}lt_1(X)$ implica la existencia de un homomorfismo de álgebras $\sigma : \mathcal{A}lt_1(X) \to \mathcal{A}lt_1(X)^{\mathrm{op}}$ tal que $\sigma(x) = -x$, $\sigma(y) = -y$ y $\sigma(z) = -z$. Es fácil comprobar que los elementos generadores del ideal I quedan fijos por σ. Por lo tanto se induce un homomorfismo de álgebras $\tau : \mathcal{A}lt_1(X)/I \to (\mathcal{A}lt_1(X)/I)^{\mathrm{op}}$ que cambia el signo a cada una de las clases de equivalencia $\overline{x} := x + I$, $\overline{y} := y + I$ y $\overline{z} := z + I$. Para simplificar la notación sea $A = \mathcal{A}lt_1(X)/I$ el álgebra que estamos considerando. La aplicación $\tau : A \to A$ es lo que se llama una involución del álgebra A (es lineal y verifica

[1] El conjunto $\overline{7}$ no es más que $\overline{7} = \{1, \ldots, 7\}$.

$\tau^2 = 1_A$, $\tau(xy) = \tau(y)\tau(x)$, $\forall x, y \in A$. Definamos ahora la aplicación $* : A \times A \to A$ tal que $x * y := \frac{1}{2}(x\tau(y) + y\tau(x))$. Es fácil comprobar que las clases de equivalencia de los elementos del conjunto $B = \{1, x, y, xy, z, zx, zy, z(xy)\}$ son dos a dos ortogonales (con relación a $*$), y que $\overline{b} * \overline{b} = 1$ para todo $b \in B$. Ahora la comprobación de que las clases de equivalencia de los elementos de B forman un conjunto linealmente independiente se deja al lector. Para ver dicho conjunto es un sistema de generadores hay que demostrar que todo elemento de $\mathcal{A}lt_1(X)$ es combinación lineal de los elementos de B módulo I. Empecemos por las palabras de nivel dos en x, y, z (para las de nivel 1 el asunto es trivial). Así por ejemplo

$x^2 = -1 + (x^2 + 1) \in -1 + I$ (análogo para y^2, z^2).

$xy = t$, $yx = -t + (xy + yx) \in -t + I$.

$xz = -u + (zx + xz) \in -u + I$, $zx = u$.

$yz = -v + (zy + yz) \in -v + I$, $zy = v$.

Por lo tanto todos los elementos de $\mathcal{A}lt_1(X)$ que son suma de palabras de nivel a los sumo dos, se expresan (módulo I) como combinaciones lineales de los elementos indicados. Invitamos al lector a suponer que todas las palabras de nivel menor que n son (módulo I) combinaciones lineales de los elementos del conjunto $\{1, x, y, t, z, u, v, w\}$, y a demostrar que entonces toda palabra de nivel n también lo es. Finalmente, dejamos al lector la nada trivial tarea de construir la tabla de multiplicar de este álgebra. Para allanar un poco el camino a la construcción de la mencionada tabla vamos a recorrer una parte del camino. Por ejemplo, como consecuencia de la definición de I se tiene $(xy)z = -z(xy)$ módulo I. Aplicando lo demostrado en el problema 27 sabemos que y también anticonmuta con xz módulo I y que x anticonmuta con yz (siempre módulo I). A continuación mostramos la tabla donde se ha suprimido la fila y columna de la unidad y donde los productos deben entenderse en módulo I:

$\cdot$	x	y	xy	z	zx	zy	$z(xy)$
x	-1	xy	$-y$	$-zx$	z	$-z(xy)$	zy
y		-1	x	$-zy$	$z(xy)$	z	$-zx$
xy			-1	$-z(xy)$	yz	zx	z
z				-1	$-x$	$-y$	$-xy$
zx					-1	$-xy$	y
zy						-1	$-x$
$z(xy)$							-1

Problema 30 (Construcción del álgebra de octoniones split). *Sea F un cuerpo de característica distinta de dos y consideremos el conjunto $X = \{x, y, z\}$, así como la F-álgebra alternativa libre con unidad generada por X (denotada $\mathcal{A}lt_1(X)$). Consideremos el ideal I de $\mathcal{A}lt_1(X)$ generado por los elementos $x^2 + 1$, $y^2 + 1$, $z^2 - 1$, $xy + yx$, $xz + xz$, $yz + zy$, y*

$(xy)z+z(xy)$. Demuéstrese que $\mathbb{O}_s := \mathcal{A}lt_1(X)/I$ tiene dimensión ocho y complétese la tabla de multiplicar de este álgebra (defínase $t := xy$, $u := zx$, $v = zy$, $w = zt$ y compruébese que las clases de equivalencia de los elementos del conjunto $B = \{1, x, y, t, z, u, v, w\}$ son una base cuya tabla de multiplicar se pide calcular). El álgebra $\mathbb{O}_s$ se llama álgebra de octoniones split sobre el cuerpo F.

Sugerencia: utilizar el álgebra de matrices de Zorn para este problema.

Problema 31 *Demuéstrese que en $\mathbb{O}_s$, los elementos $e_1 = \frac{1}{2}(1 - z)$ y $e_2 = \frac{1}{2}(1 + z)$ son idempotentes ortogonales (es decir, $e_i^2 = e_i$ para todo $i = 1, 2$, y $e_i e_j = 0$ para $i \neq j$). Compruébese que $\mathbb{O}_s = Fe_1 \oplus Fe_2 \oplus U \oplus V$ donde U y V son subespacios de dimensión tres tales que:*

1. *$e_2 x = x$, y $xe_1 = 0$, para todo $x \in U$.*
2. *$e_2 x = 0$ y $xe_1 = x$, para todo $x \in V$.*
3. *$x^2 = y^2 = 0$ para cualesquiera $x \in U$, $y \in V$.*
4. *$UU \subset V$, $VV \subset U$.*
5. *$UV \subset Fe_1$ y $VU \subset Fe_2$.*

Problema 32 *Sea $B = \{e_i\}_{i=1}^n$ la base canónica del espacio $\mathbb{R}^n$ y denotemos por $\langle x, y\rangle$ el producto escalar euclídeo de $x, y \in \mathbb{R}^n$. Se define el álgebra de* Clifford $\mathrm{CL}(n)$ *como el cociente de la $\mathbb{R}$-álgebra asociativa libre con unidad $\mathcal{A}ss_1(B)$ por el ideal I generado por los elementos $e_i e_j + e_j e_i + 2\langle e_i, e_j\rangle$. Denotemos por $\bar{x}$ la clase de equivalencia del elemento $x \in \mathcal{A}ss_1(B)$ en el cociente $\mathrm{CL}(n) = \mathcal{A}ss_1(B)/I$. Demuéstrese que:*

1. *$\forall \bar{x} \in \mathrm{CL}(n)$ se tiene $\bar{x}^2 = -\|x\|^2 \cdot \bar{1}$.*
2. *$\forall \bar{x}, \bar{y} \in \mathrm{CL}(n)$ se tiene $\bar{x}\bar{y} + \bar{y}\bar{x} = -2\langle x, y\rangle \cdot \bar{1}$.*

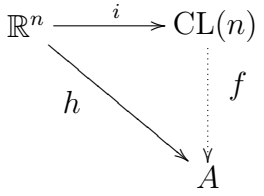
Problema 33 *En la situación del problema anterior, demuéstrese que $\dim(\mathrm{CL}(n)) \leq 2^n$ comprobando que el siguiente conjunto de productos es un sistema de generadores de $\mathrm{CL}(n)$:*

$$\overline{e_{i_1}} \cdots \overline{e_{i_k}},$$

donde $i_1 < \cdots < i_k$, y $1 \leq k \leq n$.

Problema 34 *Demuéstrese que $\mathrm{CL}(0) \cong \mathbb{R}$, $\mathrm{CL}(1) \cong \mathbb{C}$ y que $\mathrm{CL}(2) \cong \mathbb{H}$. Estúdiese $\mathrm{CL}(3)$ (encuentre su tabla de multiplicar y analícese la simplicidad de este álgebra. Si es posible encontrar un álgebra conocida a la que $\mathrm{CL}(3)$ sea isomorfa).*

Problema 35 *Consideremos la aplicación lineal* $i : \mathbb{R}^n \to \mathrm{CL}(n)$ *tal que* $i(e_j) := \overline{e_j}$ *para cada* $j = 1, \ldots, n$. *Compruébese que para cada* $x \in \mathbb{R}^n$ *se tiene* $i(x)^2 = -\|x\|^2\overline{1}$. *Desmuéstrese que* $\mathrm{CL}(n)$ *tiene la siguiente propiedad universal: sea* A *otra* $\mathbb{R}$*-álgebra asociativa con unidad, y* h *una aplicación lineal* $h : \mathbb{R}^n \to A$ *verificando* $h(x)^2 = -\|x\|^2 1$ *para cada* $x \in \mathbb{R}^n$. *Entonces existe un único homomorfismo de álgebras con unidad* $f : \mathrm{CL}(n) \to A$ *haciendo conmutativo el triángulo:*



Problema 36 *Comprueba que la aplicación lineal* $i : \mathbb{R}^n \to \mathrm{CL}(n)$ *definida en el problema anterior es un monomorfismo. (*Sugerencia: demuéstrese que existe un endomorfismo $\theta_1 : \mathrm{CL}(n) \to \mathrm{CL}(n)$ tal que $\theta_1(\overline{e_1}) = \overline{e_1}$ mientras que $\theta_1(\overline{e_j}) = 0$ para todo $j > 1$.*)*

Problema 37 *Demuéstrese que existe un homomorfismo de* $\mathbb{R}$*- álgebras* $\theta : \mathrm{CL}(n) \to \mathrm{CL}(n-1)$ *tal que* $\theta(\overline{e_i}) = \overline{e_i}$ *para* $i < n$ *y* $\theta(\overline{e_n}) = 0$. *Utilizando este hecho demuéstrese inductivamente que el sistema de generadores de* $\mathrm{CL}(n)$ *introducido en el problema 33, es en realidad una base del álgebra. Conclúyase que* $\dim(\mathrm{CL}(n)) = 2^n$.

Capítulo 4

Álgebras alternativas

4.1. Definiciones preliminares

Para un álgebra A sobre un cuerpo F, llamaremos $\mathfrak{s}$lasociador a la aplicación trilineal $A \times A \times A \to A$ tal que a cada terna (x, y, z) de elementos le asocia el nuevo elemento $(xy)z - x(yz)$. Denotaremos la imagen de la aplicación 'asociador' en la forma (x, y, z). Dicho en otras palabras

$$(x, y, z) := (xy)z - x(yz),\ \forall x, y, z \in A.$$

Tendremos también ocasión de utilizar los operadores de multiplicación por la derecha y por la izquierda definidos para cada $x \in A$ mediante las aplicaciones $L_x, R_x : A \to A$ tales que $L_x(y) := xy$, $R_x(y) := yx$ para cada $y \in A$.

Definición 3 *Sea F un cuerpo y A una F-álgebra , diremos que A es alternativa cuando toda pareja de elementos $x, y \in A$ satisfacen las identidades*

$$x^2(xy) = x(xy), \qquad (yx)x = yx^2.$$

Estas identidades reciben el nombre de identidades alternativas. Resulta obvio a partir de la definición que el álgebra opuesta de un álgebra alternativa es también un álgebra alternativa. Las identidades alternativas se pueden expresar en términos de asociadores así:

$$(x, x, y) = 0 = (y, x, x)$$

y en términos de operadores de multiplicación de esta otra forma:

$$L_{x^2} = L_x^2,\ R_{x^2} = R_x^2.$$

Proposición 1 *En un álgebra alternativa, el asociador es una función alternante de sus argumentos dicho en otras palabras*

$$(x, y, z) = -(y, x, z), (x, y, z) = -(x, z, y), (x, y, z) = -(z, y, x)$$

para cualesquiera $x, y, z \in A$.

Dem. Como $(x+y, x+y, z) = 0$ para cualesquiera $x, y, z \in A$, se tendrá: $(x, y, z)+(y, x, z) = 0$ y hemos demostrado que el asociador es función alternante de sus dos primeros argumentos. Pasando al álgebra opuesta se tendrá que es función alternante de los argumentos segundo y tercero. Entonces $(x, y, z) = -(y, x, z) = (y, z, x) = -(z, y, x)$ lo que demuestra que el asociador es también función alternante de los argumentos primero y tercero.■

Definición 4 *Diremos que un álgebra A es 'flexible' cuando cualquier pareja de elementos $x, y \in A$ satisface la identidad*

$$(xy)x = x(yx).$$

Corolario 2 *Cada álgebra alternativa es 'flexible'.*

Dem. La identidad 'flexible' es equivalente a la igualdad $(x, y, x) = 0$ pero $(x, y, x) = -(x, x, y) = 0$ en un álgebra alternativa. ■

Teorema 4 *En un álgebra alternativa A se satisfacen las identidades de Moufang*

$$(xax)y = x(a(xy)), \tag{4.1}$$

$$y(xax) = ((yx)a)x, \tag{4.2}$$

$$(xy)(ax) = x(ya)x \tag{4.3}$$

para cualesquiera $x, y, a \in A$.

Dem.

$$\begin{aligned}(xax)y - x(a(xy)) &= (xa, x, y) + (x, a, xy) = -(x, xa, y) - (x, xy, a) = \\ &= -(x(xa))y + x((xa)y) - (x(xy))a + x((xy)a) = \\ &= -(x^2a)y - (x^2y)a + x[(xa)y + (xy)a] = \\ &= -(x^2, a, y) - x^2(ay) - (x^2, y, a) - x^2(ya) + x[(xa)y + (xy)a] = \\ &= -x^2(ay) - x^2(ya) + x[(xa)y + (xy)a] = \\ &= x[-x(ay) - x(ya) + (xa)y + (xy)a] = x[(x, a, y) + (x, y, a)] = 0.\end{aligned}$$

Pasando al álgebra opuesta se demuestra la segunda igualdad. Para demostrar la tercera hagamos:

$$\begin{aligned}(xy)(ax) - x(ya)x &= (x, y, ax) + x(y(ax)) - x(ya)x = \\ &= (x, y, ax) - x(y, a, x) = \\ &= -(x, ax, y) - x(y, a, x) = \\ &= -(xax)y + x((ax)y) - x(y, a, x) = \\ &= -(xax)y + x[(ax)y - (y, a, x)] = -x(a(xy)) + x[(ax)y - (y, a, x)] = \\ &= -x[a(xy) - (ax)y + (y, a, x)] = -x[-(a, x, y) + (y, a, x)] = 0\end{aligned}$$

lo que completa la demostración.■

La identidad de Moufang 4.2 se puede escribir en la forma

$$(y, xa, x) = -(y, x, a)x \tag{4.4}$$

ya que $(y, xa, x) = (y(xa))x - y(xax) = (y(xa))x - ((yx)a)x = -(y, x, a)x$. Linealizando esta última se tiene

$$(y, xa, z) + (y, za, x) = -(y, x, a)z - (y, z, a)x \tag{4.5}$$

para cualesquiera elementos $x, y, z, a \in A$.

Teorema 5 (Artin) *En un álgebra alternativa, la subálgebra generada por cualesquiera dos elementos es asociativa.*

Dem. Sea A un álgebra alternativa y $x, y \in A$. La subálgebra generada por x e y está formada por las sumas de elementos del tipo $p(x, y)$ donde $p(x, y)$ denota un producto donde cada factor es x o y, con una determinada distribución de paréntesis. Llamaremos 'grado' de $p(x, y)$ el número de factores que aparecen en $p(x, y)$. Por ejemplo, si $p(x, y) = x^2((yx)x)$, entonces el grado de $p(x, y)$ es 5 (este hecho lo denotaremos escribiendo $\partial p(x, y) = 5$). Para demostrar que la subálgebra generada por x e y es asociativa, veremos que $(p, q, r) = 0$ siendo $p = p(x, y)$, $q = q(x, y)$, $r = r(x, y)$ tres productos genéricos de la citada subálgebra. Vamos a demostrar este hecho por inducción sobre el número $\partial p + \partial q + \partial r$. El valor más pequeño que este número puede tomar es 3. En este caso se tiene trivialmente $(x, x, x) = (y, y, y) = 0$, $(x, x, y) = 0$, $(y, y, x) = 0$ y el resto de las posibilidades ya están contempladas entre alguna de estas por el carácter alternante del asociador. Supongamos entonces que la asociatividad se tiene siempre que $\partial p + \partial q + \partial r$ sea menor que n. Vamos a demostrar entonces que $(p, q, r) = 0$ cuando $\partial p + \partial q + \partial r = n > 3$.

Analicemos los siguientes casos:

1. Sólo uno de los tres productos tiene grado mayor que uno. Supongamos que $q = xq'$ con $\partial q' = \partial q - 1$. Entonces (p, q, r) es igual a alguno de los siguientes:

   (a) $(x, xq', x) = -(x, x, xq') = 0$.

   (b) $(x, xq', y) = -(y, xq', x) = (y, x, q')x = 0$ por hipótesis de inducción y usando 4.4.

   (c) $(y, xq', y) = -(y, y, xq') = 0$.

2. Al menos dos de los tres productos tienen grado mayor que uno. En este caso dos de los tres productos p, q y r deben empezar por el mismo elementos (pongamos x). Supongamos pues que q y r empiezan por x, del tal modo que $q = xq'$, $r = xr'$ con $\partial q' = \partial q - 1$, $\partial r' = \partial r - 1$. Se tiene entonces $(p, q, r) = (p, xq', xr') = -(xr', xq', p)$ y aplicando 4.5 para $y = xr'$, $a = q'$, $z = p$, tendremos

$$-(xr', xq', p) = (xr', pq', x) + (xr', x, q')p + (xr', p, q')x =$$

$$= -(pq', xr', x) = (pq', x, r')x = 0$$

donde para la penúltima desigualdad se ha utilizado la identidad 4.4 y además la hipótesis de inducción nos ha permitido igualar a cero los asociadores cuyo grado es inferior a n. Señalemos por fin que si q empieza por x y r empieza por y, en este caso si $\partial p > 1$ y p empieza por ejemplo por x, podemos razonar como antes a partir de p y q. Si $p = x$ ó $p = y$ podemos aplicar la identidad 4.4 para obtener $(p, q, r) = 0$.

■

4.2. Descomposición de Peirce

Para una álgebra asociativa finito-dimensional y simple, se demostró en el capítulo precedente que cada ideal por la derecha (resp. izquierda) no nulo, posee un idempotente no nulo. En realidad este resultado puede generalizarse a un ambiente mucho más general con muy poco esfuerzo adicional. Supongamos que A es una F-álgebra asociativa de dimensión finita y que no es una nilálgebra (es decir, algún elemento de A no es nilpotente). Veremos que en este caso A posee un idempotente no nulo. En efecto, podemos razonar por inducción sobre la dimensión de A. Si $\dim(A) = 1$, entonces $A = Fx$ con $x^2 = \lambda x$ y λ no nulo. Definamos $e := \lambda^{-1}x$, entonces $e^2 = \lambda^{-2}x^2 = \lambda^{-2}\lambda x = \lambda^{-1}x = e$. En consecuencia A tiene un idempotente no nulo. Supongamos ahora que la propiedad es cierta para las álgebras de dimensión menor que n que no sean nilálgebras. Sea entonces A un álgebra con $\dim(A) = n$ y admitamos que A no es una nilálgebra. Sea $x \in A$ un elemento no nilpotente. Consideremos el ideal por la derecha xA (respectivamente el ideal por la izquierda Ax). Estos ideales son subálgebras y no son nilálgebras ($x^2 \in xA$ luego si xA fuera una nilálgebra, x^2 sería nilpotente y entonces x lo sería en contra de la suposición que estamos haciendo). Si alguno de los ideales laterales xA o Ax está contenido estrictamente en A, ese ideal contendrá entonces un idempotente no nulo por hipótesis de inducción. Supongamos pues $A = xA = Ax$. Entonces los operadores de multiplicación L_x y R_x son inversibles. Sean $u, u' \in A$ tales que $xu = x$, $u'x = x$. En ese caso $L_xL_u = L_x$, $L_{u'}L_x = L_x$ lo que implica $L_u = L_{u'} = \mathrm{Id}$. De forma análoga se deduce que $R_u = R_{u'} = \mathrm{Id}$. Por tanto $u' = L_u(u') = R_{u'}(u) = u$. Esto implica $L_u = R_u = \mathrm{Id}$ luego A tiene a u como unidad y por tanto como idempotente.

Proposición 2 *Sea A un álgebra alternativa de dimensión finita y supongamos que A no es una nilálgebra. Entonces A contiene un idempotente no nulo.*

Dem. Sea $x \in A$ un elemento no nilpotente. Consideremos la subálgebra de A generada por x. Esta subálgebra es asociativa de dimensión finita y contiene a x que no es nilpotente. Por tanto contiene un idempotente no nulo y en consecuencia A también.■

Una vez que tenemos resuelta la existencia de idempotentes en álgebras alternativas de dimensión finita que no sean nilálgebras, pasamos a demostrar la posibilidad de hacer la descomposición de Peirce. Para ello vamos a utilizar resultados elementales de álgebra lineal.

Proposición 3 *Sea f un endomorfismo idempotente de un F-espacio vectorial V (es decir, lo que se llama una proyección de V). Entonces $V = V_0 \oplus V_1$ donde*

$$V_0 = \ker(f) = \{x \in V : f(x) = 0\},$$

$$V_1 = \ker(f - Id) = \{x \in V : f(x) = x\}.$$

Dem. Todo elemento $x \in V$ se puede escribir en la forma $x = f(x) + (x - f(x))$ donde $f(x) \in V_1$ pues $f(f(x) = f(x)$, y $x - f(x) \in V_0$ dado que $f(x - f(x)) = f(x) - f^2(x) = f(x) - f(x) = 0$. Esto demuestra que $V = V_0 + V_1$. Por otra parte $V_0 \cap V_1 = \{0\}$ pues al tomar $x \in V_0 \cap V_1$ se tiene $f(x) = 0$, $f(x) = x$ lo que implica $x = 0$.■

Proposición 4 *Sean $f, g \in End_F(V)$ dos proyecciones que conmutan. Entonces $V = V_{00} \oplus V_{01} \oplus V_{10} \oplus V_{11}$ donde $V_{ij} := \{x \in V : f(x) = ix, g(x) = jx\}$ para cualesquiera $i, j = 0, 1$.*

Dem. Descompongamos V respecto de f en la forma $V = V_0 \oplus V_1$ dada por la proposición anterior. Notemos que cada V_i con $i = 0, 1$ es g-invariante, es decir, $g(V_i) \subset V_i$ para $i = 0, 1$. En efecto, si $f(x) = ix$ entonces $f(g(x)) = g(f(x)) = ig(x)$ lo que implica que $g(x) \in V_i$. Podemos entonces considerar las dos restricciones de g a cada uno de los subespacios V_i $(i = 0, 1)$. Sea pues $g : V_i \to V_i$, aplicando la proposición anterior podemos escribir $V_i = V_{i0} \oplus V_{i1}$ donde $V_{ij} := \{x \in V_i : g(x) = jx\}$ $(i = 0, 1)$. Así pues $V = V_0 \oplus V_1 = V_{00} \oplus V_{01} \oplus V_{10} \oplus V_{11}$ como queríamos demostrar. ■

Corolario 3 *Sea A una F-álgebra alternativa y $e \in A$ un idempotente. Se tiene entonces una descomposición de Peirce lateral $A = A_0 \oplus A_1$ donde $A_i := \{x \in A : ex = ix\}$ $(i = 0, 1)$. Análogamente se tiene una descomposición por el otro lado $A = A'_0 \oplus A'_1$ con $A'_i := \{x \in A : xe = ix\}$ $(i = 0, 1)$. Además existe también una descomposición de Peirce bilátera*

$$A = A_{00} \oplus A_{01} \oplus A_{10} \oplus A_{00}$$

donde $A_{ij} := \{x \in A : ex = ix, xe = jx\}$ para $i, j = 0, 1$.

Dem. Como el álgebra es alternativa $L_{x^2} = L_x^2$ y $R_{x^2} = R_x^2$ para cada $x \in A$. Tomando $x = e$ (un idempotente) se tiene $L_e = L_{e^2} = L_e^2$ e igualmente $R_e = R_{e^2} = R_e^2$ lo que significa que L_e y R_e son proyecciones del F-espacio subyacente a A. Además por la identidad flexible $L_e R_e = R_e L_e$ y por tanto podemos aplicar la proposición precedente para obtener la descomposición de Peirce bilátera.■

Veamos ahora algunas propiedades de la descomposición de Peirce (bilátera). Por ejemplo vamos a demostrar que

$$A_{ij} A_{jk} \subset A_{ik}, \qquad A_{ij} A_{ij} \subset A_{ji}$$

para cualesquiera $i, j, k = 0, 1$. Para la primera relación de inclusión tomemos $x_{ij} \in A_{ij}$, $y_{kl} \in A_{kl}$. Entonces

$$\begin{array}{rcc} e(x_{ij}y_{kl}) & = & -(e, x_{ij}, y_{kl}) + (ex_{ij})y_{kl} = \\ & = & (x_{ij}, e, y_{kl}) + (ex_{ij})y_{kl} = \\ & = & jx_{ij}y_{kl} - kx_{ij}y_{kl} + ix_{ij}y_{kl} = \\ & = & (i + j - k)x_{ij}y_{kl} \end{array},$$

y análogamente $(x_{ij}y_{kl})e = (k+l-j)x_{ij}y_{kl}$. Haciendo entonces $j = k$ se obtiene la primera inclusión, mientras que haciendo $k = i$, $l = j$ se obtiene la segunda. Obsérvese que en particular A_{ii} $(i = 0, 1)$ son subálgebras de A. Además si tomamos $x \in A_{11}$, $y \in A_{00}$ se tiene (aplicando las identidades de Moufang) que $xy = (exe)y = e(x(ey)) = 0$ y dualmente $yx = 0$. Así $A_{ii}A_{jj} = 0$ si i y j son distintos. Se dice que estas subálgebras son *ortogonales*. Las relaciones $A_{01}A_{01} \subset A_{10}$, $A_{10}A_{10} \subset A_{01}$ que se han obtenido arriba son más débiles que en el caso asociativo donde se tiene $A_{01}A_{01} = A_{10}A_{10} = 0$.

Como en el caso asociativo, se definen los idempotentes ortogonales como aquellas parejas de idempotentes e, f tales que $ef = fe = 0$. Igual que en el caso asociativo, la suma de idempotentes ortogonales es un idempotente. Para dos idempotentes ortogonales e, f se tiene

$$\begin{array}{c} (x, e, f) = (xe)f = (xe)f^2 = ((xe)f)f = (x, e, f)f = -(x, f, e)f = \\ = -((xf)e)f = -x(fef) = 0 \end{array}$$

Como además $(x, e, e) = 0$ (una de las identidades alternativas), concluimos que para un sistema de idempotentes ortogonales $\{e_1, \ldots, e_n\}$, se verifican $(x, e_i, e_j) = 0$ para cualesquiera i, j y además $(x, e_i, e) = 0$ siendo $e = \sum_i e_i$.

Teorema 6 (Descomposición de Peirce relativa a un sistema de idempotentes ortogonales). *Sea $\{e_1, \ldots, e_n\}$ un conjunto de idempotentes ortogonales de un álgebra alternativa A, entonces existe una descomposición en suma directa de subespacios*

$$A = \bigoplus_{i,j=0}^{n} A_{ij}$$

donde para cada $i, j \in \{0, \ldots, n\}$ el subespacio A_{ij} es el conjunto de aquellos $x \in A$ tales que $e_k x = \delta_{ki} x$, $xe_k = \delta_{kj} x$, para $k = 1, \ldots, n$.

Dem. Supongamos que la descomposición existe. Sea entonces $x \in A$ descompuesto en la forma $x = \sum_{k,j=0}^{n} x_{kj}$ con $x_{kj} \in A_{kj}$. Vamos a demostrar que entonces los sumandos x_{kj} son únicos. Definamos $e = \sum_i e_i$, entonces $e_i x e_j = x_{ij}$, y $e_i x = \sum_{l=0}^{n} x_{il}$, además $e_i x e = \sum_{l=1}^{n} x_{il}$ lo que implica que $x_{i0} = e_i x - e_i x e$. En forma análoga $x_{0i} = xe_i - exe_i$. Por último

$$\begin{array}{rcc} x_{00} & = & x - \sum_{i,j=1}^{n} x_{ij} - \sum_{i=1}^{n} x_{i0} - \sum_{i=1}^{n} x_{0i} = \\ & = & x - \sum_{i,j} e_i x e_j - \sum_i (e_i x - e_i x e) - \sum_i (x e_i - e x e_i) = \\ & = & x - exe - (ex - exe) - (xe - exe) = x - ex - xe + exe. \end{array}$$

Se demuestra además que cada uno de estos x_{kj} pertenecen al correspondiente A_{kj}. Por tanto cada x es expresable en forma única como $x = \sum x_{kj}$, donde $x_{kj} \in A_{kj}$. ■

Proposición 5 (Propiedades de la descomposición de Peirce).

$$A_{ij}A_{jk} \subset A_{ik}, \qquad (i,j,k = 0,1,\ldots,n). \tag{4.6}$$

$$A_{ij}A_{ij} \subset A_{ji}, \qquad (i,j = 0,1,\ldots n). \tag{4.7}$$

$$A_{ij}A_{kl} = 0, \qquad k \neq j, (i,j) \neq (k,l), \tag{4.8}$$
$$(i,j,k,l = 0,1,\ldots,n).$$

$$x^2 = 0 \ \forall x \in A_{ij}, (i \neq j). \tag{4.9}$$

$$xy = -yx \qquad \forall x,y \in A_{ij}, (i \neq j). \tag{4.10}$$

$$(x,y,z) = 0 \qquad si\ (i,j,k) \neq (i,i,i) \tag{4.11}$$
$$\forall x \in A_{ij}, \forall y \in A_{jk}, \forall z \in A_{ki}.$$

$$(x,yz,t) = 0 \qquad si\ i \neq j \tag{4.12}$$
$$\forall x,t \in A_{ii}, \forall y \in A_{ij}, \forall z \in A_{ji}.$$

$$(xy)z = (yz)x = (zx)y \qquad si\ i \neq j \tag{4.13}$$
$$\forall x,y,z \in A_{ij}.$$

$$x(yz) = (xz)y = z(xy) \qquad si\ i \neq j \tag{4.14}$$
$$\forall x,y \in A_{ij}, \forall z \in A_{jj}.$$

$$x(zy) = (zx)y = (xy)z \qquad si\ i \neq j \tag{4.15}$$
$$\forall x,y \in A_{ij}, \forall z \in A_{ii}.$$

$$[x,t]^1(yz) = 0 \qquad si\ i \neq j \tag{4.16}$$
$$\forall x,t \in A_{jj}, \forall y,z \in A_{ij}.$$

$$(yz)[x,t] = 0 \qquad si\ i \neq j \tag{4.17}$$
$$\forall x,t \in A_{ii}, \forall y,z \in A_{ij}.$$

$$(x_{ii}a)^m = (x_{ii}a_{ii})^{m-1} \sum_{k=0}^{n} x_{ii}a_{ik} \tag{4.18}$$

donde $a = \sum_{k=0}^{n} a_{ii}$ *es la descomposición de Peirce de* a.

$$(x_{ij}a)^m = (x_{ij}a_{ji})^{m-1} \sum_{k=0}^{n} x_{ij}a_{jk} + (x_{ij}a_{ji})^{m-1} \tag{4.19}$$
$$si\ i \neq j.$$

$$e_i(x_{ij}a)^m e_i = (x_{ij}a_{ji})^m, \qquad (i,j = 0,1,\ldots,n). \tag{4.20}$$

[1] Recuérdese que $[a,b] := ab - ba$.

Dem. Veamos (2.6): sea $x \in A_{ij}$, $y \in A_{jk}$. Entonces $(e_i, x, y) = xy - e_i(xy)$ lo que implica $e_i(xy) = xy - (e_i, x, y) = xy + (x, e_i, y) = xy + \delta_{ij}xy - \delta_{ij}xy = xy$. Análogamente se demuestra $(xy)e_k = xy$.

(2.7): sean $x, y \in A_{ij}$, entonces $e_j(xy) = -(e_j, x, y) + (e_jx)y = (x, e_j, y) + \delta_{ij}xy = xy - \delta_{ij}xy + \delta_{ij}xy = xy$ y análogamente se tendría $(xy)e_i = xy$.

(2.8): sean $x \in A_{ij}$, $y \in A_{kl}$. Si $k = l$ entonces $xy = x(e_kye_k) = ((xe_k)y)e_k = 0$ por una de las identidades de Moufang. Si $i = j$ la cosa es también bastante trivial: $xy = (e_ixe_i)y = e_i(x(e_iy)) = 0$ ya que $i = j$ es distinto de k. Podemos suponer pues que k es distinto de l y j distinto de i. Recordemos que a partir de la identidad de Moufang $y(xax) = [(yx)a]x$ se obtiene la linealización

$$y[(xa)z] + y[(za)x] = [(yx)a]z + [(yz)a]x$$

y haciendo $y = x_{ij}$, $x = e_k$, $a = y_{kl}$, $z = e_l$ se obtiene

$$x_{ij}[(e_ky_{kl})e_l] + x_{ij}[(e_ly_{kl})e_k] = [(x_{ij}e_k)y_{kl}]e_l + [(x_{ij}e_l)y_{kl}]e_k$$

de donde $x_{ij}y_{kl} + \delta_{lk}x_{ij}y_{kl} = \delta_{jl}(x_{ij}y_{kl})e_k$ y como $\delta_{kl} = 0$ tenemos $x_{ij}y_{kl} = \delta_{jl}(x_{ij}y_{kl})e_k$ y en caso de ser j y l distintos ya se tiene el resultado apetecido. Si $j = l$ sólo tenemos $x_{ij}y_{kj} = (x_{ij}y_{kj})e_k$. Pero

$$x_{ij}y_{kj} = (x_{ij}e_j)y_{kj} = (x_{ij}, e_j, y_{kj}) = -(e_j, x_{ij}, y_{kj}) = e_j(x_{ij}y_{kj}).$$

Esto implica que $e_i(x_{ij}y_{kj}) = e_i[e_j(x_{ij}y_{kj})] = 0$ ya que para dos idempotentes ortogonales e y f se demostró que $(e, f, A) = 0$ (implicando $e(fA) = 0$). Finalmente

$$x_{ij}y_{kj} = (e_ix_{ij})y_{kj} = (e_i, x_{ij}, y_{kj}) + e_i(x_{ij}y_{kj}) = (e_i, x_{ij}, y_{kj}) = -(x_{ij}, e_i, y_{kj}) = 0.$$

(2.9) y (2.10): sea $x \in A_{ij}$ siendo i y j diferentes (por tanto alguno de ellos es no nulo). Si suponemos que i es nulo, $x^2 = (e_ix)(e_ix) = e_i(xe_i)x$ (Teorema de Artin) pero $xe_i = 0$ lo que demuestra que $x^2 = 0$. Para demostrar (2.10) tomamos $x, y \in A_{ij}$, entonces $(x + y)^2 = 0$ y desarrollando $xy + yx = 0$.

(2.11): $(x, y, z) = -(y, x, z) = -(yx)z + y(xz)$ pero $yx = 0$, $xz = 0$ aplicando (4.8).

(2.12): $(x, yz, t) = (x(yz))t - x((yz)t) = -(x, y, z)t + ((xy)z)t - x(y, z, t) - x(y(zt))$ pero $x(y(zt)) = (xy)(zt)$ gracias a (4.11), en consecuencia $(x, yz, t) = -(x, y, z)t + ((xy)z)t - x(y, z, t) - (xy)(zt)) = -(x, y, z)t + (xy, z, t) - x(y, z, t)$ pero $(x, y, z) \in (A_{ii}, A_{ij}, A_{ji}) = 0$ por el apartado anterior,

$$(y, z, t) \in (A_{ij}, A_{ii}, A_{ii}) = 0$$

por idéntico motivo, $(xy, z, t) \in (A_{ij}, A_{ji}, A_{ii}) = 0$ también por el apartado anterior.

(2.13): sean $x, y, z \in A_{ij}$ (siendo i diferente de j), entonces $(xy)z = -(yx)z = -(y, x, z) - y(xz) = (y, z, x) - y(xz) = (yz)x - y(zx) - y(xz) = (yz)x$ y con análogos razonamientos se demuestra la otra igualdad.

(2.14): tomemos $x, y \in A_{ij}$, $z \in A_{jj}$, entonces $x(yz) = -(x, y, z) + (xy)z$ pero $(xy)z \in A_{ji}A_{jj} = 0$. Así pues $x(yz) = -(x, y, z) = (x, z, y) = (xz)y - x(zy)$. Como $x(zy) \in$

$A_{ij}(A_{jj}A_{ij}) = 0$ se tiene $x(yz) = (xz)y$. Por otra parte $x(yz) = (x, z, y) = -(z, x, y) = -(zx)y + z(xy)$ pero como $(zx)y \in (A_{jj}A_{ij})A_{ij} = 0$ se tiene la otra parte de la igualdad. El apartado (2.15) se demuestra en forma análoga al que acabamos de demostrar.

(2.16): Partiendo de la identidad de Moufang 4.3 $(xw)(ax) = x(wa)x$ y por un proceso de linealización, se obtiene

$$(sw)(ar) + (rw)(as) = (s(wa))r + (r(wa))s$$

y haciendo $s = x$, $w = t$, $a = y$, $r = z$ se obtiene

$$(xt)(yz) + (zt)(yx) = (x(ty))z + (z(ty))x$$

pero como $x, t \in A_{jj}$, $y, z \in A_{ij}$, se tiene $ty \in A_{jj}A_{ij} = 0$ $(i \neq j)$. Por tanto $(xt)(yz) = -(zt)(yx)$ para cualesquiera $t, x \in A_{jj}$, $y, z \in A_{ij}$. Como $yz = -zy$ tenemos $-(zt)(yx) = (xt)(yz) = -(xt)(zy) = (yt)(zx) = -(zx)(yt) = (tx)(yz)$. En definitiva $(xt)(yz) = (tx)(yz)$ o lo que es lo mismo $[x, t](yz) = 0$. La identidad 4.17 es consecuencia de la que acabamos de demostrar pasando al álgebra opuesta.

(2.18): hay que demostrar $(x_{ii}a)^m = (x_{ii}a_{ii})^{m-1}\sum_{k=0}^{n} x_{ii}a_{ik}$, hagamos inducción sobre m. Para $m = 1$, $x_{ii}a = \sum_{j,k} x_{ii}a_{jk} = \sum_k x_{ii}a_{ik}$ luego la identidad se satisface en este caso. Supongamos que la identidad se satisface para m y veamos lo que ocurre para $m + 1$:

$$(x_{ii}a)^{m+1} = (x_{ii}a)^m(x_{ii}a) = (x_{ii}a_{ii})^{m-1}(\sum_{k=0}^{n}(x_{ii}a_{ik})(x_{ii}a)) =$$

$$= (x_{ii}a_{ii})^{m-1}\sum_{j,k=0}^{n}(x_{ii}a_{ik})(x_{ii}a_{ij}),$$

y los únicos sumandos no nulos en la suma anterior son los que se obtienen para $k = i$ (ya que para $k = j$ se tiene el sumando $(x_{ii}a_{ij})(x_{ii}a_{ij}) = 0$ al ser el cuadrado de un elemento de A_{ij} con $i \neq j$). Por tanto

$$(x_{ii}a)^{m+1} = (x_{ii}a_{ii})^{m-1}\sum_{j=0}^{n}(x_{ii}a_{ii})(x_{ii}a_{ij}) = (x_{ii}a_{ii})^m\sum_{k=0}^{n}(x_{ii}a_{ik})$$

como queríamos demostrar.

El resto de las demostraciones se dejan como ejercicios para el lector.■

4.3. Elementos nilpotentes

El estudio de los elementos nilpotentes y de los propiamente nilpotentes es también una pieza clave en la teoría de estructura de las álgebras alternativas. En esta sección demostraremos que cada álgebra alternativa semisimple en dimensión finita posee unidad. La descomposición de la unidad como suma de idempotentes irreducibles será posteriormente un hecho fundamental para la clasificación del álgebra en función de la mayor o menor cuantía de aparezcan en dicha descomposición.

Definición 5 *Un elemento z de un álgebra alternativa se dice* propiamente nilpotente *cuando za es nilpotente para cada $a \in A$.*

Nótese que decir que z es propiamente nilpotente es equivalente a afirmar que az es nilpotente para cada $a \in A$, dado que $(az)^{m+1} = a(za)^m z$. Por otra parte si z es propiamente nilpotente, entonces z es nilpotente (pues z^2 es nilpotente). El radical de un álgebra alternativa de dimensión finita se define como el nilideal maximal de A. Se demuestra en [9, Theorem 3.7, p. 40] que el radical de un álgebra alternativa coincide con el conjunto de todos los elementos propiamente nilpotentes. No es fácil demostrar que el conjunto de los elementos propiamente nilpotentes de un álgebra alternativa es un ideal. Hay sin embargo una situación particular, en la que tal demostración es relativamente fácil:

Lema 6 *Sea A una F-álgebra alternativa de dimensión finita, con unidad* 1*, y supongamos que* 1 *es el único idempotente no nulo de A. Entonces cada elemento $z \in A$ o bien tiene inverso, o es propiamente nilpotente. El conjunto R de todos los elementos propiamente nilpotentes es un ideal de A.*

Dem. Si un elemento z no es nilpotente, la subálgebra generada por z no es una nilálgebra y por tanto contiene un idempotente no nulo. Por hipótesis este idempotente es la unidad de A y podemos escribir:

$$1 = \alpha_0 z^n + \cdots + \alpha_{n-1} z$$

de forma que $1 = z(\alpha_0 z^{n-1} + \cdots + \alpha_{n-1}) = zy$ donde $y = \alpha_0 z^{n-1} + \cdots + \alpha_{n-1}$. Entonces claramente z e y conmutan y por tanto $yz = 1$ implicando que todo elemento no nilpotente es inversible. Demostremos ahora que cada elemento nilpotente es propiamente nilpotente. Sea $z \in A$ nilpotente, si para un $a \in A$, el producto za no es nilpotente, entonces es inversible por lo demostrado anteriormente. Supongamos que $z^m = 0$, $z^{m-1} \neq 0$, entonces

$$0 \neq z^{m-1} = z^{m-1}[(za)(za)^{-1}] = [z^{m-1}(za)](za)^{-1} = (z^m a)(za)^{-1} = 0$$

una contradicción. Por tanto todo nilpotente es propiamente nilpotente. Considerando entonces un elemento arbitrario podemos decir que o bien es nilpotente en cuyo caso es propiamente nilpotente, o en caso contrario es inversible. Nos queda demostrar que el conjunto de los elementos propiamente nilpotentes R es un ideal. Por lo previamente demostrado se tiene $RA \subset R$, $AR \subset R$. Veamos que R es cerrado para la suma: sean $z, z' \in R$, si por casualidad $z + z'$ no es propiamente nilpotente, entonces tiene un inverso y. A partir de $(z + z')y = 1$ se deduce $z'y = 1 - zy$ y como zy es nilpotente la serie

$$1 + zy + (zy)^2 + \cdots$$

es en realidad una suma finita y si hacemos el cálculo

$$(1 - zy)(1 + zy + (zy)^2 + \cdots) = [1 + (zy) + (zy)^2 + \cdots] - [(zy) + (zy)^2 + \cdots] = 1$$

y análogamente se demuestra que $(1 + zy + (zy)^2 + \cdots)(1 - zy) = 1$. Entonces $z'y = 1 - zy$ es inversible pero como además es nilpotente al ser $z' \in R$, llegamos a una contradicción. ■

Si $\{e_1, \ldots, e_n\}$ es un conjunto de idempotentes ortogonales de cardinal máximo, está claro que entonces $e := \sum_i e_i$ es un idempotente maximal y cada e_i es un idempotente irreducible (indescomponible en suma de idempotentes ortogonales no nulos). Si $A = \oplus_{i,j=0}^n A_{ij}$ es la descomposición de Peirce de A con relación al conjunto de idempotentes, sabemos que cada A_{ii} es una subálgebra de A. Además A_{00} es una nilálgebra pues en caso contrario contendría un idempotente no nulo (que sería ortogonal a e, en contra de la maximalidad de éste último). La subálgebra A_{ii} tiene un único idempotente no nulo (a saber: e_i) pues si $u \in A_{ii}$ es un idempotente no nulo, $u \neq e_i$ entonces $e_i = u + (e_i - u)$ y $(e_i - u)^2 = e_i + u - e_i u - u e_i = e_i + u - 2u = e_i - u$ lo que quiere decir que $e_i - u$ es un idempotente y $u(e_i - u) = u - u = 0$, $(e_i - u)u = u - u = 0$, es decir tendríamos una descomposición de e_i en suma de idempotentes ortogonales no nulos. Resumiendo los resultados del último párrafo, podemos enunciar el siguiente lema:

Lema 7 *Sea $A = \oplus_{ij} A_{ij}$ la descomposición de Peirce de A relativa a un sistema de idempotentes ortogonales $\{e_1, \ldots, e_n\}$ de cardinal máximo. Entonces cada e_i es un idempotente irreducible y $e := \sum_i e_i$ un idempotente maximal. La subálgebra A_{00} es una nilálgebra y cada A_{ii} es tal que dispone de un único idempotente no nulo: e_i. El conjunto de elementos propiamente nilpotentes de A_{ii} es un ideal de A_{ii}.*

Bajo las mismas condiciones del lema precedente, podemos definir para cualesquiera $i, j = 0, 1, \ldots n$ los conjuntos

$$G_{ij} := \{x \in A_{ij} : \text{ los elementos de } xA_{ji} \text{ son nilpotentes } \}.$$

Es interesante observar que $x \in G_{ij}$ si y sólo si los elementos de $A_{ji}x$ son todos nilpotentes. Merece la pena señalar la igualdad

$$G_{00} = A_{00}.$$

Para demostrar el contenido no evidente sea $x \in A_{00}$, como A_{00} es una nilálgebra, cada elemento de $xA_{00} \subset A_{00}$ es nilpotente lo que implica que $x \in G_{00}$. Del mismo modo, si $x \in A_{0j}$ se tiene $xA_{j0} \subset A_{00}$ luego los elementos de xA_{0j} son todos nilpotentes. Así pues $x \in G_{0j}$ y se tiene la igualdad

$$G_{0j} = A_{0j}.$$

Pasando al álgebra opuesta se tendría $G_{j0} = A_{j0}$.

Lema 8 *Cada G_{ij} es un subespacio de A y $G_{ij} \subset \mathrm{Rad}(A)$.*

Dem. Hemos demostrado en el párrafo anterior que G_{00}, G_{0j} y G_{j0} son subespacios vectoriales de A. Además si $x_{00} \in G_{00}$ y $a \in A$ es arbitrario, se tiene $(x_{00}a)^m = (x_{00}a_{00})^{m-1} \sum_{k=0}^n x_{00}a_{0k}$ y como $x_{00}a_{00}$ es nilpotente se tiene que x_{00} es propiamente nilpotente, es decir, un elemento de $\mathrm{Rad}(A)$. Así hemos demostrado $A_{00} = G_{00} \subset \mathrm{Rad}(A)$. Si $x_{0j} \in G_{0j}$ la identidad 4.19 demuestra de forma análoga que $x_{0j} \in \mathrm{Rad}(A)$. Por otra parte si ahora tomamos un elemento $x_{j0} \in G_{j0}$, el teorema de Artin implica la igualdad

$$(x_{j0}a_{0j})^{m-1} = x_{j0}(a_{0j}x_{j0})^{m-2}a_{0j}$$

y usando la identidad 4.19 se tendría que x_{j0} es propiamente nilpotente, es decir un elemento del radical de A. Demostremos finalmente que cada G_{ij} $(i, j \neq 0)$ es un subespacio contenido en $\mathrm{Rad}(A)$. Sean $s, s' \in G_{ij}$, y $a, a' \in A_{ji}$, entonces sa y $s'a$ son elementos (nilpotentes) de A_{ii}, el conjunto de elementos nilpotentes de A_{ii} es un ideal (que coincide con el conjunto de elementos propiamente nilpotentes de A_{ii}). Así pues $\alpha sa + \beta s'a$ es nilpotente para cualesquiera escalares α y β. Esto demuestra que $\alpha s + \beta s' \in G_{ij}$ y por tanto G_{ij} es un subespacio. Supongamos elegido un elemento $z \in G_{ij}$, entonces las identidades 4.18 y 4.19 demuestran que $z \in \mathrm{Rad}(A)$. ■

Como consecuencias de los resultados que hemos establecido podemos enunciar los siguientes dos corolarios:

Corolario 4 *Sea e un idempotente de un álgebra alternativa A de dimensión finita. Sea $A = A_{00} \oplus A_{10} \oplus A_{01} \oplus A_{11}$ la descomposición de Peirce relativa al idempotente e, entonces $\mathrm{Rad}(A_{ii}) = A_{ii} \cap \mathrm{Rad}(A)$, para todo $i = 0, 1$.*

Dem. Si un elemento $x \in A_{ii} \cap \mathrm{Rad}(A)$ entonces xa es nilpotente para todo a, en particular lo es para los $a \in A_{ii}$. Esto implica que $x \in \mathrm{Rad}(A_{ii})$. Supongamos ahora $x \in \mathrm{Rad}(A_{ii})$, entonces xa_{ii} es nilpotente para cada $a \in A$ y siendo a_{ii} la proyección de a en A_{ii}. Ahora la identidad 4.18 implica que xa es nilpotente y por tanto $x \in A_{ii} \cap \mathrm{Rad}(A)$. ■

Corolario 5 *Sea e un idempotente maximal de un álgebra alternativa A y sea $A = A_{00} \oplus A_{10} \oplus A_{01} \oplus A_{11}$ la descomposición de Peirce de A con relación a e, entonces $A_{10} + A_{01} + A_{00} \subset \mathrm{Rad}(A)$.*

Dem. Escribamos e como suma de idempotentes irreducibles ortogonales $e = \sum e_i$, sea $A = \oplus_{ij} A'_{ij}$ la descomposición de Peirce de A con relación a $\{e_1, \ldots\}$. Sabemos entonces que $A_{10} = \sum_i A'_{i0} = \sum_i G_{i0}$, $A_{01} = \sum_i A_{0i} = \sum_i G_{0i}$, $A_{00} = A'_{00} = G_{00}$. Como habíamos demostrado que $G_{i0}, G_{0i}, G_{00} \subset \mathrm{Rad}(A)$ se tiene $A_{10} + A_{01} + A_{00} \subset \mathrm{Rad}(A)$. ■

Teorema 7 *Toda álgebra alternativa de dimensión finita no nula y semisimple (de radical nulo) tiene unidad.*

Dem. Sea A una tal álgebra , como A no puede ser una nilálgebra debe contener un idempotente no nulo. En particular debe contener un idempotente maximal e. Si hacemos la descomposición de Peirce de A con relación a e nos encontramos con que $A_{01} + A_{10} + A_{00} \subset \mathrm{Rad}(A) = 0$. Por tanto $A = A_{11}$ y e es la unidad de A. ■

4.4. Álgebras de Cayley-Dickson

Supóngase que A es una F-álgebra con unidad (no necesariamente asociativa) provista de una *involución* (es decir, un antiautomorfismo involutivo, o aplicación F-lineal $A \to A$, $x \mapsto \overline{x}$ tal que $\overline{\overline{x}} = x$, $\overline{xy} = \overline{y}\ \overline{x}$ para cualesquiera $x, y \in A$). Supondremos además que la involución es tal que para todo $x \in A$ se tiene

$$x + \overline{x} \in F1, \qquad x\overline{x} \in F1. \tag{4.21}$$

Esto implica que para todo x se satisface la ecuación

$$x^2 - t(x)x + n(x)1 = 0$$

donde $t(x), n(x) \in F$ están dados por $t(x)1 = x + \overline{x}$, $n(x)1 = x\overline{x}$. La aplicación $t : A \to F$ tal que $x \mapsto t(x)$ es lineal y se llamará en lo sucesivo *la aplicación traza*. La aplicación $n : A \to F$ se denominará aplicación *norma*. Como $\overline{1} = 1$ se tiene $t(\alpha 1) = 2\alpha$, $n(\alpha 1) = \alpha^2$ para todo escalar α.

Sea ahora B un F-álgebra unitaria (y de dimensión finita) con involución $b \mapsto \overline{b}$ satisfaciendo 4.21. Por el proceso de *Cayley-Dickson* vamos a construir otra F-álgebra de dimensión el doble que la de B, de modo que esta nueva álgebra conserve algunas de las propiedades de B y contenga a esta última como subálgebra . Esta nueva álgebra que vamos a denotar A no es más que la que se obtiene en el F-espacio vectorial producto $B \times B$, fijando un escalar no nulo $\mu \neq 0$ y definiendo el producto:

$$(b_1, b_2)(b_3, b_4) := (b_1 b_3 + \mu b_4 \overline{b_2}, \overline{b_1} b_4 + b_3 b_2).$$

El álgebra A así obtenida se denotará también por $A = \mathrm{CD}(B, \mu)$. Esta nueva álgebra tiene por unidad a $(1, 0)$, y encierra una copia de B, a saber la subálgebra $B' = \{(x, 0) : x \in B\}$. Por otra parte el elemento $v = (0, 1)$ es tal que $v^2 = \mu 1$ y A es la suma directa de subespacios

$$A = B' \oplus vB'$$

donde B' y vB' tienen la misma dimensión. Si se identifican los elementos de B' con los de B, los elementos de A son de la forma $x = b_1 + vb_2$, $b_i \in B$, $i = 1, 2)$ y la multiplicación en A se puede reescribir de la forma

$$(b_1 + vb_2)(b_3 + vb_4) = (b_1 b_3 + \mu b_4 \overline{b_2}) + v(\overline{b_1} b_4 + b_3 b_2).$$

En particular para cualesquiera $b, b' \in B$ se tiene

$$(vb)b' = v(b'b),$$

$$b(vb') = v(\overline{b}b'),$$

$$(vb)(vb') = \mu b'\overline{b}.$$

Se puede definir una involución en A haciendo para todo $x = b_1 + vb_2$, $\overline{x} := \overline{b_1} - vb_2$. Resulta además que esta involución es tal que $x + \overline{x}, x\overline{x} \in F1$ para todo $x \in A$. El lector debe comprobar que si $x = b_1 + vb_2$, entonces $t(x) = t(b_1)$ y $n(x) = n(b_1) - \mu n(b_2)$.

Teorema 8 *$CD(B,\mu)$ es alternativa si y sólo si B es asociativa.*

Dem. Para demostrar que A es alternativa basta demostrar que $(x,x,y)=0$ para cualesquiera $x,y\in A$ (ya que al ser A un álgebra con involución, el hecho de que se satisfaga $x(xy)=x^2y$ implica automáticamente $(yx)x=yx^2$ para cualesquiera $x,y\in A$). Ahora bien como $x+\overline{x}=t(x)1$, la nulidad de (x,x,y) es equivalente a la nulidad de $(x,\overline{x},y)$. Si escribimos $x=b_1+vb_2$, $\overline{x}=\overline{b_1}-vb_2$, $y=b_3+vb_4$, entonces

$$\begin{aligned}(x,\overline{x},y)=(b_1,\overline{b_1},b_3)+(b_1,\overline{b_1},vb_4)-(b_1,vb_2,b_3)-(b_1,vb_2,vb_4)+\\ +(vb_2,\overline{b_1},b_3)+(vb_2,\overline{b_1},vb_4)-(vb_2,vb_2,b_3)-(vb_2,vb_2,vb_4).\end{aligned}\tag{4.22}$$

Si B es asociativa se tiene $(b_1,\overline{b_1},b_3)=0$. Además

$$(b_1,\overline{b_1},vb_4)=n(b_1)vb_4-b_1(\overline{b_1}(vb_4))=n(b_1)vb_4-b_1(v(b_1b_4)=$$

$$=n(b_1)vb_4-v(\overline{b_1}(b_1b_4))=n(b_1)vb_4-n(b_1)vb_4=0.$$

También:

$$(b_1,vb_2,b_3)=(b_1(vb_2))b_3-b_1((vb_2)b_3)=(v(\overline{b_1}b_2))b_3-b_1(v(b_3b_2))=$$

$$=v[b_3(\overline{b_1}b_2)]-v[\overline{b_1}(b_3b_2)]$$

$$(vb_2,\overline{b_1},b_3)=((vb_2)\overline{b_1})b_3-(vb_2)(\overline{b_1}b_3)=(v(\overline{b_1}b_2))b_3-v[(\overline{b_1}b_3)b_2]=$$

$$=v[b_3(\overline{b_1}b_2)-(\overline{b_1}b_3)b_2]$$

y por lo tanto $-(b_1,vb_2,b_3)+(vb_2,\overline{b_1},b_3)=-v(\overline{b_1},b_3,b_2)=0$ al ser B asociativa. De forma análoga $-(b_1,vb_2,vb_4)+(vb_2,\overline{b_1},vb_4)=-\mu(b_1,b_4,\overline{b_2})=0$. Por otra parte

$$(vb_2,vb_2,b_3)=((vb_2)(vb_2))b_3-(vb_2)((vb_2)b_3)=\mu n(b_2)b_3-(vb_2)(v(b_3b_2))=$$

$$=\mu n(b_2)b_3-\mu(b_3b_2)\overline{b_2}=\mu n(b_2)b_3-\mu b_3(b_2\overline{b_2})=\mu n(b_2)b_3-\mu n(b_2)b_3=0.$$

Y finalmente

$$(vb_2,vb_2,vb_4)=(vb_2)^2(vb_4)-(vb_2)((vb_2)(vb_4))=\mu n(b_2)vb_4-vb_2(\mu b_4\overline{b_2})=$$

$$=\mu n(b_2)vb_4-\mu(vb_2)(b_4\overline{b_2})=\mu n(b_2)vb_4-\mu v((b_4\overline{b_2})b_2)=$$

$$=\mu n(b_2)vb_4-\mu n(b_2)vb_4=0.$$

Lo que demuestra que si B es asociativa, entonces A es alternativa. Recíprocamente, si A es alternativa, se debe tener $(x,\overline{x},y)=0$ y la identidad 4.22 implica $-(b_1,vb_2,b_3)+(vb_2,\overline{b_1},b_3)=0$. Entonces

$$0=-(b_1,vb_2,b_3)+(vb_2,\overline{b_1},b_3)=$$

$$-(b_1(vb_2))b_3+b_1((vb_2)b_3)+((vb_2)\overline{b_1})b_3-(vb_2)(\overline{b_1}b_3)=$$

$$= -(v(\overline{b_1}b_2))b_3 + b_1(v(b_3b_2)) + (v(\overline{b_1}b_2))b_3 - v((\overline{b_1}b_3)b_2) =$$

$$= v[-b_3(\overline{b_1}b_2) + \overline{b_1}(b_3b_2) + b_3(\overline{b_1}b_2) - (\overline{b_1}b_3)b_2] = -v(\overline{b_1}, b_3, b_2)$$

y como v es un elemento inversible ($v^2 = \mu \neq 0$) se tiene la asociatividad de B. ■

Sea A una F-álgebra a la que se puede aplicar el proceso de Cayley-Dickson , es decir, A tiene una involución $x \mapsto \overline{x}$ tal que $x + \overline{x}, x\overline{x} \in F1$ para todo x. Uno puede definir una forma cuadrática $n : A \to F$ mediante $n(a) := a\overline{a}$. La comprobación de que n es una forma cuadrática es rutinaria, basta demostrar que

1. $n(\lambda x) = \lambda^2 n(x)$ para todos $\lambda \in F$, $x \in A$.

2. La aplicación $f : A \times A \to F$ dada por $f(x, y) := n(x + y) - n(x) - n(y)$, es bilineal (esta aplicación se llamará en lo sucesivo, la forma polar de n).

La primera condición es automática para la forma $n(a) = a\overline{a}$. En cuanto a la segunda tenemos

$$f(a, b) = (a + b)\overline{(a + b)} - a\overline{a} - b\overline{b} = a\overline{b} + b\overline{a}$$

lo que demuestra que f es una forma bilineal. Concluimos que n es una forma cuadrática. Si A es alternativa, esta forma cuadrática verifica $n(ab) = n(a)n(b)$ para cualesquiera $a, b \in A$. En efecto

$$n(ab) = (ab)\overline{(ab)} = (ab)(\overline{b}\ \overline{a}) = n(b)a\overline{a} = n(a)n(b).$$

Esta serie de hechos da pie a la siguiente definición

Definición 6 *Una F-álgebra A provista de una forma cuadrática $q : A \to F$ diremos que es un álgebra de composición cuando:*

1. *A tiene unidad.*

2. *$q(ab) = q(a)q(b)$ para cualesquiera $a, b \in A$.*

3. *q es no degenerada.*

Recordemos que q es no degenerada cuando para todo $a \in A$ se tiene que si $f(a, A) = 0$, entonces obligatoriamente $a = 0$ (aquí f es la forma polar de q).

Proposición 6 *Sea A una F-álgebra asociativa unitaria y con involución $x \mapsto \overline{x}$ tal que para todo $x \in A$ se tiene $x + \overline{x}, x\overline{x} \in F$,1 Supongamos que la forma cuadrática $n(a) := a\overline{a}$ es no degenerada. Sea $A' = CD(A, \mu)$ con su involución $\overline{(x, y)} := (\overline{x}, -y)$ y su forma cuadrática $n((x, y)) = (x, y)\overline{(x, y)}$. Entonces la forma cuadrática inducida en A' es también no degenerada.*

Dem. Supongamos que existe $(a,b) \in A'$ tal que $0 = f((a,b),(x,y))$ para cualesquiera $x, y \in A$. Como

$$f((a,b),(x,y)) = (a,b)(\overline{x},-y) + (x,y)(\overline{a},-b) =$$
$$= (a\overline{x} - \mu y\overline{b}, -\overline{a}y + \overline{x}b) + (x\overline{a} - \mu b\overline{y}, -\overline{x}b + \overline{a}y) =$$
$$= (a\overline{x} + x\overline{a} - \mu(y\overline{b} + b\overline{y}), 0)$$

de donde se deduce $f(a,x) = 0 = f(b,y)$ para cualesquiera $x, y \in A$, y siendo f es este caso la forma polar de la norma n de A. Por hipótesis, se tiene la no-degeneración de dicha norma de A lo que implica $a = b = 0$.■

Corolario 6 *Las álgebras obtenidas por el proceso de Cayley-Dickson a partir de un álgebra asociativa unitaria y con involución cuya forma cuadrática asociada sea no degenerada, son necesariamente álgebras de composición.*

Dem. Lo único que faltaba por ver era el carácter no degenerado de la norma del álgebra , pero esto se tiene gracias a la proposición anterior. ■

Proposición 7 *Sea A una F-álgebra con unidad e involución $x \mapsto \overline{x}$ tal que para cada $x \in A$ se tiene $x+\overline{x}, x\overline{x} \in F1$. Entonces si la forma cuadrática $n(x) = x\overline{x}$ es no degenerada, el álgebra A es simple o isomorfa a $F \times F$ con producto por componentes e involución de intercambio.*

Dem. Sea I un ideal de A distinto de A. Supongamos en primer lugar que $\overline{I} = I$. Como $I \cap F$,$1 = 0$ se tiene $a + \overline{a} = 0$, $a\overline{a} = 0$ para cada $a \in I$. Si ahora tomamos elementos $a \in I$, $x \in A$ se tiene $a\overline{x} \in I$ luego

$$f(a,x) = a\overline{x} + x\overline{a} = a\overline{x} + \overline{a\overline{x}} = 0$$

lo que implica $a = 0$ por no degeneración de n. Esto demuestra que para todo ideal I tal que $\overline{I} = I$ se tiene $I = 0$ o $I = A$. Sea ahora T un ideal no nulo cualquiera de A distinto de A. Es evidente que $\overline{T}$ es otro ideal de A no nulo u distinto de A. Definamos $I := T + \overline{T}$, entonces I es un ideal no nulo de A y evidentemente $\overline{I} = I$. Por lo demostrado previamente se debe tener $A = I$. Si ahora definimos $J = T \cap \overline{T}$ resulta que J es otro ideal de A (distinto de A) y $\overline{J} = J$. En definitiva $J = 0$ y tenemos $A = T \oplus \overline{T}$. Como $T\overline{T} \subset T \cap \overline{T} = 0$ e igualmente $\overline{T}T = 0$ la multiplicación en A adopta la forma

$$(x + y)(x' + y') = xx' + yy'$$

para cualesquiera $x, y \in T$, $x', y' \in \overline{T}$. Veamos que T es unidimensional. Sean $s, t \in T$ con $t \neq 0$ y definamos $\lambda = t + \overline{t}$, $\mu = s + \overline{s}$ (que son elementos de F). Si ocurriera $\lambda = 0$ se tendría $t = -\overline{t} \in T \cap \overline{T} = 0$. Por tanto $\lambda \neq 0$, por otra parte $\lambda s = (t + \overline{t})s = ts + \overline{t}s$ pero $\overline{t}s \in \overline{T}T = 0$, lo que permite escribir $\lambda s = ts$. También $\mu t = (s + \overline{s})t = t(s + \overline{s}) = ts + t\overline{x}$ pero $t\overline{s} \in T\overline{T} = 0$ y por tanto $\mu t = ts = \lambda s$, es decir, $s = \lambda^{-1}\mu t$. Esto demuestra que

$T \cong F$ luego $\overline{T} \cong F$. Si denotamos por $\theta : T \to F$ un isomorfismo de F-álgebras , disponemos automáticamente del isomorfismo de F-álgebras $\omega : A = T \oplus \overline{T} \to F \times F$ tal que $\omega(t+\overline{s}) = (\theta(t), \theta(s))$ para cualesquiera $s, t \in T$. Si dotamos a $F \times F$ con la involución de intercambio $\overline{(x,y)} := (y,x)$ (para todos $x, y \in F$), entonces ω es un isomorfismo de álgebras con involución, es decir para cada $a \in A$ se tiene $\overline{\omega(a)} = \omega(\overline{a})$. El lector puede comprobar los detalles que faltan.■

Proposición 8 *Sea A una F-álgebra de composición con forma cuadrática n y forma polar asociada f, entonces cada elemento satisface una ecuación cuadrática con coeficientes en F y A es un álgebra alternativa. La aplicación $x \mapsto \overline{x} := f(1,x) - x$ es una involución de A tal que $x + \overline{x}, x\overline{x} \in F$,1. Si definimos $t(x) := x + \overline{x}, n(x) := x\overline{x}$, se satisface*

$$x^2 - t(x)x + n(x)1 = 0$$

para cada $x \in A$.

Dem. Como $n(x)n(y+w) = n(x(y+w)) = n(xy+xw)$, entonces

$$n(x)n(y+w) - n(x)n(y) - n(x)n(w) = n(xy+xw) - n(xy) - n(xw)$$

es decir, $n(x)f(y,w) = f(xy,xw)$ de donde

$$n(a+b)f(y,w) = f(ay+by, aw+bw) =$$

$$= f(ay,aw) + f(ay,bw) + f(by,aw) + f(by,bw)$$

y como $n(a+b) = f(a,b) + n(a) + n(b)$ se tiene

$$f(a,b)f(y,w) + n(a)f(y,w) + n(b)f(y,w) =$$

$$f(ay,aw) + f(ay,bw) + f(by,aw) + f(by,bw)$$

y simplificando

$$f(a,b)f(y,w) = f(ay,bw) + f(by,aw). \tag{4.23}$$

haciendo $b = 1$, $y = au$ tenemos

$$f(a,1)f(au,w) = f(a(au),w) + f(au,aw).$$

y como $f(au,aw) = n(a)f(u,w)$ esta última ecuación se puede reescribir como

$$f(a(au),w) + n(a)f(u,w) - f(a,1)f(au,w) = 0$$

$$f(a(au) + n(a)u - f(a,1)au, w) = 0$$

que como w es arbitrario implica (por no degeneración de f) que

$$a(au) + n(a)u - f(a,1)au = 0 \tag{4.24}$$

para cualesquiera $a, u \in A$. Si hacemos $u = 1$ se obtiene

$$a^2 - f(a,1)a + n(a)1 = 0$$

lo que demuestra la primera parte de la proposición. Para demostrar que A es alternativa multipliquemos la ecuación anterior por u a la derecha:

$$a^2u - f(a,1)au + n(a)u = 0$$

y restando a esta igualdad la igualdad (4.24) se llega a $a^2u = a(au)$ para cualesquiera $a, u \in A$. Análogamente se demostraría $ua^2 = (ua)a$ para cualesquiera $u, a \in A$. Demostremos ahora que $\overline{x} := f(x,1) - x$ es una involución, es fácil comprobar que dicha aplicación es lineal. Además $\overline{\overline{x}} = \overline{f(x,1) - x)} = f(x,1) - \overline{x} = f(x,1) - f(x,1) + x = x$. Habíamos demostrado antes que para cada x se tiene $x^2 - f(x,1)x + n(x) = 0$. Haciendo $x = a + b$ se obtiene

$$ab + ba - f(a,1)b - f(b,1)a + f(a,b) = 0$$

Por otra parte a partir de la identidad (4.23) podemos deducir que

$$f(1,a)f(1,b) = f(1,ab) + f(a,b) \tag{4.25}$$

y sustituyendo esto en la igualdad de antes:

$$ab + ba - f(a,1)b - f(b,1)a + f(1,a)f(1,b) - f(1,ab) = 0$$

de donde

$$(f(1,a) - a)(f(1,b) - b) = f(1,ab) - ba$$

pero a partir de la identidad (4.25) se tiene $f(1,ab) = f(1,ba)$. Esto demuestra que $\overline{a}\overline{b} = \overline{ba}$. Además $x + \overline{x} = f(1,x) \in F$ (por tanto $t(x) := f(1,x)$) y $x\overline{x} = xf(1,x) - x^2 = n(x) \in F$. Resulta demás evidente que para todo x se satisface $x^2 - t(x)x + n(x) = 0$. ■

Proposición 9 *Sea A un álgebra de composición con norma n y forma polar f. Entonces se satisfacen las identidades $f(xy,z) = f(x,z\overline{y}) = f(y,\overline{x}z)$ para cualesquiera $x, y, z \in A$.*

Dem. Por un lado:

$$f(xy,z) = (xy)\overline{z} + z(\overline{y}\ \overline{x}) = (x,y,\overline{z}) + x(y\overline{z}) + z(\overline{y}\ \overline{x}) =$$

$$= (x,y,\overline{z}) + x(y\overline{z}) - (z,\overline{y},\overline{x}) + (z\overline{y})\overline{x} = -(x,y,z) - (z,y,x) + f(x,z\overline{y}) =$$

$$= -(x,y,z) + (x,y,z) + f(x,z\overline{y}) = f(x,z\overline{y}).$$

La otra identidad se demuestra con razonamientos análogos. ■

Teorema 9 *Sea A un álgebra de composición y B una subálgebra conteniendo a la unidad de A. Entonces $B^\perp B + BB^\perp \subset B^\perp$. Para cualesquiera $a, b \in B$ y $v \in B^\perp$ se tiene*

$$\overline{v} = -v, \quad av = v\overline{a}, \quad (vb)a = v(ab), \quad a(vb) = v(\overline{a}b), \quad (va)(vb) = -n(v)b\overline{a}.$$

Dem. Como B tiene unidad entonces $\overline{B} = B$. Si $x \in B^\perp$, se tiene $f(xB, B) = f(x, B\overline{B}) = f(x, B^2) = f(x, B) = 0$ lo que demuestra que $B^\perp B \subset B^\perp$. Análogamente se tendría $BB^\perp \subset B^\perp$. si $v \in B^\perp$, entonces $0 = f(1, v) = t(v)$ luego $\overline{v} = -v$. Para todo $a \in B$ se tiene $0 = f(v, a) = v\overline{a} - av$ lo que implica $av = v\overline{a}$. Por otra parte, como $vb \in B^\perp$, se tiene $f(vb, a) = 0$ lo que es equivalente a $(vb)\overline{a} - a(\overline{b}v) = 0$. Así $(vb)\overline{a} = a(\overline{b}v)$. Por otra parte

$$(vb)\overline{a} = (v, b, \overline{a}) + v(b\overline{a}) = -(b, v, \overline{a}) + v(b\overline{a}) = (\overline{b}, v, \overline{a}) + v(b\overline{a}) =$$

$$= (\overline{b}v)\overline{a} - \overline{b}(v\overline{a}) + v(b\overline{a}) = (vb)\overline{a} - \overline{b}(v\overline{a}) + v(b\overline{a})$$

lo que permite establecer la igualdad $\overline{b}(v\overline{a}) = v(b\overline{a})$ o lo que es lo mismo $b(va) = v(\overline{b}a)$ o si se prefiere $a(vb) = v(\overline{a}b)$. Esto demuestra de paso la igualdad $(vb)a = v(ab)$. Finalmente

$$(va)(vb) = (v, a, vb) + v(a(vb)) = -(v, vb, a) + v(v(\overline{a}b)) = (v, vb, \overline{a}) - n(v)\overline{a}b =$$

$$= -n(v)b\overline{a} - v((vb)\overline{a}) - n(v)\overline{a}b = -n(v)b\overline{a} + n(v)\overline{a}b - n(v)\overline{a}b = -n(v)b\overline{a}.$$

■

Proposición 10 *Sea A una F-álgebra de composición. Entonces:*

1. *Si $\dim(A) > 1$, la involución de A no puede ser la identidad.*
2. *Existe siempre una subálgebra (que contiene a la unidad de A) no degenerada de dimensión a lo sumo dos.*

Dem. Veamos la primera parte. Tomemos $x \in A$ tal que x no sea múltiplo escalar de 1. Si la involución es la identidad $x + x = t(x) \in F$ lo que implica que $2x \in F$. Por tanto si la característica es distinta de dos llegamos a contradicción. Así F es un cuerpo de característica dos. Por otra parte, de ser la identidad una involución se deduce que A es un álgebra conmutativa. Pero entonces si denotamos por f la forma polar de la forma cuadrática n del álgebra de composición, sabemos que $f(x, y) = xy + yx = 2xy = 0$ y por tanto n es degenerada en contra de que A es de composición.

Veamos el segundo apartado. Por subálgebra no degenerada de A entendemos una subálgebra B (unitaria) tal que la restricción de f a B es una forma bilineal no degenerada. Si el cuerpo base es de característica distinta de dos, entonces podemos tomar $B = F1$. Supongamos que la característica es dos. En este caso al ser A de composición, se tendrá $\dim(A) > 1$. Sea pues $x \in A$ tal que $\{1, x\}$ es linealmente independiente. Si para todo x que sea linealmente independiente con 1 se tiene $t(x) = 0$, entonces la traza es nula en general $t(A) = 0$ pero esto implica que $\overline{a} = a$ para cada a, es decir la involución sería la identidad.

Así pues debe existir un x linealmente independiente de 1 tal que $t(x) \neq 0$. Consideremos entonces la subálgebra B formada por todas las combinaciones lineales de 1 y x (el hecho de que x satisface una ecuación de segundo grado con coeficientes en F, garantiza que B es una subálgebra). La restricción de f a B tiene por matriz (referida a la base $\{1, x\}$):

$$\begin{pmatrix} 0 & t(x) \\ t(x) & 0 \end{pmatrix}$$

cuyo determinante es no nulo al ser $t(x) \neq 0$. Esto demuestra que B es no degenerada. ■

Antes de abordar los últimos resultados de esta sección vamos a dar una lista de álgebras de composición:

1. Todo cuerpo de característica distinta de dos es un álgebra de composición (sobre sí mismo) con involución la identidad y por tanto norma $n(x) = x^2$ que es automáticamente no degenerada y multiplicativa. Si el cuerpo es de característica dos la norma es degenerada (de hecho su forma polar es idénticamente nula).

2. Para dar ejemplos de álgebras de composición bidimensionales, debemos presentar las F-álgebras $K(\mu)$ con $\mu \in F$. Esta álgebra es la suma directa $K(\mu) = F,1 \oplus Fv$ con $v^2 = v + \mu$, $4\mu + 1 \neq 0$ e involución $\overline{\alpha + \beta v} = (\alpha + \beta) - \beta v$. La norma viene dada por $n(z) := z\overline{z}$ para cada $z \in A$. Es fácil comprobar que $K(0)$ es isomorfa al álgebra $F \times F$ con producto por componentes e involución de intercambio (por tanto es un álgebra de composición split). Además, si el polinomio $t^2 - t - \mu$ es reducible, se puede demostrar que $K(\mu)$ es isomorfa a $K(0)$. Si por el contrario, el polinomio $t^2 - t - \mu$ es irreducible, $K(\mu)$ es un cuerpo extensión cuadrática de F. Si la característica de F es distinta de dos, se puede demostrar que $K(\mu) = \mathrm{CD}(F, \gamma)$ (para algún γ). En efecto, definiendo $v_1 := v - 1/2$ se tiene $v_1^2 = \mu + \frac{1}{4}$ y utilizando la base $\{1, v_1\}$ de $K(\mu)$ se observa que $K(\mu)$ se obtiene a partir de F por el proceso de Cayley-Dickson para algún escalar no nulo γ. Recíprocamente, las álgebras $\mathrm{CD}(F, \gamma)$ son todas del tipo $K(\mu)$ ya que si en $\mathrm{CD}(F, \gamma)$ consideramos $v = (0, 1)$ y $u := v + 1/2$, encontramos que $u^2 = u + \mu$ donde $\mu = \gamma - 1/4$, entonces $\mathrm{CD}(F, \gamma) = K(\mu)$. Las álgebras de este apartado son asociativas y conmutativas pero la involución nunca es la identidad.

3. Para mostrar álgebras de composición de dimensión cuatro podemos presentar las álgebras $Q(\mu, \beta)$ (con $\beta \neq 0$). Estas álgebras son por definición $Q(\mu, \beta) := \mathrm{CD}(K(\mu), \beta)$, y se denominan álgebras *de cuaterniones generalizados*. Son asociativas pero no conmutativas.

4. Podemos introducir álgebras de composición de dimensión ocho. Estas serían las álgebras $C(\mu, \beta, \gamma) = \mathrm{CD}(Q(\mu, \beta), \gamma)$ con $\gamma \neq 0$. Dichas álgebras se llaman *álgebras de Cayley* o también álgebras de octoniones generalizados. Son alternativas pero no asociativas. Evidentemente si se aplica el proceso de Cayley-Dickson a estas álgebras , no obtenemos álgebras alternativas. Por eso desde el punto de vista de las álgebras de composición, tenemos de dejar de aplicar el proceso de Cayley-Dickson en este punto.

A la vista de los ejemplos que acabamos de dar, cabe plantearse la cuestión sobre la existencia de otras álgebras de composición no isomorfas a alguna de las de la lista anterior. El lector puede demostrar como un ejercicio relativamente sencillo que cada álgebra de composición de dimensión uno o dos del tipo F o $K(\mu)$. La respuesta a la cuestión anterior en general viene dada por el siguiente:

Teorema 10 *Sea A una F-álgebra de composición, entonces A es isomorfa a alguna de las álgebras F, $K(\mu)$, $Q(\mu,\beta)$ o $C(\mu,\beta,\gamma)$. Si la característica de F es dos, no puede darse la posibilidad $A \cong F$.*

Dem. Si $\dim(A) \in \{1,2\}$ el asunto es bastante sencillo. Si suponemos que $\dim(A) > 2$ la Proposición 10 nos asegura la existencia de una subálgebra B propia conteniendo a la unidad de A no degenerada y de dimensión a lo sumo dos. Se tiene por tanto una descomposición $A = B \oplus B^{\perp}$ (todo subespacio S no degenerado y de dimensión finita de una espacio X provisto de una forma bilineal simétrica, descompone a X en la forma $X = S \oplus S^{\perp}$). Entonces podemos encontrar un $v \in B^{\perp}$ de norma $n(v) = \gamma_1$ no nula (si la norma se anulara sobre $B^{\perp}$ se llega a que f es degenerada). Por el Teorema 9 este elemento v satisface las condiciones

$$\overline{v} = -v, \quad av = v\overline{a}, \quad (vb)a = v(ab), \quad a(vb) = v(\overline{a}b), \quad (va)(vb) = -n(v)b\overline{a}$$

para cualesquiera $a, b \in B$. Se tiene entonces que $B_1 := B \oplus vB$ es una subálgebra contenida en A y por las propiedades expuestas de v, se tiene $B_1 = \mathrm{CD}(B,\gamma)$. Se demuestra sin problema que B_1 es no degenerada. Si $B_1 \neq A$ podemos repetir el proceso aplicado a B con B_1. Así tenemos la existencia de $v_1 \in B_1^{\perp}$ de norma $n(v_1) = \gamma_1 \neq 0$ y tal que v_1 satisface propiedades análogas a las que cumplía v. Podemos entonces definir $B_2 = B_1 \oplus v_1 B_1 = \mathrm{CD}(B_1, \gamma_1)$ que resultará ser una subálgebra no degenerada y conteniendo a la unidad de A. En caso de que $B_2 \neq A$ reiteramos este proceso constructivo de nuevas álgebras B_3, etc. Entonces se debe tener $A = B_3$ (si B era de dimensión uno) o $A = B_2$ en caso de que B fuese bidimensional. En efecto si $B = F$, el álgebra B_3 es alternativa pero no asociativa y por tanto B_4 que estaría contenida en A ya no sería alternativa, una contradicción. En caso de que B fuera bidimensional, su involución no sería la identidad, B_1 sería asociativa pero no conmutativa y B_2 seria alternativa pero no asociativa. Por tanto $A = B_2$ toda vez que A_3 no sería alternativa.

En cualquier caso vemos que A se obtiene a partir de F o de $K(\mu)$ (en característica dos) por aplicación del proceso de Cayley-Dickson .■

Vamos a acabar esta sección estudiando las álgebras de composición split sobre cualquier cuerpo. Observemos en primer lugar que si A es una F-álgebra que contiene un idempotente $e \neq 0, 1$, entonces A es split. En efecto se tiene $e(e-1) = 0$ con $e \neq 0, 1$. Recíprocamente, si A es split y tomamos un $x \in A$ de norma nula, se tiene $x^2 = t(x)x$. Analicemos dos posibilidades:

1. Todo elemento de A de norma nula tiene también traza nula.

2. Existe un elemento de A de norma nula pero traza no nula.

En el primer caso si tomamos $a \in A - \{0\}$ con $n(a) = 0$, se tiene para todo $x \in A$ que $n(ax) = n(a)n(x) = 0$. Pero entonces $t(ax) = 0$ y teniendo en cuenta la identidad (4.25) $f(1,a)f(1,x) = f(1,ax) + f(a,x)$ se deduce que $f(a,x) = t(a)t(x) - t(ax) = 0$ lo que contradice el carácter no degenerado de f. Así la segunda posibilidad se da necesariamente y podemos asegurar la existencia de un $x \in A$ con $n(x) = 0$ pero $t(x) = \alpha \neq 0$. Como se tiene $x^2 = \alpha x$, definiendo $e := \alpha^{-1}x$ tenemos $e^2 = \alpha^{-2}x^2 = \alpha^{-2}\alpha x = \alpha^{-1}x = e$, es decir, un idempotente no nulo (como además $n(x) = 0$ no puede darse $e = 1$).

Hemos demostrado entonces:

Lema 9 *Un álgebra de composición es split si y sólo si contiene un idempotente no nulo y distinto de la unidad.*

Corolario 7 *Toda álgebra de composición split contiene como subálgebra una copia de $K(0)$. En particular toda álgebra de composición split bidimensional es isomorfa a $K(0)$.*

Dem. Sea A la F-álgebra y $e \in A$ un idempotente $e \neq 0, 1$. Sea B la subálgebra generada por $\{1, e\}$. Claramente B consiste en todas la combinaciones lineales $\alpha + \beta e$ con $\alpha, \beta \in F$. Como $e^2 = e$, la traza de e es 1 y su norma es nula. Por tanto $\overline{e} = 1 - e$. Así para un elemento genérico $\lambda + \mu e$ de B la involución queda perfectamente determinada:

$$\overline{\lambda + \mu e} = \lambda + \mu(1 - e) = (\lambda + \mu) - \mu e$$

lo que acaba la demostración de que $B \cong K(0)$.■

Teorema 11 *Toda álgebra de composición split es isomorfa a alguna de las siguientes: $K(0)$, $Q(0,1)$, o $C(0,1,1)$.*

Dem. Sea A un álgebra de composición split y B una subálgebra de A isomorfa a $K(0)$. Entonces B tiene una base $\{1, e\}$ donde $e^2 = e$ y la involución de B viene determinada por $\overline{e} = 1 - e$. Si $B \neq A$ vamos a demostrar que existe $v \in B^\perp$ tal que $v^2 = 1$. En principio tenemos la existencia de $u \in B^\perp$ de norma no nula. Este elemento verifica $\overline{u} = -u$, y $u^2 = -n(u) = \alpha \neq 0$. Además $uB \subset B^\perp$. Definamos entonces $v = u + \alpha^{-1}(1 - \alpha)ue \in B^\perp$. Por otra parte $(ue)^2 = ueue = u^2\overline{e}e = \alpha(1 - e)e = 0$ y

$$v^2 = u^2 + \alpha^{-1}(1 - \alpha)(u^2 e + ueu) = \alpha + \alpha^{-1}(1 - \alpha)(\alpha e + u(u\overline{e}) =$$

$$= \alpha + \alpha^{-1}(1 - \alpha)(\alpha e + \alpha\overline{e}) = \alpha + (1 - \alpha)t(e) = \alpha + 1 - \alpha = 1.$$

Por otra parte como $v \in B^\perp$ se tiene $\overline{v} = -v$. De este modo $B_1 := B \oplus vB = \mathrm{CD}(B, 1) \cong \mathrm{CD}(K(0), 1) = Q(0,1)$. Si $B_1 \neq A$ podemos repetir este proceso encontrando $v_1 \in B_1^\perp$ tal que $v_1^2 = 1$. Definiríamos entonces $B_2 = B_1 \oplus v_1 B_1 = \mathrm{CD}(B_1, 1) \cong \mathrm{CD}(Q(0,1), 1) = C(0,1,1)$. Entonces B_2 es alternativa y no asociativa. Por tanto debe coincidir con A pues en caso contrario encontraríamos $v_2 \in B_2^\perp$ tal que $v_2^2 = 1$ y $B_2 \oplus v_2 B_2 = \mathrm{CD}(B_2, 1)$ sería

una subálgebra de A pero esto no puede ser pues A es alternativa lo que implicaría que $\mathrm{CD}(B_2, 1)$ lo es (y por tanto B_2 sería asociativa en contra de los establecido).■

A la vista de lo establecido en los problemas, donde se propone como ejercicio el demostrar que para un álgebra real A en las condiciones de aplicarle el proceso de Cayley-Dickson , se tiene $\mathrm{CD}(A, \mu) \cong \mathrm{CD}(A, 1)$ si $\mu > 0$, y $\mathrm{CD}(A, \mu) \cong \mathrm{CD}(A, -1)$ si $\mu < 0$, las álgebras de composición reales que surgen a partir de $\mathbb{R}$ serían solo $\mathbb{C} = \mathrm{CD}(\mathbb{R}, -1)$ y $\mathbb{C}_s = \mathrm{CD}(\mathbb{R}, 1)$. Esta última $\mathbb{C}_s$ es la única álgebra de composición real split en dimensión dos. Las álgebras que surgen a partir de $\mathbb{C}$ aplicando el proceso de Cayley-Dickson serían $\mathbb{H} = \mathrm{CD}(\mathbb{C}, -1)$ (de división) y $\mathbb{H}_s = \mathrm{CD}(\mathbb{C}, 1)$ (esta última es split). Las álgebras $\mathrm{CD}(\mathbb{C}_s, \mu)$ son todas split (al contener a $\mathbb{C}_s$) por tanto isomorfas a la única $\mathbb{R}$-álgebra de composición split de dimensión cuatro: $\mathbb{H}_s$. Por último las $\mathbb{R}$-álgebras que surgen a partir de $\mathbb{H}$ por el proceso de Cayley-Dickson son $\mathbb{O} = \mathrm{CD}(\mathbb{H}, -1)$ (de división) y $\mathbb{O}_s = \mathrm{CD}(\mathbb{H}, 1)$ (split). Todas las álgebras $\mathrm{CD}(\mathbb{H}_s, \mu)$ al ser split, son isomorfas a $\mathbb{O}_s$. Así la lista completa salvo isomorfismos de las $\mathbb{R}$-álgebras de composición es: $\mathbb{R}$, $\mathbb{C}$, $\mathbb{C}_s$, $\mathbb{H}$, $\mathbb{H}_s$, $\mathbb{O}$, y $\mathbb{O}_s$.

4.5. Álgebras alternativas simples

En esta sección vamos a estudiar las álgebras alternativas simples de dimensión finita. Como tales álgebras son semisimples (al tener unidad el radical debe ser nulo), podemos descomponer la unidad como una suma de idempotentes irreducibles ortogonales.

Lema 10 *Sea A un álgebra alternativa simple y de dimensión finita. Sea $e \neq 1$ un idempotente. Entonces en la descomposición de Peirce de A con relación a e, $A_{11} = eAe$ es un álgebra asociativa.*

Dem. Como consecuencia de las fórmulas 4.11 y 4.6 se tiene $(A_{10}A_{01})A_{11} \subset A_{10}A_{01}$ luego $A_{10}A_{01}$ es un ideal de A_{11}. Análogamente $A_{01}A_{10}$ es un ideal de A_{00}. En consecuencia

$$I = A_{10}A_{01} + A_{10} + A_{01} + A_{01}A_{10}$$

es un ideal de A. Como A es simple $I = 0$ o $I = A$. La primera posibilidad implicaría $A_{10} = A_{01} = 0$ luego $A = A_{11} + A_{00}$. En este caso tanto A_{11} como A_{00} son ideales de A y por simplicidad, uno de ellos debe ser nulo y el otro coincidiría con A. Al ser $e \neq 1$ se debe tener $A_{11} = 0$ y en este caso es evidente que A_{11} es asociativa. Si $I = A$ se tiene $A_{11} = A_{10}A_{01}$, $A_{00} = A_{01}A_{10}$. Ahora la asociatividad de A_{11} es un corolario de la fórmula 4.12. ■

Lema 11 *Sea A un álgebra alternativa simple de dimensión finita y sea $1 = e_1 + \cdots + e_n$ una descomposición de la unidad como suma de idempotentes ortogonales no nulos (no necesariamente irreducibles). Si $n \geq 3$, entonces A es asociativa.*

Dem. Sea $A = \oplus_{ij} A_{ij}$ la descomposición de Peirce de A con relación a $\{e_1, \ldots, e_n\}$. Si hacemos también la descomposición de A relativa a e_1:

$$A = A'_{11} \oplus A'_{10} + A'_{01} + A'_{00}$$

sabemos que[2] $A'_{11} = A_{11}$ mientras que

$$A'_{10} = \oplus_{i=2}^{n} A_{1i}, \quad A'_{01} = \oplus_{i=2}^{n} A_{i1}, A'_{00} = \oplus_{i,j=2}^{n} A_{ij}.$$

Además por el lema 10 $A'_{11} = A_{11}$ es un álgebra asociativa. Si llamamos $e = e_2 + \cdots + e_n$ y hacemos la descomposición de Peirce de A con relación a e tenemos $A = B_{11} + B_{10} + B_{01} + B_{00}$ donde $B_{11} = \oplus_{i,j=2}^{n} A_{ij}$, $B_{00} = A_{11}$ (nuevamente aludimos a los problemas de este capítulo). Como $B_{11} = A'_{00}$ es asociativa, ya sólo nos queda demostrar que $A'^2_{10} = A'^2_{01} = 0$ para concluir que A es asociativa (problemas del final del capítulo). Pero siendo $A'_{10} = \sum_{i>1} A_{1i}$, basta demostrar que $A^2_{1i} = 0$ para tener en virtud de las propiedades de la descomposición de Peirce, que $A'^2_{10} = 0$. Pero a su vez, el demostrar que $A^2_{1i} = 0$ para $i > 1$ es bastante trivial y aquí es donde utilizaremos el hecho crucial de que $n \geq 3$. Consideremos el idempotente $u = e_1 + e_i$ $(i > 1)$, entonces uAu es un álgebra asociativa pues $u \neq 1$ por ser $n \geq 3$ y gracias al lema 10. Pero

$$uAu = A_{11} + A_{1i} + A_{i1} + A_{ii}$$

es la descomposición de Peirce de uAu con relación al idempotente u. Esto implica en particular que $A^2_{1i} = A^2_{i1} = 0$, acabando la demostración del lema. ■

El lema precedente hace que en lo sucesivo, tengamos que enfocar la atención en aquellas álgebras alternativas simples (de dimensión finita) en las que la unidad sea o bien un idempotente irreducible, o se exprese como una suma de a lo sumo dos idempotentes ortogonales irreducibles.

Lema 12 *Sea A una F-álgebra alternativa simple y de dimensión finita. Supongamos que:*

1. $1 = e_1 + e_2$ *para dos idempotentes ortogonales irreducibles* e_i,
2. $A_{ii} (= e_i A e_i) = F e_i$, $(i = 1, 2)$.
3. *A no es asociativa.*

Entonces A es isomorfa al álgebra de Cayley split $C(0, 1, 1)$.

Dem. Tomemos cualquier subálgebra semisimple B de A tal que $e_1, e_2 \in B$ (por ejemplo A podría ser una tal subálgebra). En la descomposición de Peirce de B relativa a $\{e_1, e_1\}$ tenemos $B = B_{11} \oplus B_{12} \oplus B_{21} \oplus B_{22}$, con $B_{ij} \subset A_{ij}$ y por tanto $B_{ii} = F e_i$. Como $B_{12} B_{21} \subset B_{11} = F e_1$ podemos definir una forma bilineal $< , >: B_{12} \times B_{21} \to F$ tal que $x_{12} x_{21} =< x_{12}, x_{21} > e_1$ (para cualesquiera $x_{ij} \in B_{ij}$). Del mismo modo podremos definir otra forma bilineal $< , >: B_{21} \times B_{12} \to F$ tal que $x_{21} x_{12} =< x_{21}, x_{12} > e_2$. Ahora bien $x_{12} x_{21} x_{12} =<$

[2] Véanse los problemas de este capítulo.

$x_{12}, x_{21} > x_{12} =< x_{21}, x_{12} > x_{12}$ lo que implica la igualdad $< x_{12}, x_{21} >=< x_{21}, x_{12} >$ para cualesquiera $x_{ij} \in B_{ij}$. Veamos que $< \ , \ >$ es no degenerada. Si $< x_{12}, \_ >= 0$ entonces $x_{12}B_{21} = 0$ pero entonces $x_{12} \in G_{12} \subset \mathrm{Rad}(B) = 0$ lo que implica $x_{12} = 0$. Análogamente se demuestra que si $< \_, x_{21} >= 0$ entonces $x_{21} = 0$. Esto implica la igualdad $\dim(B_{12}) = \dim(B_{21})$ (en particular $\dim(A_{12}) = \dim(A_{21})$). Además, dado $x_{12} \neq 0$ existe $b_{21} \in B_{21}$ tal que $x_{12}b_{21} = e_1$. Entonces $b_{21}x_{12}$ no puede ser nulo, pues si lo fuera tendríamos $0 = b_{21}x_{12}b_{21} = b_{21}$ lo que conduciría a la contradicción $e_1 = 0$. Así pues $b_{21}x_{12} = \alpha e_2$ con $\alpha \neq 0$, entonces $x_{12}b_{21}x_{12} = \alpha x_{12}$ implicando $x_{12} = \alpha x_{12}$ y entonces $\alpha = 1$. Así pues

$$x_{12}b_{21} = e_1, \qquad b_{21}x_{12} = e_2 \tag{4.26}$$

En caso de que $B \neq A$ se tiene $\dim(B) = 2 + 2\dim(B_{12}) < \dim(A) = 2 + 2\dim(A_{12})$ lo que implica $B_{12} \neq A_{12}$ (e igualmente $B_{21} \neq A_{21}$). Entonces existe $f_{12} \in A_{12}$ tal que f_{12} no está en B_{12}. Sea $\{u_1, \ldots, u_k\}$ una base de B_{12} y $\{w_1, \ldots, w_k\}$ una base de B_{21} tal que $< u_i, w_j >= \delta_{ij}$ (delta de Kronecker). Definamos el elemento

$$g_{12} := f_{12} - \sum_{i=1}^{k} < f_{12}, w_i > u_i$$

que sigue siendo un elemento de A_{12} que no está en B_{12}. Además $< g_{12}, w_j >= 0$ para todo $j = 1, \ldots, k$. Como (4.26) es aplicable para $B = A$ tenemos la existencia de $g_{21} \in B_{21}$ tal que $g_{12}g_{21} = e_1$, $g_{21}g_{12} = e_2$. Definamos a continuación el elemento

$$h_{21} = g_{21} - \sum_{j=1}^{k} < u_j, g_{21} > w_j$$

que pertenece a A_{21}. Además

$$g_{12}h_{21} = e_1 - \sum_{j} < u_j, g_{21} > g_{12}w_j = e_1 - \sum_{j} < u_j, g_{21} >< g_{12}, w_j > e_1 = e_1$$

y análogamente $h_{21}g_{12} = e_2$. Además

$$< u_i, h_{21} >=< u_i, g_{21} > - \sum_{j=1}^{k} < u_i, w_j >< u_j, g_{21} >=$$

$$=< u_i, g_{21} > - < u_i, g_{21} >= 0.$$

Definamos a continuación $v := g_{12} + h_{21}$. Este elemento está no está en B ya que g_{12} es no elemento de B_{12}. Además

$$v^2 = g_{12}h_{21} + h_{12}g_{21} = e_1 + e_2 = 1$$

Supongamos ahora que B es un álgebra con involución $b \mapsto \overline{b}$ tal que

$$b + \overline{b}, b\overline{b} \in F,1$$

(por ejemplo B podría ser $B = Fe_1 \oplus Fe_2$ con la involución $\overline{\alpha e_1 + \beta e_2} = \beta e_1 + \alpha e_2$). A partir de la igualdad $x^2 - t(x)x + n(x) = 0$, aplicada a los vectores u_i y a los w_j se deduce

$$\overline{v_i} = -v_i, \qquad \overline{w_j} = -w_j$$

y teniendo también en cuenta que $n)(e_1) = n(e_2) = 0$ se tiene $e_i - t(e_i)e_i = 0$ lo que implica $t(e_i) = 1$ luego $e_i + \overline{e_i} = 1$ y entonces $\overline{e_1} = e_2$. Entonces si hacemos $b = \alpha e_1 + \sum_i \alpha_i u_i + \sum_j \beta_j W_j + \beta e_2$, entonces $\overline{b} = \alpha e_2 - \sum_i \alpha_i u_i - \sum_j \beta_j W_j + \beta e_1$. Por tanto, teniendo en cuenta que $u_i h_{21} = 0$ y que $w_j g_{12} = 0$ tenemos:

$$bv = \alpha g_{12} + \sum_i \alpha_i u_i g_{12} + \sum_j \beta_j w_j h_{12} + \beta h_{21} =$$

$$= \beta h_{21} - \sum_i \alpha_i g_{12} u_i - \sum_j \beta_j h_{12} w_j + \alpha g_{12} = v\overline{b}.$$

Si partimos del álgebra $B = Fe_1 \oplus Fe_2 \cong K(0)$ que es asociativa y conmutativa, se tiene que entonces $B \oplus vB$ es el álgebra obtenida a partir de B por el proceso de Cayley-Dickson para $\mu = 1$, es decir, $B_1 := B \oplus vB = \mathrm{CD}(B, 1) \cong \mathrm{CD}(K(0), 1) = Q(0, 1)$ que es por tanto un álgebra de cuaterniones split. Si $B_1 \neq A$ entonces partiendo de B_1 y aplicando lo anterior construiríamos

$$B_2 := B_1 \oplus v_1 B_1 = \mathrm{CD}(B_1, 1) \cong C(0, 1, 1)$$

que sería entonces un álgebra de Cayley o de octoniones generalizados. Si $B_2 \neq A$ repetiríamos la historia llegando a que A (que es alternativa) contendría una subálgebra $\mathrm{CD}(B_2, 1)$ que no sería alternativa (al no ser asociativa B_2). ■

Como corolario del lema anterior podemos ya clasificar las álgebras alternativas simples de dimensión finita sobre un cuerpo algebraicamente cerrado. En primer lugar, hay que recordar al lector que si F es un cuerpo algebraicamente cerrado y D es una F-álgebra de división de dimensión finita, entonces $D \cong F$ (para demostrarlo considérese el polinomio minimal de cada elemento no nulo que será necesariamente de primer grado). Sea ahora A una F-álgebra alternativa simple de dimensión finita y no asociativa (F algebraicamente cerrado como antes), entonces su unidad se descompone como suma de dos idempotentes ortogonales e irreducibles $1 = e_1 + e_2$. Para poder aplicar el Lema 12 debemos comprobar que $A_{ii} (= e_i A e_i) = Fe_i$, $(i = 1, 2)$. Pero sabemos que A_{ii} es una subálgebra cuya unidad e_i es el único idempotente no nulo. En tales álgebras (véase el Lema 6) los elementos caen siempre dentro de dos categorías: o son inversibles o son nilpotentes (y por tanto propiamente nilpotentes). Pero por el Corolario 4, $\mathrm{Rad}(A_{ii}) = A_{ii} \cap \mathrm{Rad}(A) = 0$ lo que implica que A_{ii} es semisimple y entonces no puede contener elementos propiamente nilpotentes no nulos (luego tampoco contiene elementos nilpotentes no nulos). Así A_{ii} es una F-álgebra de división de dimensión finita. Al ser F algebraicamente cerrado, se tiene $A_{ii} = Fe_i$ como queríamos demostrar. En consecuencia el Lema 12 implica que $A \cong C(0, 1, 1)$.

Teorema 12 *Sea F un cuerpo algebraicamente cerrado y A una F-álgebra alternativa simple y de dimensión finita. Entonces A es o bien asociativa y por tanto isomorfa a $\mathcal{M}_n(F)$ para algún $n \geq 1$, o bien es isomorfa a un álgebra de octoniones split $C(0,1,1)$.*

Podemos dar una versión del teorema anterior sin la hipótesis de clausura algebraica del cuerpo base. Para ello necesitaremos el siguiente lema:

Lema 13 *Sea A una F-álgebra (unitaria) y $K \supset F$ un cuerpo extensión de F. Supongamos que la K-álgebra extensión por escalares $A_K := K \otimes_F A$ es una K-álgebra de composición. Entonces A es una F-álgebra de composición con la restricción de la norma de A_K.*

Dem. Supongamos A sumergida en A_K y sea $n : A_K \to K$ la norma de A_k. Veamos que para cada $x \in A$, su norma como elemento de A_K está en el cuerpo F. Sabemos que

$$x^2 - t(x)x + n(x) = 0$$

donde $x \in A$, $t(x), n(x) \in K$. Sea $\{u_i\}_{i=0}^n$ una base de A con $u_0 = 1$ (este mismo conjunto resulta ser una base del K-espacio A_K). Supongamos que $u_i u_j = \sum_k \gamma_{ijk} u_k$ con las constantes de estructura $\gamma_{ijk} \in F$. Sea $x \in A$ tal que $x \notin F$,1. Entonces $x = \sum_i \lambda_i u_i$ con algún $\lambda_k \neq 0$ ($k \neq 0$). La ecuación $x^2 - t(x)x + n(x) = 0$ se convierte entonces en

$$\sum_{ijk} \lambda_i \lambda_j \gamma_{ijk} u_k - t(x) \sum_k \lambda_k u_k + n(x) = 0$$

lo que implica que para $k \neq 0$ se tendrá

$$\sum_{ij} \lambda_i \lambda_j \gamma_{ijk} - t(x)\lambda_k = 0$$

y si $\lambda_k \neq 0$ podremos concluir que $t(x) \in F$. Entonces $\overline{x} = 1 - x$ luego $\overline{x} \in A$ y por tanto $n(x) = x\overline{x} \in A$. Si $x = \lambda$,1 con $\lambda \in F$, entonces $\overline{x} = x$ y $n(x) = x\overline{x} \in A$. De este modo A esta provista de una forma cuadrática $n : A \to F$ (restricción de la de A_K). Veamos que dicha forma cuadrática es no degenerada. Para cualesquiera $x, y \in A$ sea $f(x, y)$ la forma polar de n aplicada a x e y (esta es restricción de la forma polar de la norma de A_K). Supongamos que $x \in A$ es tal que $f(x, A) = 0$. Para cada $y \in A_K$ se tiene $y = \sum_i k_i u_i$ con $k_i \in K$. Además $f(x, y) = \sum_i k_i f(x, u_i) = 0$ ya que para cada i se tiene $f(x, u_i) = 0$. Por ser A_K un álgebra de composición se tiene entonces $x = 0$. Así A resulta ser un álgebra de composición. ■

Definición 7 *Un álgebra alternativa A sobre un cuerpo F se dice que es central cuando su centro $Z(A)$ definido como el conjunto de elementos $Z(A) = \{x \in A : [x, A] = (x, A, A) = 0\}$ coincide con F.*

Las álgebras alternativas simples de dimensión finita tiene centro no nulo al ser unitarias. Además el centro es un cuerpo pues si tomamos $x \in Z(A)$ con $x \neq 0$, el subespacio $xA = Ax$ resulta ser un ideal (no nulo) de A al ser $(xA)A = x(AA) \subset xA$. Entonces $xA = A$ lo que implica que $1 \in xA$ y por tanto $1 = xy = yx$ para algún $y \in A$. Esto demuestra que x es inversible en A. Pero el elemento y resulta también ser un elemento del centro $Z(A)$ ya que a partir de $xa = ax$ para todo $a \in A$ se tiene $y(xa) = y(ax)$, y por tanto $(yx)a = y(ax)$, lo que nos lleva a la igualdad $a = y(ax) = (ya)x$. En consecuencia $ay = ((ya)x)y = (ya)(xy) = ya$ lo que demuestra que $[y, A] = 0$. Para demostrar que $(y, A, A) = 0$ tomemos $a, b \in A$ cualesquiera. Entonces $a = xa' = a'x$ (siendo $a' = ya = ay$) y también $b = xb' = b'x$ (para $b' = yb = by$). Entonces

$$(ay)b = ((a'x)y)b) = a'b = a'(xb') = (a'x)b' = ab' = a(yb)$$

lo que demuestra $(A, y, A) = 0$ y por el carácter alternante de los asociadores se tiene $(y, A, A) = 0$.

Así para un álgebra alternativa simple A de dimensión finita, su centro $Z(A)$ es un cuerpo y podemos considerar A como una $Z(A)$-álgebra . Vista de este modo, A sería central. Podríamos entonces aplicar el siguiente resultado de [10, Theorem 2, p.137]

Teorema 13 *Sea A un álgebra central simple sobre un cuerpo F y sea K cualquier extensión del cuerpo F, entonces el álgebra $A_K := K \otimes_F A$ es (central) simple.*

Utilizando este último resultado podemos por fin obtener la clasificación de las álgebras alternativas simples de dimensión finita:

Teorema 14 *Sea A un álgebra alternativa simple de dimensión finita sobre un cuerpo F. Entonces o bien:*

1. *A es asociativa y por tanto isomorfa a $\mathcal{M}_n(D)$ donde D es una F-álgebra de división de dimensión finita.*

2. *A no es asociativa en cuyo su centro (al que denotaremos por Z) es un cuerpo y A considerada como una Z-álgebra es un álgebra de Cayley-Dickson .*

Dem. Supongamos que A no es asociativa, y consideremos A como álgebra sobre su centro Z. Entonces A es central simple y podemos aplicar el Teorema 13. Si K es la clausura algebraica de Z, el álgebra $A_K := K \otimes_Z A$ es central simple pero no asociativa (ya que la aplicación $A \to A_K$ tal que $a \mapsto a \otimes 1$ es un monomorfismo de Z-álgebras). Esto quiere decir que $A_K \cong C(0, 1, 1)$ es un álgebra de octoniones split y por tanto un álgebra de composición. Aplicando el Lema 13 resulta que la Z-álgebra A es de composición y como no es asociativa, solo puede ser un álgebra de Cayley-Dickson .■

4.6. Problemas

Esta sección de problemas va a estar dedicada a la descomposición de Peirce y al proceso de Cayley-Dickson.

Problema 38 *Demuéstrense las identidades que se han dejado como ejercicio al lector en la proposición relativa a las propiedades de la descomposición de Peirce (Proposición 5).*

Problema 39 *Sea A un álgebra alternativa con unidad y $1 = e_1 + \cdots + e_n$ una descomposición de la unidad como suma de idempotentes ortogonales no nulos. Demuéstrese que si se descompone A con relación al idempotente e_1 en la forma $A = A'_{11} + A'_{10} + A'_{01} + A'_{00}$ se tienen las relaciones: $A'_{11} = A_{11}$, $A'_{10} = \oplus_{i>1} A_{1i}$, $A'_{01} = \oplus_{i>1} A_{i1}$, $A'_{00} = \oplus_{i,j>1} A_{ij}$.*

Problema 40 *Bajo las mismas condiciones que en el problema anterior considérese el idempotente $e = e_2 + \cdots + e_n$. Demuéstrese que si $A = B_{11} + B_{10} + B_{01} + B_{00}$ es la descomposición de Peirce de A con relación a e, entonces $B_{11} = \oplus_{i,j=2}^{n} A_{ij}$, $B_{00} = A_{11}$. Identifíquense los subespacios B_{10} y B_{01}.*

Problema 41 *Bajo las condiciones de los dos problemas anteriores, demuéstrese que si $u = e_1 + e_i$ entonces la descomposición de Peirce de uAu con relación a e_1 es*

$$uAu = C_{11} + C_{10} + C_{01} + C_{00}$$

donde $C_{11} = A_{11}$, $C_{10} = A_{1i}$, $C_{01} = A_{i1}$, y $C_{00} = A_{ii}$.

Problema 42 *Sea e un idempotente de un álgebra alternativa y $A = A_{00} + A_{01} + A_{10} + A_{11}$ la descomposición de Peirce de A relativa a e. Demuéstrese que A es asociativa si y sólo si A_{ii} lo es (para $i = 0, 1$) y $A_{10}^2 = A_{01}^2 = 0$.*

Problema 43 *Sea A una $\mathbb{R}$-álgebra a la que se puede aplicar el proceso de Cayley-Dickson. Demuéstrese que si $\mu > 0$ entonces $CD(A, \mu) \cong CD(A, 1)$ mientras que si $\mu < 0$ entonces $CD(A, \mu) \cong CD(A, -1)$ (sugerencia: búsquense isomorfismos del tipo $(x, y) \mapsto (x, ky)$ donde $x, y \in A$, $k \in \mathbb{R}$).*

Problema 44 *Sea A un álgebra compleja a la que se puede aplicar el proceso de Cayley-Dickson. Demuéstrese que para cualquier $\mu \neq 0$ se tiene $CD(A, \mu) \cong CD(A, 1)$. Compruébese que lo anterior es aplicable no solo sobre los complejos, sino también para álgebras sobre cuerpos algebraicamente cerrados.*

Problema 45 *Si definimos $\mathbb{C}_s := CD(\mathbb{R}, 1)$, demuéstrese que existe un isomorfismo entre el álgebra de complejos 'split' $\mathbb{C}_s$ y el álgebra definida sobre $\mathbb{R} \times \mathbb{R}$ con producto por componentes:*

$$(x, y)(x', y') := (xx', yy')$$

para $x, y, x', y' \in \mathbb{R}$.

Problema 46 *En el álgebra CD*$(\mathbb{C}, -1)$ *definamos los elementos* $1 = (1, 0)$, $I = (i, 0)$, $J = (0, 1)$, $K = (0, -i)$. *Compruébese que* $\{1, I, J, K\}$ *es una base de CD*$(\mathbb{C}, -1)$, *respecto a la cual la tabla de multiplicar del álgebra es*

.	I	J	K
I	-1	K	$-J$
J	$-K$	-1	I
K	J	$-I$	-1

.

Conclúyase que CD$(\mathbb{C}, -1)$ *es isomorfa al álgebra* $\mathbb{H}$ *de cuaterniones reales de división (por tanto es un álgebra asociativa pero no conmutativa).*

Problema 47 *En el álgebra CD*$(\mathbb{C}, 1)$ *definamos los elementos* $1 = (1, 0)$, $I = (i, 0)$, $J = (0, 1)$, $K = (0, -i)$. *Compruébese que* $\{1, I, J, K\}$ *es una base de CD*$(\mathbb{C}, 1)$, *respecto a la cual la tabla de multiplicar del álgebra es*

.	I	J	K
I	-1	K	$-J$
J	$-K$	1	$-I$
K	J	I	1

.

Esta álgebra se denomina álgebra de 'cuaterniones split' y se denota por $\mathbb{H}_s$. *El calificativo 'split' hace alusión a la existencia de divisores de cero, ¡compruébese!*

Problema 48 *Demuéstrese que el álgebra* $\mathbb{H}_s$ *de cuaterniones split es isomorfa al álgebra* $\mathcal{M}_2(\mathbb{R})$ *de matrices cuadradas* 2×2 *sobre los reales. Sugerencia: en* $\mathcal{M}_2(\mathbb{R})$, *tomemos las matrices* $1 =$*matriz identidad,*

$$I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, K = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

una vez comprobado que estas matrices forman una base del álgebra , constrúyase la tabla de multiplicar relativa a dicha base.

Problema 49 *Demuéstrese que CD*$(\mathbb{C}_s, 1)$ *es isomorfa a* $\mathbb{H}_s$, *para ello tómese en CD*$(\mathbb{C}_s, 1)$ *la base* $1 = (1, 0)$, $I = (0, i)$, $J = (0, 1)$, $K = (-i, 0)$ *y constrúyase la tabla de multiplicar. Compruébese también que CD*$(\mathbb{C}_s, -1)$ *es isomorfa a* $\mathbb{H}_s$ *(en este caso se puede hacer* $I = (0, 1)$, $J = (i, 0)$, $K = (0, i)$*).*

Problema 50 *Generalizando el problema anterior se pide demostrar lo siguiente: sea A un álgebra asociativa con un elemento v tal que* $v\overline{v} = -1$. *Demuéstrese que entonces la aplicación* $f : CD(A, +1) \to CD(A, -1)$ *dada por* $f(x, y) := (x, yv)$ *es un isomorfismos de álgebras con involución.*

Problema 51 *Sea B un álgebra a la que se puede aplicar el proceso de Cayley-Dickson . Demuéstrese que:*

1. *B es asociativa y conmutativa si y sólo si $CD(B,\mu)$ es asociativa.*

2. *B es asociativa, conmutativa y de involución identidad si y sólo si $CD(B,\mu)$ es asociativa y conmutativa.*

Problema 52 *Demuéstrese que sobre un cuerpo algebraicamente cerrado F, cualquier álgebra de composición de dimensión mayor que uno es split. Por tanto las álgebras de composición sobre un tal cuerpo son: F (en caso de característica distinta de dos), $K(0)$, $Q(0,1)$ y $C(0,1,1)$.*

Problema 53 *Sean X e Y dos F-espacios vectoriales de dimensión finita y $f : X \times Y \to F$ una aplicación bilineal. Supóngase que:*

1. *$f(x,Y) = 0$ implica $x = 0$.*

2. *$f(X,y) = 0$ implica $y = 0$.*

Demuéstrese que $\dim(X) = \dim(Y)$ y para cada base $\{u_i\}$ de X existe una base $\{w_j\}$ de Y tal que $f(u_i, w_j) = \delta_{ij}$ (la delta de Kronecker).

Problema 54 *Sea F un cuerpo, en el F-espacio vectorial tridimensional F^3 definimos la forma bilineal simétrica $< \cdot | \cdot >: F \times F \to F$ tal que si $x = (x_1, x_2, x_3)$, $y = (y_1, y_2, y_3)$, entonces $< x|y >:= \sum_{i=1}^{3} x_i y_i$. Por otra parte definamos $\wedge : F^3 \times F^3 \to F^3$ tal que*

$$x \wedge y = \begin{vmatrix} i & j & k \\ x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \end{vmatrix} = \left(\begin{vmatrix} x_2 & x_3 \\ y_2 & y_3 \end{vmatrix}, -\begin{vmatrix} x_1 & x_3 \\ y_1 & y_3 \end{vmatrix}, \begin{vmatrix} x_1 & x_2 \\ y_1 & y_2 \end{vmatrix} \right).$$

Consideremos el F-espacio vectorial

$$A = \begin{pmatrix} F & F^3 \\ F^3 & F \end{pmatrix}$$

es decir el conjunto formado por todas las matrices con escalares en la diagonal y vectores de F^3 en los lugares $(1,2)$ y $(2,1)$. Dicho conjunto se dota de estructura de F-espacio vectorial con operaciones por 'componentes'. Definamos el siguiente producto en A:

$$\begin{pmatrix} \alpha & v \\ w & \beta \end{pmatrix} \begin{pmatrix} \alpha' & v' \\ w' & \beta' \end{pmatrix} := \begin{pmatrix} \alpha\alpha' + < v|w' > & \alpha v' + \beta' v - w \wedge w' \\ \alpha' w + \beta w' + v \wedge v' & \beta\beta' + < w|v' > . \end{pmatrix}$$

Demuéstrese que la aplicación

$$\overline{\begin{pmatrix} \alpha & v \\ w & \beta \end{pmatrix}} := \begin{pmatrix} \beta & -v \\ -w & \alpha \end{pmatrix}$$

es una involución para el producto definido en A. Este álgebra es conocida como el álgebra de matrices de Zorn. Demuéstrese que A es una F-álgebra de composición de dimensión ocho y split. Conclúyase que $A \cong C(0,1,1)$.

Problema 55 *Dado un cuerpo F, sea $\{i,j,k\}$ la base canónica del F-espacio vectorial F^3. En la F-álgebra de las matrices de Zorn A del problema anterior, tomamos la base*

$$e_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad e_2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix},$$

$$e_3 = \begin{pmatrix} 0 & i \\ 0 & 0 \end{pmatrix}, \; e_4 = \begin{pmatrix} 0 & j \\ 0 & 0 \end{pmatrix}, \; e_5 = \begin{pmatrix} 0 & k \\ 0 & 0 \end{pmatrix},$$

$$e_6 = \begin{pmatrix} 0 & 0 \\ i & 0 \end{pmatrix}, \; e_7 = \begin{pmatrix} 0 & 0 \\ j & 0 \end{pmatrix}, \; e_8 = \begin{pmatrix} 0 & 0 \\ k & 0 \end{pmatrix}.$$

Demuéstrese que la tabla de multiplicar en la base $\{e_i : i = 1, \ldots, 8\}$ es:

$$\begin{pmatrix} e_1 & 0 & e_3 & e_4 & e_5 & 0 & 0 & 0 \\ 0 & e_2 & 0 & 0 & 0 & e_6 & e_7 & e_8 \\ 0 & e_3 & 0 & e_8 & -e_7 & e_1 & 0 & 0 \\ 0 & e_4 & -e_8 & 0 & e_6 & 0 & e_1 & 0 \\ 0 & e_5 & e_7 & -e_6 & 0 & 0 & 0 & e_1 \\ e_6 & 0 & e_2 & 0 & 0 & 0 & -e_5 & e_4 \\ e_7 & 0 & 0 & e_2 & 0 & e_5 & 0 & -e_3 \\ e_8 & 0 & 0 & 0 & e_2 & -e_4 & e_3 & 0 \end{pmatrix},$$

donde la entrada (i,j) de la matriz anterior es precisamente el producto $e_i e_j$. Compruébese directamente que A es un álgebra simple.

Problema 56 *Sea $\mathbb{O}_s = CD(\mathbb{H}, 1)$ el álgebra de octoniones split reales. Demuéstrese directamente que $\mathbb{O}_s \cong A$ donde A es el álgebra de matrices de Zorn sobre $\mathbb{R}$.*

Problema 57 *Sea $\mathbb{O} = CD(\mathbb{H}, -1)$ el álgebra de octoniones reales de división. Si consideramos la base estandar $\{1, i, j, k\}$ de $\mathbb{H}$, podemos construir la base de $\mathbb{O}$ dada por:*

$$e_1 = (1,0), e_2 = (i,0), e_3 = (j,0), e_4 = (j,0),$$

$$e_5 = (0,1), e_6 = (0,i), e_7 = (0,j), e_8 = (0,k).$$

Demuéstrese que la tabla de multiplicar de $\mathbb{O}$ respecto a esta base es[3]

$$\begin{pmatrix} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 & e_8 \\ e_2 & -e_1 & e_4 & -e_3 & -e_6 & e_5 & -e_8 & e_7 \\ e_3 & -e_4 & -e_1 & e_2 & -e_7 & e_8 & e_5 & -e_6 \\ e_4 & e_3 & -e_2 & -e_1 & -e_8 & -e_7 & e_6 & e_5 \\ e_5 & e_6 & e_7 & e_8 & -e_1 & -e_2 & -e_3 & -e_4 \\ e_6 & -e_5 & -e_8 & e_7 & e_2 & -e_1 & -e_4 & e_3 \\ e_7 & e_8 & -e_5 & -e_6 & e_3 & e_4 & -e_1 & -e_2 \\ e_8 & -e_7 & e_6 & -e_5 & e_4 & -e_3 & e_2 & -e_1 \end{pmatrix}.$$

[3]Como de costumbre el elemento (i,j) de la tabla es el producto $e_i e_j$.

Compruébese que la aplicación lineal $\mathbb{O} \to \mathbb{O}$ *tal que* $e_1 \mapsto e_1$, $e_i \mapsto -e_i$ $(i \neq 1)$, *es una involución de* $\mathbb{O}$, *y que la aplicación* $n : \mathbb{O} \to \mathbb{R}$ *definida por* $\mathfrak{n}(x) := x\overline{x}$, *es una forma cuadrática definida positiva. Conclúyase a partir de este hecho, que* $\mathbb{O}$ *es un álgebra de división.*

Problema 58 *Clasifíquense las álgebras alternativas simples de dimensión finita sobre el cuerpo* $\mathbb{R}$ *de los reales.*

Capítulo 4

Nociones básicas y primeros resultados sobre álgebras de Lie

En este capítulo seguiremos la referencia [2]. Recordemos que si F es un cuerpo y L una F-álgebra cuyo producto denotaremos de la forma $L \times L \to L$ tal que $(x, y) \mapsto [x, y]$, entonces diremos que L es un *álgebra de Lie* si

i) $[x, x] = 0$ para cada $x \in L$.

ii) $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$ para cualesquiera $x, y, z \in L$.

La segunda de las identidades recibe el nombre de *identidad de Jacobi*. Observemos que la primera identidad implica la anticonmutatividad: $[x, y] = -[y, x]$ para todos $x, y \in L$ sin más que partir de $[x + y, x + y] = 0$ y usar la bilinealidad del producto[1].

Entre los ejemplos más naturales de álgebras de Lie podemos destacar el de las *álgebras antisimetrizadas de álgebras asociativas*. Recordemos la definición de tal construcción: si A es una F-álgebra cualquiera, entonces el álgebra A^- cuyo F-espacio vectorial subyacente coincide con el de A, pero dotada del producto $[x, y] := xy - yx$, se denominará el álgebra antisimetrizada de A (se denotará por A^-). Es fácil comprobar que si A es asociativa, entonces A^- es de hecho un álgebra de Lie . Esto también es cierto si A es alternativa sobre un cuerpo de característica dos o tres (véase el problema 60).

Como caso particular de álgebra de Lie antisimetrizada, podemos considerar el de la F-álgebra $\mathfrak{gl}(V)$ (conocida como *álgebra lineal general*) donde V es un F-espacio vectorial. Este álgebra se define como la antisimetrizada de la F-álgebra asociativa $\mathrm{End}_F(V)$ de los endomorfismos del espacio vectorial V (con la composición como producto). Si V es de dimensión finita n, el álgebra $\mathrm{End}_F(V)$ se puede identificar con el álgebra de matrices $\mathcal{M}_n(F)$. Si denotamos por e_{ij} la matriz elemental con un uno en la posición (i, j) y cero en los demás lugares[2], es fácil comprobar que la multiplicación de este tipo de matrices se ajusta a la fórmula

$$e_{ij}e_{kl} = \delta_{jk}e_{il}$$

[1] Si el cuerpo es de característica distinta de dos, entonces i) es equivalente a la anticonmutatividad.

[2] Como es sabido, $\{e_{ij}\}$ es una base del álgebra de matrices cuadradas.

donde δ_{jk} es la delta de Kronecker. Se suele emplear la notación $\mathfrak{gl}(n,F)$ para el álgebra de Lie antisimetrizada de $\mathcal{M}_n(F)$. El producto en este álgebra vendría dado por las expresiones:

$$[e_{ij}, e_{kl}] = \delta_{jk}e_{il} - \delta_{li}e_{kj}.$$

4.1. Álgebras de Lie clásicas.

Una observación interesante sobre las álgebras $\mathfrak{gl}(V)$ es que mientras que $\mathcal{M}_n(F)$ es un álgebra simple, el álgebra de Lie $\mathfrak{gl}(V)$ no lo es: el conjunto de matrices de la forma $\lambda 1$ donde 1 representa la identidad $1 : V \to V$, y λ es cualquier elemento de F, es un ideal. Representaremos a este ideal con la notación $F1$. Podemos entonces considerar el álgebra cociente $\mathfrak{gl}(V)/F1$. En el problema 61 se pide la demostración de que bajo condiciones adecuadas, existe un isomorfismo entre este cociente, y el álgebra de Lie $\mathfrak{sl}(V)$ de los endomorfismos $f : V \to V$ de traza nula. Recordemos que la traza de una matriz cuadrada no es más que la suma de los elementos de la diagonal. Es fácil demostrar que la traza de xy coincide con la traza de yx. Esto implica que las trazas de una matriz x y de la matriz pxp^{-1} (con p inversible) coinciden. Por tanto matrices semejantes tienen la misma traza y esto posibilita el hablar de la traza de un endomorfismo sobre un espacio de dimensión finita (como la traza de cualquiera de las matrices del endomorfismo, fijada una base). En consecuencia podemos definir el espacio $\mathfrak{sl}(V)$ de todos los endomorfismos de V de traza nula. Dado que para cualesquiera $x, y \in \mathfrak{gl}(V)$, se tiene que $\text{traza}(xy) = \text{traza}(yx)$, todo endomorfismo $[x, y]$ es de traza nula, lo que podemos expresar mediante la relación

$$[\mathfrak{gl}(V), \mathfrak{gl}(V)] \subset \mathfrak{sl}(V).$$

Esto implica que $\mathfrak{sl}(V)$ es una subálgebra de $\mathfrak{gl}(V)$.

Si fijamos una base de V, podemos denotar por x' la matriz de un endomorfismo x de V en dicha base. Como las matrices de los endomorfismos de $\mathfrak{sl}(V)$ son de traza nula, el conjunto de matrices

$$\mathfrak{sl}(n,F) := \{m \in \mathcal{M}_n(F) : \text{traza}(m) = 0\},$$

es un álgebra de Lie que no es más que la expresión matricial del álgebra $\mathfrak{sl}(V)$. Para encontrar la dimensión de $\mathfrak{sl}(V)$ podemos considerar la aplicación lineal traza, $\text{traza} : \mathfrak{gl}(V) \to F$ que a cada matriz asocia su traza. Esta aplicación es lineal y su núcleo es precisamente $\mathfrak{sl}(V)$. Así se tiene $\mathfrak{gl}(V)/\mathfrak{sl}(V) \cong F$ lo que implica que $\dim(\mathfrak{sl}(V)) = \dim(\mathfrak{gl}(V)) - 1$.

Definición 8 *Sea V un F-espacio vectorial de dimensión $l+1$. El álgebra $\mathfrak{sl}(l+1,F)$ de las matrices cuadradas de orden $l+1$ y traza nula (o bien el álgebra $\mathfrak{sl}(V)$), diremos que es un* álgebra de Lie clásica de tipo A_l. *Este álgebra recibe el nombre de* álgebra lineal especial. *Su dimensión es $(l+1)^2 - 1 = l^2 + 2l$.*

Consideremos ahora un F-espacio vectorial[3] V de dimensión $2l+1$ y sea $f : V \times V \to F$ una forma bilineal simétrica no degenerada tal que su matriz respecto a una base B sea

$$f' = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1_l \\ 0 & 1_l & 0 \end{pmatrix}$$

donde 1_l representa la matriz identidad $l \times l$. Entonces definimos el *álgebra ortogonal* $\mathfrak{o}(V)$ como la subálgebra de los endomorfismos $x : V \to V$ tales que $f(x(v), w) = -f(v, x(w))$ para cualesquiera $v, w \in V$. Se comprueba que $\mathfrak{o}(V)$ es una subálgebra de $\mathfrak{gl}(V)$. Si denotamos por x' a la matriz de x respecto a B, y escribimos x' con la misma estructura de bloques que la matriz de f, es decir

$$x' = \begin{pmatrix} a & b_1 & b_2 \\ c_1 & m & n \\ c_2 & p & q \end{pmatrix},$$

entonces resulta que $x \in \mathfrak{o}(V)$ si y sólo si $x'f' = -f'x'^t$, y esto ocurre exactamente cuando $a = 0$, $c_1 = -b_2^t$, $c_2 = -b_1^t$, $q = -m^t$, $n^t = -n$, $p^t = -p$. El conjunto de todas estas matrices es entonces un álgebra de Lie de matrices, isomorfa a $\mathfrak{o}(V)$ y se denotará por $\mathfrak{o}(2l+1, F)$.

Definición 9 *El álgebra de Lie $\mathfrak{o}(2l+1, F)$ se dice que es un álgebra de Lie clásica de tipo B_l. Su dimensión es $2l^2+l$ (hágase el problema 64) y no es más que la expresión matricial de $\mathfrak{o}(V)$, donde V es un F-espacio vectorial de dimensión $2l+1$ provisto de una forma bilineal simétrica no degenerada como en el párrafo anterior.*

Sea ahora V un F-espacio vectorial de dimensión $2l$ provisto de una forma bilineal antisimétrica no degenerada f. Supondremos que F es de característica distinta de dos. Respecto a cierta base B la matriz de f es del tipo

$$f' = \begin{pmatrix} 0 & 1_l \\ -1_l & 0 \end{pmatrix}.$$

Denotemos por $\mathfrak{sp}(V)$ la subálgebra de $\mathfrak{gl}(V)$ formada por todos los endomorfismos x tales que $f(x(v), w) = -f(v, x(w))$ para cualesquiera elementos $v, w \in V$. El lector puede comprobar que el corchete de $\mathfrak{gl}(V)$ aplicado a dos elementos de $\mathfrak{sp}(V)$ vuelve a dar un elemento de $\mathfrak{sp}(V)$. En términos matriciales, si representamos x por su matriz respecto a B, con la misma estructura de bloques que la matriz s, resulta que $x \in \mathfrak{sp}(V)$ si y sólo si $x'f' = -f'x'^t$, y esto ocurre si y sólo si la matriz de x en B es del tipo

$$\begin{pmatrix} m & n \\ p & q \end{pmatrix}$$

donde $n^t = n$, $p^t = p$, $m^t = -q$. El conjunto de tales matrices forma un álgebra de Lie que denotaremos por $\mathfrak{sp}(2l, F)$, y que es visiblemente isomorfa a $\mathfrak{sp}(V)$. Este álgebra es de dimensión $2l^2 + l$ y se llamará *el álgebra simpléctica*.

[3]Supondremos que la característica de F no es dos.

Definición 10 *El álgebra de Lie* $\mathfrak{sp}(2l, F)$ *(o bien* $\mathfrak{sp}(V)$*) se dice que es un álgebra de Lie clásica de tipo* C_l*. Estas álgebras tienen dimensión* $2l^2 + l$*.*

Consideremos finalmente un F-espacio vectorial V de dimensión $2l$[4] provisto de una forma bilineal simétrica no degenerada f cuya matriz respecto de cierta base B es

$$f' = \begin{pmatrix} 0 & 1_l \\ 1_l & 0 \end{pmatrix}.$$

Podemos considerar entonces el conjunto de endomorfismos $x \in \mathfrak{gl}(V)$ que satisfacen la condición

$$f(x(v), w) = -f(v, x(w)),$$

para cualesquiera $v, w \in V$. Ese conjunto de endomorfismos es en realidad una subálgebra de $\mathfrak{gl}(V)$, que se denotará también de la forma $\mathfrak{o}(V)$. Dejamos al lector determinar la forma de las matrices que representan a estos endomorfismos respecto de la base B. Digamos, eso sí, que este álgebra tiene dimensión $2l^2 - l$.

Definición 11 *El álgebra de Lie* $\mathfrak{o}(2l, F)$ *(o bien* $\mathfrak{o}(V)$*) de dice que es un álgebra de Lie clásica de tipo* D_l*. Como se sabe, estas álgebras son isomorfas y tiene dimensión* $2l^2 - l$*.*

4.2. Otras álgebras de Lie.

Otros ejemplos muy interesantes de álgebras de Lie son las álgebras de Lie de derivaciones. Si A es una F-álgebra, se define una derivación como una aplicación F-lineal $D : A \to A$ tal que

$$D(xy) = D(x)y + xD(y)$$

para cualesquiera $x, y \in A$. El conjunto

$$\mathrm{Der}(A) := \{D \in \mathrm{End}_F(A) : D \text{ es una derivación } \}$$

es una subálgebra de $\mathfrak{gl}(A)$. El punto clave para demostrar esto radica en que el corchete $[D_1, D_2] = D_1D_2 - D_2D_1$ de dos derivaciones, vuelve a ser una derivación (véase el problema 63).

Por último debemos citar otras álgebras de Lie de matrices que serán importantes para nosotros. Todas ellas son subálgebras del álgebra de Lie $\mathfrak{gl}(n, F)$. La primera de ellas es el álgebra $\tau(n, F)$ que es la subálgebra de $\mathfrak{gl}(n, F)$ de las matrices triangulares superiores, es decir, matrices (a_{ij}) tales que $a_{ij} = 0$ si $i > j$. La segunda es el álgebra $\mathfrak{n}(n, F)$ que es el álgebra de matrices triangulares superiores estrictas (es decir, $a_{ij} = 0$ si $i \geq j$), y por último, el álgebra $\mathfrak{d}(n, F)$ de todas las matrices diagonales. El lector puede hacer el ejercicio 65 donde se pide establecer algunas relaciones entre estas álgebras.

Un caso especialmente interesante es el de las derivaciones de las *álgebras de Jordan*. Supongamos que J es un álgebra de Jordan con unidad sobre un cuerpo F. Por definición

[4]Recordemos que el cuerpo base F sigue siendo de característica distinta de dos.

esto quiere decir que J es un F-espacio vectorial provisto de un operador $U : J \to \mathrm{End}_F(J)$ tal que $a \mapsto U_a$, de modo que

(1) $U_{tx} = t^2 U_x$ para $t \in F$, $x \in J$.

(2) Para cualquiera $a, b \in J$, La aplicación $U_{a,b} := U_{a+b} - U_a - U_b$ es bilineal simétrica).

Se deben satisfacer además las siguientes identidades (así como sus linealizaciones):

1. $U_1 = 1_J$,
2. $U_x V_{y,x} = V_{x,y} U_x = U_{U_x(y),x}$,
3. $U_{U_x(y)} = U_x U_y U_x$,

donde $V_{x,y} z := U_{x,z}(y)$ para cualesquiera $x, y \in J$. En este caso se define una derivación como una aplicación $D : J \to J$ tal que $[D, U_x] = U_{D(x),x}$ para cada $x \in J$. Queremos comprobar que el conjunto $\mathrm{Der}(J)$ formado por todas las derivaciones es una subálgebra de Lie de $\mathfrak{gl}(J)$. Para ello bastará demostrar que $[D, D'] \in \mathrm{Der}(J)$ para cualesquiera $D, D' \in \mathrm{Der}(J)$. Vamos a necesitar calcular el corchete $[D, U_{a,b}]$ que no es otra cosa que

$$[D, U_{a,b}] = [D, U_{a+b}] - [D, U_a] - [D, U_b] = U_{D(a+b),a+b} - U_{D(a),a} - U_{D(b),b} =$$

$$= U_{D(a),b} + U_{D(b),a}.$$

Aplicando esta igualdad (junto con la identidad de Jacobi), tenemos:

$$[[D, D'], U_x] = -[[D', U_x]D] - [[U_x, D], D'] = -[U_{D'(x),x}, D] + [U_{D(x),x}, D'] =$$

$$= U_{D(D'(x)),x} + U_{D'(x),D(x)} - U_{D'(D(x)),x} - U_{D(x),D'(x)} = U_{[D,D'](x),x}.$$

Esto prueba que $\mathrm{Der}(J)$ es un álgebra de Lie.

4.3. Representaciones.

Una *representación* de una F-álgebra de Lie L es un homomorfismo $\phi : L \to \mathfrak{gl}(V)$. El espacio V se llama el *espacio de la representación*. Una de las nociones más interesantes es la de representación adjunta. Esta viene dada por la aplicación $\mathrm{ad} : L \to \mathfrak{gl}(L)$ donde para cada $x \in L$, la aplicación $\mathrm{ad}(x) : L \to L$ se define como $\mathrm{ad}(x)y := [x, y]$ para cada $y \in L$. Para comprobar que ciertamente se trata de una representación de L tenemos que demostrar que $\mathrm{ad}([x, y]) = [\mathrm{ad}(x), \mathrm{ad}(y)]$ para cualesquiera elementos $x, y \in L$. Pero para cada $z \in L$ se tiene:

$$[\mathrm{ad}(x), \mathrm{ad}(y)]z = \mathrm{ad}(x)\,\mathrm{ad}(y)z - \mathrm{ad}(y)\,\mathrm{ad}(x)z = [x, [y, z]] - [y, [x, z]] =$$

$$= [x, [y, z]] + [y, [z, x]] = -[z, [x, y]] = [[x, y], z] = \mathrm{ad}([x, y])z,$$

lo que demuestra la igualdad requerida.

Si no planteamos cuál es el núcleo de la representación adjunta, veremos enseguida que se trata del conjunto de elementos $x \in L$ tales que $[x, L] = 0$. Este conjunto se denominará el *centro* de L y se denotará por $\mathrm{Z}(L)$. El centro es visiblemente un ideal de L. Esto tiene una consecuencia inmediata: si L es simple, $\mathrm{Z}(L) = 0$ y entonces la representación adjunta es un monomorfismo. En consecuencia, *toda álgebra de Lie simple es isomorfa a un álgebra de Lie de aplicaciones lineales*[5].

El concepto de representación se puede ver desde la óptica de los módulos. Sea L una F-álgebra de Lie, entonces un F-espacio vectorial V provisto de una aplicación $L \times V \to V$ tal que $(x, v) \mapsto xv$, se dice que es un *L-módulo* si se satisfacen las identidades:

1) $(x + x')v = xv + x'v$, $\forall x, x' \in L$, $\forall v \in V$.

2) $x(v + v') = xv + xv'$, $\forall x \in L$, $\forall v, v' \in V$.

3) $(\lambda x)v = \lambda(xv) = x(\lambda v)$, $\forall \lambda \in F$, $\forall x \in L$, $\forall v \in V$.

4) $[x, x']v = x(x'v) - x'(xv)$, $\forall x, x' \in L$, $\forall v \in V$.

Las nociones de representación y de módulo para un álgebra de Lie L son equivalentes. Así si $\phi : L \to \mathfrak{gl}(V)$ es una representación, entonces V es un L-módulo definiendo $L \times V \to V$ mediante $xv := \phi(x)(v)$. Recíprocamente, si partimos de un L-módulo V, entonces definiendo $\phi : L \to \mathfrak{gl}(V)$ por la igualdad $\phi(x)(v) := xv$ se tiene una representación.

Ahora que tenemos definidos módulos sobre álgebras de Lie, podemos dar la definición de homomorfismo de L-módulos. Así, si L es una F-álgebra, y tenemos ciertos L-módulos V y W, un *homomorfismo de V a W* no será más que una aplicación F-lineal $f : V \to W$, tal que $f(xv) = xf(v)$ para todos $x \in L$, $v \in V$. Se puede considerar entonces la categoría de L-módulos con las definiciones obvias y resaltar el hecho de que las nociones categóricas habituales tienen aquí perfecto sentido (núcleos, imágenes, submódulos, módulos cocientes, teoremas de isomorfía, etc).

Definición 12 *Dos representaciones $\phi : L \to \mathfrak{gl}(V)$, $\phi' : L \to \mathfrak{gl}(V')$ se dicen* equivalentes *cuando los L-módulos asociados V y V' son isomorfos. Un L-módulo V no nulo se dice* irreducible *si tiene exactamente dos submódulos: 0 y V. Un L-módulo V se dice* completamente reducible *si V es una suma directa de L-módulos irreducibles.*

4.4. Álgebras de Lie solubles y nilpotentes.

Dada una F-álgebra de Lie L, podemos construir lo que se llama la *serie derivada* definiendo $L^{(0)} = L$, $L^{(1)} = [L, L]$, $L^{(i)} = [L^{(i-1)}, L^{(i-1)}]$, etc. Diremos que L es *soluble* cuando existe un i tal que $L^{(i)} = 0$. Por ejemplo las álgebras de Lie abelianas (todo corchete es nulo) son evidentemente solubles. Sin embargo las álgebras de Lie simples no pueden ser solubles. El lector puede demostrar (véase el problema 72) que el álgebra $\tau(n, F)$ de las matrices triangulares superiores es soluble.

[5]Este es un resultado que contrasta con el que se tiene en teoría de álgebras de Jordan, donde existen álgebras simples no sumergibles en álgebras simetrizadas de álgebras asociativas.

Proposición 11 *Sea L un álgebra de Lie.*

1. *Si L es soluble, entonces cada subálgebra y cada imagen homomórfica de L es soluble.*
2. *Si I es un ideal soluble de L tal que L/I es soluble, entonces L es soluble.*
3. *Si I y J son ideales solubles de L, entonces $I + J$ es soluble.*

Dem. Sea L soluble y K una subálgebra suya. Es inmediato comprobar que $K^{(i)} \subset L^{(i)}$ para cada i. Por tanto una subálgebra de un álgebra soluble es siempre soluble. Sea ahora $\phi : L \to M$ un epimorfismo con L soluble. Es evidente que $M^{(0)} = \phi(L^{(0)})$. Si suponemos que $M^{(i)} = \phi(L^{(i)})$, entonces

$$M^{(i+1)} = [M^{(i)}, M^{(i)}] = [\phi(L^{(i)}), \phi(L^{(i)})] = \phi([L^{(i)}, L^{(i)}]) = \phi(L^{(i+1)})$$

lo que demuestra que para todo n se tiene $M^{(n)} = \phi(L^{(n)})$ y por tanto si L es soluble, también lo es M. Esto demuestra el primer apartado de la proposición. Veamos el segundo. Supongamos que $(L/I)^{(n)} = 0$, sea $\pi : L \to L/I$ la proyección canónica. Como $\pi(L^{(n)}) = (L/I)^{(n)} = 0$ tenemos entonces $L^{(n)} \subset \ker(\pi) = I$. Al ser I soluble, debe ser $I^{(m)} = 0$ para cierto m. Pero entonces $(L^{(n)})^{(m)} \subset I^{(m)} = 0$ y como $(L^{(n)})^{(m)} = L^{(n+m)}$ hemos demostrado que L es soluble. Finalmente demostremos que $I + J$ es soluble cuando I y J lo son. evidentemente $J/I \cap J$ es soluble al ser imagen epimórfica de J. Pero

$$\frac{I + J}{I} \cong \frac{J}{I \cap J}$$

lo que implica que $I + J/I$ es soluble y como I lo es, el segundo apartado de la proposición implica que $I + J$ es soluble. ■

Esta proposición tiene una aplicación inmediata. Supongamos que un álgebra de Lie L tiene un ideal soluble maximal[6] S. Entonces si tomamos otro ideal soluble I, se tiene de inmediato que $I + S$ es soluble por la proposición anterior. La maximalidad de S implica entonces que $S = I + S$ y por tanto $I \subset S$. En consecuencia el ideal soluble contiene a todos los ideales solubles de L. Esto implica que S es único. Si por ejemplo L es de dimensión finita, está asegurada la existencia de un ideal soluble de dimensión máxima (por tanto maximal). Esto demuestra la existencia de un único ideal soluble maximal que llamaremos el *radical* de L y denotaremos por $\mathrm{Rad}(L)$. Cuando $\mathrm{Rad}(L) = 0$ diremos que L es *semisimple* (por ejemplo un álgebra de Lie simple de dimensión finita es semisimple).

Teorema 15 *Sea L un álgebra de Lie con radical $Rad(L)$. Entonces*

$$Rad(L/Rad(L)) = 0.$$

[6]Es decir, un elemento maximal en la familia de los ideales solubes del álgebra.

Dem. Si tomamos un ideal soluble de $L/\mathrm{Rad}(L)$, dicho ideal es de la forma $U/\mathrm{Rad}(L)$ donde U es un ideal de L que contiene a $\mathrm{Rad}(L)$. Ahora bien, como el cociente $U/\mathrm{Rad}(L)$ es soluble y $\mathrm{Rad}(L)$ también, aplicando el segundo apartado de la proposición precedente, tendremos que U es soluble luego $U \subset \mathrm{Rad}(L)$ implicando $U/\mathrm{Rad}(L) = 0$. Así, el único ideal soluble de $L/\mathrm{Rad}(L)$ es el nulo, lo que implica la nulidad de su radical. ■

Comencemos ahora el estudio de las álgebras de Lie nilpotentes. Para ello partiremos de un álgebra de Lie L y definiremos lo que se llama la *serie central descendente* escribiendo: $L^0 = L$, $L^1 = [L, L]$, $L^2 = [L, L^1]$, y en general $L^i = [L, L^{i-1}]$. Se dirá que L es *nilpotente* si existe un i tal que $L^i = 0$. Por ejemplo cada álgebra de Lie abeliana es nilpotente. Claramente se tiene $L^{(i)} \subset L^i$ así es que la nilpotencia implica la solubilidad de un álgebra. El recíproco es falso como puede verse en cualquiera de los problemas 73 o 74 al final de este capítulo.

Proposición 12 *Sea L un álgebra de Lie.*

(a) Si L es nilpotente, toda subálgebra y toda imagen homomórfica de L, lo es.

(b) Si $L/\,Z(L)$ es nilpotente, entonces L lo es.

(c) Si $L \neq 0$ es nilpotente, entonces su centro $Z(L)$ es no nulo.

Dem. El primer apartado se demuestra como el correspondiente apartado de la Proposición 11. Demostremos el segundo apartado. Si $L/\,\mathrm{Z}(L)$ es nilpotente, existe un n tal que $0 = (L/\,\mathrm{Z}(L))^n$, equivalentemente $L^n \subset \mathrm{Z}(L)$. Entonces $L^{n+1} = [L, L^n] = 0$ luego L es nilpotente. Demostremos por fin el último apartado. Sea L nilpotente y no nula. Si suponemos $L^k = 0$, $L^{k-1} \neq 0$ (con $k \geq 0$) entonces $[L, L^{k-1}] = 0$ lo que implica que $0 \neq L^{k-1} \subset \mathrm{Z}(L)$. En consecuencia el centro es no nulo.■

Definición 13 *Un elemento x de un álgebra de Lie L se dice* ad*-nilpotente cuando el operador* $\mathrm{ad}(x) \in \mathfrak{gl}(L)$ *es nilpotente.*

Lema 14 *Si $x \in \mathfrak{gl}(V)$ es nilpotente, entonces* $\mathrm{ad}(x)$ *es un operador nilpotente.*

Dem. Consideremos los endomorfismos $L_x : a \mapsto xa$ y $R_x : a \mapsto ax$ del espacio vectorial $\mathfrak{gl}(V)$. Es evidente que $L_x^n = L_{x^n}$, $R_x^n = R_{x^n}$ para cada entero $n \geq 0$. En consecuencia los operadores L_x y R_x son nilpotentes. Pero $\mathrm{ad}(x) = L_x - R_x$ y en todo anillo asociativo (en nuestro caso el anillo de endomorfismo del espacio $\mathfrak{gl}(V)$), la suma o diferencia de elementos nilpotentes que conmutan, es de nuevo un elemento nilpotente. Esto demuestra que $\mathrm{ad}(x)$ es nilpotente.■

Para demostrar el Teorema de Engel que asegura el carácter nilpotente de toda álgebra de Lie finito-dimensional en la que cada x sea ad-nilpotente, necesitaremos el siguiente resultado que tiene también un interés intrínseco.

Teorema 16 *Sea L una subálgebra de $\mathfrak{gl}(V)$ (con $V \neq 0$ de dimensión finita). Si todos los elementos de L son nilpotentes, entonces existe un $v \in V$ no nulo tal que $L(v) = 0$ (es decir, $x(v) = 0$, $\forall x \in L$).*

Dem. Procedemos por inducción sobre $\dim(L)$. Si esta dimensión es uno, y tomamos un generador $x \in L$ (necesariamente nilpotente), sabemos[7] que existe al menos un $v \in V$ no nulo tal que $x(v) = 0$. Supongamos entonces la propiedad demostrada para todas las álgebras de dimensión menor que la de L (que estén en las hipótesis adecuadas). Tomemos una subálgebra propia $K \neq L$ y dejemos que K actúe vía la representación adjunta sobre L. En otras palabras, consideraremos la acción $K \to \mathfrak{gl}(L)$ tal que a cada $x \in K$ le asocia el operador $\mathrm{ad}(x) : L \to L$. Como todos los elementos de L son nilpotentes, el Lema 14 implica que las aplicaciones lineales $\mathrm{ad}(x)$ son todas nilpotentes. También podemos considerar la representación $\rho : K \to \mathfrak{gl}(L/K)$ que asocia a cada $x \in K$ la aplicación lineal $\rho(x) : L/K \to L/K$ dada por $\rho(x)(y+K) := \mathrm{ad}(x)y+K$. Entonces $\rho(K)$ es una subálgebra de $\mathfrak{gl}(L/K)$ formada por elementos nilpotentes y como $\dim(\rho(K) \leq \dim(K) < \dim(L)$ podemos aplicar la hipótesis de inducción para concluir que existe un $x + K \neq K$ en L/K tal que $\rho(K)(x + K) = K$. Equivalentemente $[K, x] \subset K$ (pero $x \notin K$). Definamos $N_L(K) = \{a \in L : [K, a] \subset K\}$. Este conjunto[8] es una subálgebra de L que contiene a K. Como $x \in N_L(K)$, $x \notin K$, tenemos que $N_L(K)$ contiene estrictamente a K. Si elegimos a K como una subálgebra propia *maximal*, el contenido $K \subset N_L(K)$ implica $L = N_L(K)$ lo que quiere decir que K es un ideal de L. Vamos a demostrar que $\dim(L/K) = 1$. Razonemos por reducción al absurdo suponiendo que $\dim(L/K) > 1$. En toda álgebra de Lie no nula existen subálgebras de dimensión uno (basta considerar el subespacio generado por un elemento no nulo). Si consideramos una subálgebra de dimensión uno U/K de L/K entonces U sería una subálgebra de L que contiene a K (en contra del carácter maximal de la subálgebra propia K). En consecuencia L/K tiene dimensión uno. Podemos escribir $L = K + Fz$ (siendo F el cuerpo base, y z un elemento fuera de K).

Trabajemos ahora con el conjunto $W = \{v \in V : K(v) = 0\}$. Este espacio es no nulo por la hipótesis de inducción, y como K es un ideal de L entonces $L(W) \subset W$. En efecto: si $x \in L$, $w \in W$, $k \in K$ entonces $k(x(w)) = x(k(w)) + [k, x](w)$ y como $k(w) = 0$ tenemos $k(x(w)) = [k, x](w) \in K(w) = 0$. En consecuencia $x(w) \in W$ para cualesquiera $x \in L$, $w \in W$. Retomemos nuestro elemento z (fuera de K) que es nilpotente (como todo elemento de L). Sea $v \in W$ no nulo tal que $z(v) = 0$. Como $K(v) = 0$ tenemos $L(v) = 0$ (siendo $L = K + Fz$).■

Teorema 17 (Teorema de Engel). *Sea L un álgebra de Lie de dimensión finita. Si todos los elementos de L son* ad*-nilpotentes, entonces L es nilpotente.*

Dem. Podemos suponer de entrada que $L \neq 0$. Todos los elementos del álgebra de Lie $\mathrm{ad}(L) \subset \mathfrak{gl}(L)$ son nilpotentes, luego aplicando el Teorema 16 existe un elemento no nulo

[7] Si $x^k = 0$ y $x^{k-1} \neq 0$ existe un u tal que $x^{k-1}(u) \neq 0$ pero necesariamente $x^k(u) = 0$. Entonces podemos v como $x^{k-1}(u)$.

[8] Denominado *normalizador de K en L*.

$x \in L$ tal que $[L, x] = 0$. En consecuencia el centro $\mathrm{Z}(L)$ es no nulo y podemos considerar $L/\mathrm{Z}(L)$ cuyos elementos son todos ad-nilpotentes. Usando inducción sobre $\dim(L)$ tenemos que $L/\mathrm{Z}(L)$ es nilpotente y la segunda parte de la Proposición 12 implica que L es nilpotente.■

Definición 14 *Sea V un F-espacio de dimensión finita n. Una cadena de subespacios*

$$0 = V_0 \subset V_1 \subset \cdots \subset V_n = V$$

se dice que un flag *de subespacios si* $\dim(V_i) = i$ *para cada i. Un elemento $x \in End(V)$ que dice que* estabiliza *este flag (o que el flag* es estable *por x) cuando $x(V_i) \subset V_i$ para cada i.*

Corolario 8 *Sea L una subálgebra de $\mathfrak{gl}(V)$, siendo $V \neq 0$ un F-espacio de dimensión finita. Si todos los elementos de L son nilpotentes, existe un flag $\{V_i\}_{i=1}^n$ de V estable por L.*

Dem. Empecemos tomando un elemento no nulo v al que $L(v) = 0$. Definamos $V_1 = Fv$. Hagamos $W = V/V_1$ y observemos que la acción inducida σ de L sobre V/V_1, tal que $\sigma(x) : V/V_1 \to V/V_1$, con $\sigma(x)(v + V_1) := x(v) + V_1$, verifica que $\sigma(x)$ es un endomorfismo nilpotente de V/V_1. Aplicando la hipótesis de inducción, V/V_1 tiene un flag estable por $\sigma(L)$. A partir de aquí, no es difícil construir un flag de V estable por L. ■

Una observación importante que conviene hacer llegado este punto es la siguiente. Si $L \subset \mathfrak{gl}(V)$ es nilpotente y V de dimensión finita, existe una base B de V respecto a la cual todo $x \in L$ se representa por una matriz triangular estricta respecto a B. Esto es una consecuencia del último corolario. En particular todos los $x \in L$ son nilpotentes. Recíprocamente, si $L \subset \mathfrak{gl}(V)$ con $\dim(V)$ finita y todo $x \in L$ es nilpotente, entonces todo $x \in L$ es ad-nilpotente y por el Teorema de Engel, L es nilpotente. Tenemos así una sencilla caracterización de las subálgebras nilpotentes de $\mathfrak{gl}(V)$ cuando V es de dimensión finita.

Como aplicación del Teorema de Engel, establezcamos finalmente un resultado que nos resultará de utilidad más adelante.

Lema 15 *Sea L un álgebra de Lie nilpotente de dimensión finita, K un ideal de L no nulo. Entonces $K \cap Z(L) \neq 0$.*

Dem. Hagamos actuar L sobre K por medio de la representación adjunta. Tenemos entonces $\mathrm{ad} : L \to \mathfrak{gl}(K)$ y aplicando el Teorema 16 existe un elemento no nulo $v \in K$ anulado por cada $\mathrm{ad}(x)$ (para cada $x \in L$). Por tanto v es un elemento no nulo de $K \cap \mathrm{Z}(L)$.

4.5. Problemas.

Problema 59 *Estúdiense las álgebras de Lie nilpotentes de dimensiones dos y tres.*

Problema 60 *Demuéstrese que para un álgebra alternativa A sobre un cuerpo F de característica dos o tres, el álgebra antisimetrizada A^- es de Lie.*

Problema 61 *Sea V un F-espacio vectorial de dimensión finita n. ¿Bajo qué condiciones podemos afirmar que $\mathfrak{gl}(V)/F1 \cong \mathfrak{sl}(V)$?*

Problema 62 *Demuéstrese la simplicidad de las álgebras $\mathfrak{sl}(V)$ para un espacio vectorial de dimensión finita V.*

Problema 63 *Demuéstrese que si A es un álgebra y $D_1, D_2 \in Der(A)$, entonces $[D_1, D_2] \in Der(A)$.*

Problema 64 *Determínese la dimensión del álgebra $\mathfrak{o}(2l+1, F)$.*

Problema 65 *Verifíquese que:*

1. $\tau(n, F) = \mathfrak{d}(n, F) \oplus \mathfrak{n}(n, F)$.
2. $[\mathfrak{d}(n, F), \mathfrak{n}(n, F)] = \mathfrak{n}(n, F)$.
3. $[\tau(n, F), \tau(n, F)] = \mathfrak{n}(n, F)$.

Recuérdese que si K y H son subálgebras de L, entonces $[H, K]$ denota el subespacio de L generado por los conmutadores $[x, y]$ con $x \in H$, $y \in K$.

Problema 66 *Sea 1 la identidad de $\mathfrak{gl}(n, F)$. Supongamos que la característica de F es cero o un primo que no divida a n. Demuéstrese que $\mathfrak{gl}(n, F) = F \cdot 1 \oplus \mathfrak{sl}(n, F)$ (suma directa de subespacios).*

Problema 67 *Demuéstrese que el espacio vectorial real $\mathbb{R}^3$ provisto con el producto vectorial habitual, tiene estructura de álgebra de Lie.*

Problema 68 *Cuando la característica del cuerpo base F es cero, demuéstrese que para cada una de las álgebras de Lie clásicas $L = A_l, B_l, C_l$, o D_l, se tiene la igualdad $[L, L] = L$. Conclúyase que cada una de estas álgebras está formada por matrices de traza nula.*

Problema 69 *Sea L un álgebra de Lie sobre un cuerpo algebraicamente cerrado y sea $x \in L$. Pruébese que el subespacio de L generado por los vectores propios de $\mathrm{ad}(x)$ es una subálgebra.*

Problema 70 *Para valores pequeños de l, pueden darse isomorfismos entre algunas álgebras de Lie clásicas. Demuéstrese que A_1, B_1 y C_1 son isomorfas, mientras que D_1 es un álgebra de Lie unidimensional. Pruébese que $B_2 \cong C_2$, $D_3 \cong A_3$. ¿Qué se puede decir de D_2?*

Problema 71 *Demuéstrese que una representación de dimensión finita V de un álgebra de Lie L es completamente reducible si y sólo si para cada L-submódulo W de V, existe un L-submódulo W' tal que $V = W \oplus W'$. Indicación. Supongamos $V = \oplus_{i=1}^{n} V_i$ completamente reducible siendo cada V_i un submódulo irreducible. Sea W submódulo distinto del total, entonces existe algún i tal que $W \cap V_i = 0$. A partir de aquí se demuestra la existencia de un submódulo W' maximal de entre los que tiene intersección nula con W. Para demostrar que $W \oplus W'$ coincide con V se puede razonar por reducción al absurdo en cuyo caso llegaremos a que existe j tal que $(W \oplus W') \cap V_j = 0$.*

Problema 72 *Demuéstrese que el álgebra $\tau(n, F)$ de las matrices triangulares superiores es soluble.*

Problema 73 *Compruébese que el álgebra tridimensional con base $\{x, y, z\}$ y tabla de multiplicar $[x, x] = [y, y] = [z, z] = 0$, $[x, y] = -[y, x] = z$, $[x, z] = -[z, x] = y$, $[y, z] = [z, y] = 0$, es un álgebra de Lie. Demuéstrese que es soluble pero no nilpotente.*

Problema 74 *Determínense salvo isomorfismos las álgebra de Lie de dimensión menor o igual a dos. Compruébese que existe solo una (salvo isomorfismo) bidimensional no abeliana. Compruébese que esta es soluble pero no nilpotente.*

Capítulo 5

Álgebras de Lie semisimples

En el capítulo anterior solo hemos demostrado un resultado verdaderamente sustancioso: el Teorema de Engel. En este capítulo demostraremos algunos más para los cuales tendremos que imponer la condición de que el cuerpo base sea algebraicamente cerrado y de característica cero.

5.1. Teoremas de Lie y de Cartan.

En esencia el teorema de Engel establece la existencia de un vector propio común para un álgebra de Lie de endomorfismos nilpotentes. El teorema que demostraremos a continuación establece un resultado similar.

Teorema 18 *Sea L una F-subálgebra soluble de $\mathfrak{gl}(V)$, siendo $V \neq 0$ un F-espacio de dimensión finita, entonces V tiene un vector propio común para todos los endomorfismos de L.*

Dem. Procederemos por inducción sobre L. Para $\dim(L) = 0$ el asunto es trivial. Vamos a intentar imitar la demostración del Teorema 16. La idea es:

i) Localizar un ideal K de codimensión uno.

ii) Demostrar por inducción que existe un vector propio común para los endomorfismos de K.

iii) Verificar que L deja fijo un espacio de vectores propios de los dados en el punto anterior.

iv) Encontrar en el espacio anterior un vector propio para un $z \in L$ tal que $L = K + Fz$.

El primer apartado es fácil. Como L es soluble y de dimensión positiva, entonces contiene de forma propia a $[L, L]$. La F-álgebra $L/[L, L]$ es abeliana y por tanto cualquier subespacio suyo es automáticamente un ideal. Tomemos un tal subespacio de codimensión uno.

Sabemos que dicho subespacio es de la forma $K/[L,L]$ donde K es un ideal de L que contiene a $[L,L]$. Entonces

$$1 = \operatorname{codim}(K/[L,L]) = \dim(L/[L,L]) - \dim(K/[L,L]) = \dim(L) - \dim(K)$$

lo que demuestra que K es un ideal de L de codimensión uno (y que contiene a $[L,L]$).

Veamos el segundo apartado. Queremos aplicar la hipótesis de inducción a K. Si $K = 0$ entonces L es de dimensión uno. Cualquier vector propio de un generador de L acaba la demostración en este caso. Si $K \neq 0$ como es soluble al ser un ideal de L, podemos asegurar la existencia de un vector propio para todos los elementos de K. En definitiva si v es dicho vector propio, se tiene $x(v) = \lambda(x)v$ para cada $x \in K$. Hemos definido entonces una aplicación $\lambda : K \to F$ que es lineal como se puede comprobar sin dificultad. Denotemos por W el siguiente subespacio de V:

$$W = \{w \in V : x(w) = \lambda(x)w, \forall x \in K\}.$$

Como consecuencia de lo anterior $W \neq 0$.

Veamos el tercer apartado, es decir, queremos demostrar que L deja fijo el espacio W. Sea $w \in W$, $x \in L$, para demostrar que $x(w) \in W$ debemos ver que para cada $y \in K$ se tiene $y(x(w)) = \lambda(y)x(w)$. Pero $y(x(w)) = x(y(w)) + [y,x](w) = x(\lambda(y)w) - \lambda([x,y])w$. Por tanto nos vemos obligados a demostrar que $\lambda([x,y]) = 0$ para cualesquiera $x \in L$, $y \in K$. Para demostrar esto, fijemos $w \in W$, $x \in L$. Sea $n > 0$ el menor entero tal que $w, x(w), \ldots, x^n(w)$ son linealmente dependientes. Denotemos por W_i el subespacio de V generado por $w, x(w), \ldots, x^{i-1}(w)$ (siendo $W_0 = 0$). De este modo se tiene $\dim(W_n) = n$, $W_{n+1} = W_n$. Obviamente $x(W_n) \subset W_n$, veamos que cada $y \in K$ deja W_i invariante. Sea $0 \leq j \leq i-1$, entonces

$$y(x^j(w)) = x^j(y(w)) + [y, x^j](w) = \lambda(y)x^j(w) + [y, x^j](w),$$

para $j = 1$ la igualdad anterior nos dice que $y(x(w)) = \lambda(y)x(w) + \lambda([y,x])w \in W_i$. Suponiendo demostrado que $K(x^j(w)) \in W_i$, veamos lo que ocurre con $y(x^{j+1}(w))$:

$$y(x^{j+1}(w)) = y(x(x^j(w))) = x(y(x^j(w))) + [y,x](x^j(w))$$

y como $y(x^j(w)) \in W_i$ tendremos $x(y(x^j(w))) \in W_i$. Por otra parte como $x^j(w) \in W_i$, $[y,x] \in K$, tendremos $[y,x](x^j(w)) \in K(x^j(w)) \in W_i$. En definitiva se tiene $K(W_i) \subset W_i$. Demostremos ahora que

$$y(x^i(w)) = \lambda(y)x^i(w) (\text{mod } W_i). \tag{5.1}$$

Hagamos inducción sobre i. El caso $i = 0$ es trivial. Por otra parte

$$y(x^i(w)) = y(x(x^{i-1}(w))) = x(y(x^{i-1}(w))) + [y,x](x^{i-1}(w)). \tag{5.2}$$

Por inducción $y(x^{i-1}(w)) = \lambda(y)x^{i-1}(w) + w'$ siendo w' un elemento de W_{i-1}. Además x transforma W_{i-1} en W_i y siendo $[y,x] \in K$ se tiene $[y,x](x^{i-1}(w)) \in K(W_i) \subset W_i$. Esto demuestra la congruencia (5.1). Acabemos ahora la demostración de que $\lambda([x,y]) = 0$. Para

ello tengamos en cuenta que si $y \in K$, entonces (5.1) implica que la traza de y restringido a W_n es precisamente $n\lambda(y)$. En particular para cada x la traza de $[x, y]$ (restringida a W_n, y con $y \in K$) es $n\lambda([x, y])$. Pero como tanto x como y dejan invariante a W_n se tiene que $[x, y]|_{W_n} = [x|_{W_n}, y|_{W_n}]$ y sabemos que la traza de un conmutador es nula. En consecuencia $n\lambda([x, y]) = 0$ lo que implica en un cuerpo de característica nula que $\lambda([x, y]) = 0$.

Por último, abordemos la demostración del cuarto apartado. Tomemos un $z \in L$ tal que $L = K + Fz$. Como F es algebraicamente cerrado existe un vector propio $w_0 \in W$ de z (se aplica aquí el hecho de que W es invariante por cada elemento de L). Obviamente este w_0 es un vector propio común a todo L (y λ se puede extender a un aplicación lineal $\lambda : L \to F$ tal que $x(w_0) = \lambda(x)w_0$ para todo $x \in L$). ■

Corolario 9 (Teorema de Lie). *Sea L una subálgebra soluble de $\mathfrak{gl}(V)$ donde V es de dimensión finita. Entonces L deja fijo algún flag de V (en otras palabras, las matrices de L respecto a una base adecuada son triangulares).*

Dem. Si la dimensión de V es nulo, el resultado es trivial. Supongamos la propiedad cierta cuando la dimensión de V es menor que n. Tomemos un vector propio común $w_0 \in V$ para L. Consideremos la F-álgebra $\bar{L} = \{\bar{x} : x \in L\}$ donde $\bar{x} : V/Fw_0 \to V/Fw_0$ se obtiene por paso al cociente de x, es decir, $\bar{x}(v + Fw_0) = x(v) + Fw_0$. Se demuestra entonces que $\bar{L}$ es soluble (y evidentemente es subálgebra de $\mathfrak{gl}(V/Fw_0)$. Aplicando la hipótesis de inducción tenemos un flag

$$0 = Fw_0/Fw_0 \subset V_1/Fw_0 \subset V_2/Fw_0 \subset \cdots V_n/Fw_0 = V/Fw_0$$

de V/Fw_0 que es estabilizado por $\bar{L}$. El lector puede demostrar ahora que

$$0 \subset Fw_0 \subset V_1 \subset \cdots \subset V_n = V$$

es un flag de V estabilizado por L. ■

La situación del corolario anterior se puede aplicar a una representación finito-dimensional $\phi : L \to \mathfrak{gl}(V)$ de un álgebra soluble L. Como es natural $\phi(L)$ es una subálgebra soluble de $\mathfrak{gl}(V)$ (aplíquese el primer apartado de la Proposición 11). Entonces el teorema anterior implica la existencia de un flag de V estabilizado por $\phi(L)$. Si por ejemplo la representación considerada es la adjunta tenemos entonces un flag de L estabilizado por $\mathrm{ad}(L)$, es decir, una cadena de ideales de L cada uno de dimensión uno más que el anterior. Esto se puede enunciar del siguiente modo:

Corolario 10 *Sea L un álgebra de Lie soluble y de dimensión finita. Entonces existe una cadena de ideales de L:*

$$0 = L_0 \subset L_1 \subset \cdots \subset L_n = L$$

tal que $\dim(L_i) = i$.

Corolario 11 *Sea L soluble y de dimensión finita. Entonces, si $x \in [L,L]$ la aplicación* $\mathrm{ad}(x) : L \to L$ *es nilpotente. En particular $[L,L]$ es nilpotente.*

Dem. Consideremos un flag de ideales como en el corolario anterior. Tomemos una base $B = \{x_1, \ldots, x_n\}$ de L tal que cada subconjunto $\{x_1, \ldots, x_i\}$ sea base de L_i. Entonces las matrices de $\mathrm{ad}(L)$ respecto a la base B son elementos de $\tau(n, F)$. Esto implica que las matrices de $[\mathrm{ad}(L), \mathrm{ad}(L)] = \mathrm{ad}([L,L])$ son elementos de $\mathfrak{n}(n, F)$. En consecuencia $\mathrm{ad}(x)$ es nilpotente para cada $x \in [L,L]$ como queríamos demostrar. Aplicando el Teorema de Engel, $[L,L]$ es nilpotente. ■

5.2. Descomposición de Jordan-Chevalley.

En esta sección (y solo en ella), la característica del cuerpo base puede ser cualquiera, aunque seguiremos manteniendo la hipótesis de clausura algebraica del cuerpo F. Recordemos aquí la forma canónica de Jordan de un endomorfismo de un F-espacio vectorial de dimensión finita V. La forma canónica de Jordan estable la existencia de una base B respecto a la cual, la matriz del endomorfismo es diagonal por bloques, siendo cada bloque $n \times n$ del tipo

$$J_n(\lambda) := \begin{pmatrix} \lambda & 1 & \cdots & 0 \\ 0 & \lambda & 1 & \vdots \\ \vdots & \vdots & \ddots & 1 \\ 0 & 0 & \cdots & \lambda \end{pmatrix}, \quad (n > 1), \quad J_1(\lambda) = (\lambda)$$

donde los bloques de Jordan 1×1 son del tipo $J_1(\lambda) = (\lambda)$, y escapan necesariamente al modelo para $n > 1$.

Como la matriz $\mathrm{diag}(\lambda, \ldots, \lambda)$ conmuta con la matriz $J_n(0)$ (que es nilpotente), y $J_n(\lambda)$ es suma de las dos anteriores, podemos concluir que cada bloque de Jordan es suma de una matriz diagonal y otra nilpotente. Para generalizar estas ideas utilizaremos la siguiente definición:

Definición 15 *Sea V un espacio de dimensión finita sobre F . Sea $x \in \mathfrak{gl}(V)$ un endomorfismo. Diremos que x es* semisimple *si las raíces de su polinomio minimal son todas distintas.*

Si x es diagonalizable entonces evidentemente es semisimple. Recíprocamente si x es semisimple, como F es algebraicamente cerrado, los bloques de Jordan que aparecen en su forma canónica de Jordan deben ser de tamaño 1×1 ya que un bloque de Jordan de tamaño mayor tiene polinomio minimal con raíces múltiples. Recordemos que dos operadores semisimples que conmutan pueden ser simultáneamente diagonalizados (es decir, con respecto a la misma base). En consecuencia la suma de endomorfismos semisimples (que conmutan) es un endomorfismo semisimple. Por otra parte, si $x : V \to V$ es semisimple y W es un subespacio x-invariante de V, entonces la restricción $x|_W : W \to W$ es semisimple.

Proposición 13 *Sea V un espacio vectorial de dimensión finita sobre F y $x \in \mathfrak{gl}(V)$. Entonces:*

(a) Existen endomorfismos únicos $x_s, x_n \in \mathfrak{gl}(V)$, tales que $x = x_s + x_n$, $[x_s, x_n] = 0$, x_s es semisimple y x_n es nilpotente.

(b) Existen polinomios $p(T)$, $q(T)$ en una indeterminada, sin términos constantes, tales que $x_s = p(x)$, $x_n = q(x)$. En particular x_s y x_n conmutan con cualquier endomorfismo con el que conmute x.

(c) Si $A \subset B \subset V$ son subespacios y x transforma B en A, entonces x_s y x_n también transforman B en A.

Dem. Sea $\prod(T - a_i)^{m_i}$ la descomposición del polinomio característico de x, en factores primos. Sabemos que definiendo $V_i := \ker(x - a_i)^{m_i}$, entonces V es la suma directa de los distintos V_i, y la restricción de x a cada V_i tiene por polinomio característico $(T - a_i)^{m_i}$. Podemos aplicar el Teorema Chino del Resto en el anillo de polinomios $F[T]$ para encontrar un polinomio $p(T)$ que satisfaga las congruencias $p(T) \equiv a_i (\mathrm{mod}\ (T - a_i)^{m_i})$ y $p(T) \equiv 0 (\mathrm{mod}\ T)$. Nótese que la última congruencia es superflua si alguna de las raíces a_i es nula. $p(T)$ no tiene término constante por ser congruente con 0 módulo T. Definiendo $q(T) = T - p(T)$ tenemos otro polinomio sin término constante.

Hagamos ahora $x_s := p(x)$, $x_n = q(x) = x - p(x) = x - x_s$. Resulta entonces evidente que:

1. x_s y x_n conmutan con todo endomorfismo que conmute con x.
2. x_s y x_n dejan invariante cualquier subespacio que sea x-invariante.
3. La afirmación del apartado (c) en el enunciado del teorema que se está demostrando.

Para ver que x_s es semisimple y x_n nilpotente, procedamos del siguiente modo: como $p(T) \equiv a_i (\mathrm{mod}\ (T - a_i)^{m_i})$ se tiene que $x_s - a_i = p(x) - a_i$ se anula sobre V_i (ya que éste es el núcleo de $(x - a_i)^{m_i}$). En consecuencia x_s actúa diagonalmente sobre V_i con autovalor a_i. Por otra parte la forma canónica de Jordan de $x|_{V_i}$ está formada por bloques de Jordan del tipo $J_n(a_i)$ luego $x - x_s$ se representa matricialmente en determinada base como una matriz diagonal por bloques del tipo $J_n(0)$ lo que implica que $x_n = x - x_s$ es nilpotente.

Nos falta ver la unicidad de la descomposición $x = x_s + x_n$. Supongamos que podemos descomponer x de otra forma como una suma $x = s + n$ donde s es semisimple y n nilpotente. Entonces tanto s como n conmutan con x_s y con x_n. Como $x_s - s = n - x_n$ tenemos que un endomorfismo semisimple $x_s - s$ es igual a uno nilpotente $n - x_n$. Esto implica que $x_s - s = 0 = n - x_n$ y queda demostrada la unicidad. ■

Los endomorfismos x_s y x_n de la descomposición anterior reciben el nombre de *parte semisimple* y *parte nilpotente* de x. Esta descomposición se conoce con el nombre de *descomposición de Jordan-Chevalley* (o simplemente descomposición de Jordan) del endomorfismo x.

La descomposición de Jordan-Chevalley es una herramienta útil cuando se aplica en el siguiente ambiente: consideremos la representación adjunta del álgebra de Lie $\mathfrak{gl}(V)$ con V de dimensión finita. Si $x \in \mathfrak{gl}(V)$ es nilpotente, sabemos que $\mathrm{ad}(x)$ lo es (12). Análogamente, si x es semisimple, también $\mathrm{ad}(x)$ lo es (se pide demostrar esto en el problema 77 de esta sección.

Lema 16 *Sea $x \in \mathfrak{gl}(V)$ ($\dim(V) < \infty$), tal que $x = x_s + x_n$ es su descomposición de Jordan-Chevalley. Entonces $\mathrm{ad}(x) = \mathrm{ad}(x_s) + \mathrm{ad}(x_n)$ es la descomposición de Jordan-Chevalley de $\mathrm{ad}(x) : \mathfrak{gl}(V) \to \mathfrak{gl}(V)$.*

Dem. Ya sabemos que $\mathrm{ad}(x_s)$ y $\mathrm{ad}(x_n)$ son respectivamente semisimple y nilpotente. Además, estos operadores conmutan ya que $[\mathrm{ad}(x_s), \mathrm{ad}(x_n)] = \mathrm{ad}([x_s, x_n]) = 0$. ■

Lema 17 *Sea U una F-álgebra de dimensión finita. Entonces $Der(U)$ contiene las partes semisimples y nilpotentes de cada uno de sus elementos.*

Dem. Sea $\delta \in \mathrm{Der}(U)$ y sean $\sigma, \nu \in \mathfrak{gl}(V)$ sus partes semisimple y nilpotente. Tenemos además que U es la suma directa de los subespacios

$$U_a := \{x \in U : (\delta - a)^k x = 0 \ \exists k\}$$

tales que $a \in F$ es un autovalor de δ. El operador σ actúa sobre U_a como la multiplicación por el escalar a. Veamos ahora que $U_a U_b \subset U_{a+b}$. Para ello consideraremos la fórmula

$$(\delta - (a+b)1)^n(xy) = \sum_{i=0}^{n} \binom{n}{i} ((\delta - a1)^{n-i}x)((\delta - b1)^i y),$$

para $x, y \in U$. Si tomamos ahora $x \in U_a$, $y \in U_b$, entonces $\sigma(xy) = (a+b)xy$. Por otra parte $\sigma(x)y + x\sigma(y) = (a+b)xy$ lo que unido a lo anterior demuestra que $\sigma \in \mathrm{Der}(U)$. Como $\nu = \delta - \sigma$, entonces se trata evidentemente un elemento de $\mathrm{Der}(U)$. ■

5.3. Criterio de Cartan.

En esta sección, el cuerpo base F es de nuevo algebraicamente cerrado y de característica cero. Una poderosa herramienta para el estudio de la solubilidad de un álgebra de Lie L, es el que se basa en las trazas de ciertos endomorfismos de L. Es obvio que L es soluble si y sólo si $[L, L]$ es nilpotente, una de las implicaciones es el Corolario 11 mientras que el recíproco resulta fácil de demostrar (véase el problema 80). Por otro lado el Teorema de Engel implica que $[L, L]$ es nilpotente si y sólo si cada $\mathrm{ad}_{[L,L]}\, x$ es nilpotente (con $x \in [L, L]$). Empezamos pues con un criterio basado en trazas para la nilpotencia de un endomorfismo.

Lema 18 *Sean $A \subset B$ subespacios de $\mathfrak{gl}(V)$ (V de dimensión finita). Definamos $M = \{x \in \mathfrak{gl}(V) : [x, B] \subset A\}$. Supongamos que $x \in M$ satisface $Tr(xy) = 0$ para cada $y \in M$. Entonces x es nilpotente.*

Dem. Sea $x = s + n$ la descomposición de Jordan-Chevalley de x (donde s es la parte semisimple y n la nilpotente). Fijemos una base $B = \{v_1, \ldots, v_m\}$ de V respecto a la que x adopte su forma canónica de Jordan, es decir, la matriz de s respecto a B es $\text{diag}(a_1, \ldots, a_m)$ mientras que $n(v_i) \in \{v_{i+1}, 0\}$. Siendo F de característica cero, su cuerpo primo es $\mathbb{Q}$. Sea $E \subset F$ el subespacio de F (considerado como $\mathbb{Q}$-espacio vectorial) generado por los valores propios a_i $(i = 1, \ldots, m)$. Para demostrar que x es nilpotente, debemos ver que $s = 0$ (o equivalentemente, que $E = 0$). Dado que E tiene dimensión finita sobre $\mathbb{Q}$, bastará demostrar que el espacio dual E^* es nulo. Esto último es equivalente a demostrar que cada aplicación lineal $f : E \to \mathbb{Q}$ es nula.

Sea pues $f \in E^*$ y consideremos el elemento $y \in \mathfrak{gl}(V)$ tal que su matriz en B sea $\text{diag}(f(a_1), \ldots, f(a_m))$. Si denotamos por $\{e_{ij}\}$ la correspondiente base de $\mathfrak{gl}(V)$ tal que $e_{ij}(v_k) = \delta_{ik} v_j$, sabemos que $\text{ad}(s)e_{ij} = (a_j - a_i)e_{ij}$, $ad(y)e_{ij} = (f(a_j) - f(a_i))e_{ij}$ (véase problema 77). Tomemos ahora un polinomio $r(T) \in F[T]$ sin término independiente tal que $r(a_j - a_i) = f(a_j) - f(a_i)$ para cualesquiera i, j. La existencia de tal polinomio viene dada por el Teorema de Interpolación de Lagrange. El lector puede comprobar sin dificultad que $r(\text{ad}(s)) = \text{ad}(y)$.

El Lema 16 implica que $\text{ad}(s)$ es la parte semisimple de $\text{ad}(x)$. En consecuencia se puede escribir como un polinomio en $\text{ad}(x)$ sin término independiente. Al ser $\text{ad}(y) = r(\text{ad}(s))$, entonces, $\text{ad}(y)$ también es un polinomio en $\text{ad}(x)$ sin término constante. Como por hipótesis $\text{ad}(x)B \subset A$, lo mismo ocurrirá con $\text{ad}(y)$. En definitiva $y \in M$. Usando la hipótesis del Lema, $Tr(xy) = Tr(yx) = 0$. Pero la diagonal de la matriz de yx respecto a la base B es $\text{diag}(a_1 f(a_1), \ldots, a_m f(a_m))$. Por lo tanto $\sum_{i=1}^m a_i f(a_i) = 0$. Como $f(a_i)$ es un racional para cada i, aplicando de nuevo f tendremos $\sum_i f(a_i)^2 = 0$. Siendo los números $f(a_i)$ racionales, esta última igualdad implica que ellos son todos nulos luego $f = 0$. ■

Teorema 19 (Criterio de Cartan). *Sea L una subálgebra de $\mathfrak{gl}(V)$, donde V es de dimensión finita. Supongamos que $Tr(xy) = 0$ para cualesquiera $x \in [L, L]$, $y \in L$. Entonces L es soluble.*

Dem. Bastará demostrar que $[L, L]$ es nilpotente (véase el problema 80). Para demostrar que $[L, L]$ es nilpotente, será suficiente con demostrar que cada $x \in [L, L]$ es nilpotente (gracias al Teorema de Engel). Apliquemos entonces el Lema 18 de la forma que sigue: $A = [L, L]$, $B = L$. Por lo tanto $M = \{x \in \mathfrak{gl}(V) : [x, L] \subset [L, L]\}$. Esto implica que $L \subset M$. Para poder concluir que x es nilpotente nos hace falta demostrar que $Tr(xy) = 0$ para cada $y \in M$. Supongamos que $x = \sum_i [a_i, b_i] \in [L, L]$, $a_i, b_i \in L$, $y \in M$, entonces

$$Tr(xy) = \sum_i Tr([a_i, b_i]y) = \sum_i Tr(a_i[b_i, y]) = \sum_i Tr([b_i, y]a_i),$$

y como $y \in M$, $[b_i, y] \subset [L, L]$ luego para cada i se tiene (por hipótesis) que $Tr([b_i, y]a_i) = 0$. Por tanto el Lema 18 implica que x es nilpotente. ■

Corolario 12 *Sea L un álgebra de Lie de dimensión finita, tal que*

$$Tr(\mathrm{ad}(x), \mathrm{ad}(y)) = 0$$

para cada $x \in [L, L]$, $y \in L$. Entonces L es soluble.

Dem. Se aplica el teorema anterior vía la representación adjunta $\mathrm{ad} : L \to \mathfrak{gl}(L)$. Así obtenemos que $\mathrm{ad}(L)$ es soluble. Como el núcleo de la representación adjunta es el centro de L, tenemos que $L/\,\mathrm{Z}(L)$ es soluble luego L es soluble aplicando la Proposición 11 (ya que $\mathrm{Z}(L)$ es soluble). ■

5.4. Forma Killing.

Sea L un álgebra de Lie de dimensión finita, definamos la forma Killing $k : L \times L \to L$ escribiendo $k(x, y) = Tr(\mathrm{ad}(x)\,\mathrm{ad}(y))$. Se trata evidentemente de una forma bilineal simétrica. Esta forma es *asociativa* en el sentido de que $k([x, y], z) = k(x, [y, z])$ para cualesquiera $x, y, z \in L$. Esta identidad es una consecuencia de la fórmula $Tr([x, y]z) = Tr(x[y, z])$, propuesta en el problema 79. Empecemos esta sección con el siguiente lema:

Lema 19 *Sea I un ideal de un álgebra de Lie de dimensión finita. Si la forma de Killing de L es k y la de I (considerado como álgebra de Lie en sí mismo) es k_I, entonces $k_I = k|_{I \times I}$.*

Dem. Si $x, y \in I$, entonces $\mathrm{ad}(x)\,\mathrm{ad}(y)$ es un endomorfismo de L que transforma L en I. Aplicando el problema 81 se tiene que $k(x, y) = Tr(\mathrm{ad}(x)\,\mathrm{ad}(y) = Tr(\mathrm{ad}(x)|_I\,\mathrm{ad}(y)|_I) = k_I(x, y)$. ■

Recordemos que dada una forma bilineal simétrica $f : V \times V \to F$, el radical de f se define como el conjunto de $x \in V$ tales que $f(x, V) = 0$. Este conjunto es siempre un subespacio de V. En el caso de la forma Killing de un álgebra de Lie L, el radical es más que un subespacio: es un ideal del álgebra. En efecto, si $k(x, L) = 0$, entonces $k([x, L], L) = k(x, [L, L]) = 0$ implicando el carácter de ideal del radical de la forma Killing.

Teorema 20 *Sea L un álgebra de Lie de dimensión finita, entonces L es semisimple si y sólo si su forma Killing es no degenerada.*

Dem. Supongamos que $\mathrm{Rad}(L) = 0$ y sea S el radical de la forma Killing k de L. Para cada $x \in S$, $y \in L$ se tiene $0 = k(x, y) = Tr(\mathrm{ad}(x)\,\mathrm{ad}(y))$ (en particular para $y \in [L, L]$). Por el Corolario 12 se tiene que $\mathrm{ad}(S)$ es soluble luego S es soluble. Pero S es un ideal (y soluble) lo que nos conduce a $S \subset \mathrm{Rad}(L) = 0$, es decir, k es no degenerada.

Supongamos ahora que k es no degenerada, es decir, $S = 0$. Vamos a demostrar que cada ideal abeliano de L es nulo (esto implicará que el radical es nulo automáticamente). Sea I un ideal abeliano de L y tomemos $x \in I$, $y \in L$. La aplicación $\mathrm{ad}(x)\,\mathrm{ad}(y)$ transforma L en I luego $(\mathrm{ad}(x)\,\mathrm{ad}(y))^2$ transforma L en $[I, I] = 0$. Esto quiere decir que $\mathrm{ad}(x)\,\mathrm{ad}(y)$ es nilpotente luego su traza es nula y por tanto $k(x, y) = 0$. En definitiva hemos demostrado que $I \subset S = 0$ como queríamos. ■

5.5. Descomposición en ideales simples.

Un álgebra de Lie L se dice que es una suma directa de ideales $I_1, \ldots, I_j$ si $L = I_1 \oplus \cdots \oplus I_t$ es suma directa de los subespacio subyacentes. Esto obliga a que se tenga $[I_i, I_j] \subset I_i \cap I_j = 0$ (si $i \neq j$) lo que implica que L puede considerarse como el producto de las álgebras I_i con 'corchetes por componentes'.

Teorema 21 *Sea $L \neq 0$ un álgebra de Lie semisimple de dimensión finita. Entonces existen ideales $L_1, \ldots, L_t$ de L que son simples como (álgebras de Lie en sí mismos) y de modo que $L = \oplus_i L_i$. Más aún, cada ideal simple de L es alguno de los L_i y la forma Killing de cada L_i es la restricción de la forma Killing de L a $L_i \times L_i$.*

Dem. Tomemos un ideal arbitrario I de L. Como $I^\perp$ es un ideal (ver problema 83), y $I \cap I^\perp$ es soluble (problema 84), tenemos $I \cap I^\perp = 0$ al ser L semisimple. Por otra parte la fórmula $\dim(L) = \dim(I) + \dim(I^\perp)$ implica $L = I \perp I^\perp$. Ahora procederemos inductivamente. Si L no tiene ideales más que los triviales, entonces L es simple (ya que $[L, L] \neq 0$). En caso contrario podemos seleccionar un ideal minimal no nulo L_1. En este caso $L = L_1 \oplus L_1^\perp$. Cada ideal de L_1 es también un ideal de L luego L_1 es semisimple (y simple por minimalidad de I_1). Por la misma razón $I_1^\perp$ es semisimple luego por inducción se descompone como una suma directa de ideales simples de $L_1^\perp$ que son también ideales de L.

Veamos ahora que estos ideales L_i son únicos. Sea I un ideal simple de L, entonces $[I, L] \subset I$ es un ideal de I. No puede ser nulo pues de tenerse $[I, L] = 0$ entonces $I \subset \mathrm{Z}(L) = 0$ (el centro está contenido en el radical que es nulo). En consecuencia $[I, L] = I$ y como $L = \oplus L_i$ tenemos $I = [I, L] = \oplus_i [I, L_i]$. Cada uno de estos sumandos es un ideal de I, luego todos los sumandos menos uno son nulos y tenemos $I = [I, L_i]$ para un (y sólo un) índice i. Así $I = [I, L_i] \subset L_i$ lo que nos lleva por minimalidad de L_i a la igualdad $I = L_i$. Hemos demostrado que cada ideal simple de L es alguno de los L_i. La última afirmación del teorema es exactamente lo que se afirma en el Lema 19. ■

Corolario 13 *Si L es semisimple de dimensión finita, entonces $L = [L, L]$ y todos los ideales e imágenes homomórficas de L son semisimples. Más aún, cada ideal de L es una suma de ciertos ideales simples de L.*

5.6. Derivaciones interiores.

En un álgebra de Lie L, para cada $x \in L$ la aplicación $\mathrm{ad}(x) : L \to L$ es una derivación. Esto se sigue de inmediato de la identidad de Jacobi. Las derivaciones del tipo $\mathrm{ad}(x)$ se llaman *interiores*. El conjunto de todas ellas se denota como sabemos por $\mathrm{ad}(L) \subset \mathrm{Der}(L)$. Este conjunto de derivaciones interiores es algo más que un simple subespacio de $\mathrm{Der}(L)$, es un ideal. En efecto si tomamos $\delta \in \mathrm{Der}(L)$, entonces para cada $x \in L$ se tiene

$$[\delta, \mathrm{ad}(x)] = \mathrm{ad}(\delta(x)). \tag{5.3}$$

Podemos pues escribir $\mathrm{ad}(L) \triangleleft \mathrm{Der}(L)$. En algunos casos se da la igualdad $\mathrm{ad}(L) = \mathrm{Der}(L)$:

Teorema 22 *Si L es semisimple de dimensión finita,* $\mathrm{ad}(L) = Der(L)$.

Dem. Como $\mathrm{Rad}(L) = 0$ entonces $\mathrm{Z}(L) = 0$, el homomorfismo $\mathrm{ad} : L \to \mathrm{ad}(L)$ es un isomorfismo de álgebras de Lie. Poniendo $M := \mathrm{ad}(L)$ tenemos un álgebra de Lie semisimple luego de forma Killing no degenerada. Denotemos por D el álgebra de Lie $D := \mathrm{Der}(L)$. La ecuación (5.3) de arriba implica $[D, M] \subset M$, es decir, M es un ideal de D. Entonces, el Lema 19 implica que la forma Killing K_M de M coincide con la restricción de la forma Killing k_D de D a $M \times M$. Consideremos entonces el ideal $M^\perp$ de D. Como k_M es no degenerada, la intersección $M \cap M^\perp$ es nula. Esto implica $[M, M^\perp] = 0$. Si tomamos ahora $\delta \in M^\perp$, y aplicamos la igualdad (5.3), tendremos $0 = [\delta, \mathrm{ad}(x)] = \mathrm{ad}(\delta(x))$ para cada $x \in L$ luego $\delta = 0$. En definitiva $M^\perp = 0$ y aplicando el Problema 75 se tiene $M = D$, es decir, $\mathrm{ad}(L) = \mathrm{Der}(L)$. ■

5.7. Descomposición de Jordan-Chevalley abstracta.

Hemos introducido la descomposición de Cartan-Chevalley para elementos de $\mathfrak{gl}(V)$ siendo V un F-espacio vectorial de dimensión finita. El Teorema 22 nos permite introducir una noción de descomposición de Jordan-Chevalley para álgebras de Lie semisimples (de dimensión finita) sobre F. En efecto, la aplicación $\mathrm{ad} : L \to \mathrm{Der}(L) = \mathrm{ad}(L)$ es un isomorfismo. Para cada $x \in L$ podemos considerar la descomposición de Jordan-Chevalley de $\mathrm{ad}(x) = \mathrm{ad}(s) + \mathrm{ad}(n)$ con $\mathrm{ad}(s)$ semisimple, $\mathrm{ad}(n)$ nilpotente, y $0 = [\mathrm{ad}(s), \mathrm{ad}(n)]$. El Lema 17 junto con el Teorema 22, implican que las partes semisimples y nilpotentes de $\mathrm{ad}(x)$ están en la imagen de ad. El carácter de isomorfismo de ad implica que $x = s + n$ donde $[s, n] = 0$, s es ad-semisimple y n es ad-nilpotente. Esta es la que se conoce como *descomposición de Jordan-Chevalley abstracta* de $x \in L$, una expresión del tipo $x = s + n$ donde $[s, n] = 0$, $\mathrm{ad}(s)$ es semisimple y $\mathrm{ad}(n)$ es nilpotente. Obsérvese la unicidad de la descomposición abstracta de Jordan-Chevalley.

Por otra parte, se podría objetar en este punto que si L resulta ser un álgebra de endomorfismos de un espacio vectorial, entonces hay cierta ambigüedad pues cabe considerar para un mismo $x \in L$, su descomposición clásica de Jordan-Chevalley y su descomposición

de Jordan-Chevalley abstracta. Más adelante demostraremos que ambas nociones coinciden en el contexto indicado. Como un avance de esta situación puedes estudiarse el problema 85 donde se trabaja con un caso particular, el álgebra $\mathfrak{sl}(V)$.

5.8. Representaciones completamente reducibles.

En esta sección todas las representaciones se entenderá que son de dimensión finita. Si L es una álgebra de Lie y V un L-módulo, diremos que $V \neq 0$ es *irreducible* cuando los únicos L-submódulos de V son 0 y el propio V. Se dirá que V es *completamente reducible*[1] cuando V es una suma directa de L-submódulos irreducibles (véase el problema 86 para una formulación equivalente de la definición).

Dada un representación $\phi : L \to \mathfrak{gl}(V)$, el álgebra asociativa con unidad de $\mathrm{End}(V)$ generada por $\phi(L)$ deja invariantes exactamente los mismos subespacios de V que L. Por consiguiente todos los resultados típicos para módulos sobre álgebras asociativas (por ejemplo el Teorema de Jordan-Hölder), son válidos para módulos sobre L. Así por ejemplo si R es una F-subálgebra de $\mathrm{End}_F(V)$, entonces R actúa sobre V convirtiéndolo en un R-módulo. Si este R-módulo es irreducible, los únicos endomorfismos de V que conmutan con todos los elementos de R son los múltiplos escalares de la identidad. En efecto el Lema de Schur nos dice que la F-álgebra $D := \mathrm{End}_R(V)$ es de división. Por otra parte siendo V de dimensión finita, D también lo es y como el cuerpo F es algebraicamente cerrado D es isomorfa a F. Entonces si $f : V \to V$ es tal que $f(a.v) = af(v)$ para cualesquiera $a \in R$, $v \in V$ tenemos que $f \in D$ por lo tanto existe un escalar $\lambda \in F$ tal que $f = \lambda \mathrm{Id}_V$. Como corolario podemos enunciar el siguiente resultado que podría considerarse como una versión para álgebras de Lie, del lema de Schur:

Lema 20 *Sea $\phi : L \to \mathfrak{gl}(V)$ una representación irreducible y de dimensión finita. Entonces los únicos endomorfismos de V que conmutan con todos los $\phi(x)$ ($x \in L$) son los múltiplos escalares de la identidad.*

Dem. Basta considerar la F-álgebra asociativa y con unidad R de $\mathrm{End}_F(V)$ generada por $\phi(L)$. Los endomorfismos de V que conmutan con todos los $\phi(x)$ ($x \in L$) son exactamente los que conmutan con todos los elementos de R. Además V es un R-módulo irreducible por ser irreducible la representación ϕ. Aplicando pues el resultado asociativo descrito arriba, se acaba la demostración de este Lema. ■

Describimos a continuación una serie de construcciones que nos permitirán definir nuevos módulos a partir de módulos conocidos. En primer lugar describiremos el módulo *dual* de uno dado.

Dual. Sea V un L módulo. El espacio vectorial dual V^* se puede dotar de estructura de L-módulo (llamado *dual* si definimos para cada $f \in V^*$, $x \in L$ el elemento xf

[1] Se habla también de representación *completamente reducible* o de representación *irreducible* en el caso anterior.

de V^* dado por $(xf)(v) = -f(xv)$ para cada $v \in V$. El lector puede comprobar sin dificultad que esto dota de estructura de L-módulo a V^*.

Producto tensorial. Si V y W son L-módulos, el producto tensorial (de F-espacios) $V \otimes_F W$ se puede convertir también en un L-módulo definiendo $x(v \otimes w) = (xv) \otimes w + v \otimes xw$ para cualesquiera $x \in L$, $v \in V$, $w \in W$. De nuevo invitamos al lector a comprobar que de este modo se obtiene una estructura de L-módulo en $V \otimes W$. Como caso particular de esta construcción tenemos el caso en que V es un L-módulo. Entonces el módulo dual V^* nos da la posibilidad de construir el L-módulo $V^* \otimes_F V$.

Sea $\phi : L \to \mathfrak{gl}(V)$ una representación *fiel* (es decir, ϕ es un monomorfismo) de L (que supondremos semisimple). Definamos la forma bilineal simétrica $\beta : L \times L \to F$ dada por $\beta(x, y) := Tr(\phi(x)\phi(y))$. Esta forma es asociativa gracias una vez más a la fórmula $Tr([x, y]z) = Tr(x[y, z])$ cuya demostración se pide en el Problema 79. Como consecuencia el radical S de β es un ideal de L. Aplicando el criterio de Cartan tenemos la solubilidad de $\phi(S)$, y por tanto S es soluble luego $S = 0$ al ser L semisimple.

Supongamos ahora que L es semisimple y β cualquier forma bilineal simétrica no degenerada asociativa. Si tomamos una base $\{x_1, \ldots, x_n\}$ de L, sabemos la existencia de una base dual $\{y_1, \ldots, y_n\}$ de L relativa a β (es decir, se satisfacen las relaciones $\beta(x_i, y_j) = \delta_{ij}$, donde esta última es la delta de Kronecker).

Para cada $x \in L$ hagamos $[x, x_i] = \sum_j a_{ij}x_j$ con $a_{ij} \in F$ y $[x, y_i] = \sum_j b_{ij}y_j$, $b_{ij} \in F$. Entonces

$$a_{ik} = \sum_j a_{ij}\beta(x_j, y_k) = \beta([x, x_i], y_k) = -\beta([x_i, x], y_k) =$$

$$= -\beta(x_i, [x, y_k]) = -\sum_j \beta(x_i, b_{kj}y_j) = -b_{ki}.$$

Si tenemos ahora una representación $\phi : L \to \mathfrak{gl}(V)$ podemos definir $c_\phi(\beta) := \sum_i \phi(x_i)\phi(y_i) \in \mathrm{End}_F(V)$. Aplicando la fórmula del problema 76, así como la igualdad $a_{ik} = -b_{ki}$ que acabamos de demostrar, se tiene:

$$[\phi(x), c_\phi(\beta)] =$$

$$= \sum_i [\phi(x), \phi(x_i)\phi(y_i)] = \sum_i [\phi(x), \phi(x_i)]\phi(y_i) + \phi(x_i)[\phi(x), \phi(y_i)] =$$

$$= \sum_{i,j} a_{ij}\phi(x_j)\phi(y_i) + \sum_{ij} b_{ij}\phi(x_i)\phi(y_j) = 0$$

y por tanto $c_\phi(\beta)$ *es un endomorfismo de* V *que conmuta con todos los de* $\phi(L)$. Si calculamos la traza del endomorfismo $c_\phi(\beta)$, tendremos $Tr(c_\phi(\beta)) = \sum_i Tr(\phi(x_i)\phi(y_i)) = \sum_i \beta(x_i, y_i) = \dim(L)$. Además, si la representación ϕ resulta ser irreducible, entonces como $c_\phi(\beta)$ conmuta con todos los endomorfismos de $\phi(L)$, será en virtud del Lema 20 un múltiplo escalar de la identidad. Por lo tanto ese múltiplo es $\dim(L)/\dim(V)$ (se ve que en este caso la definición de $c_\phi(\beta)$ no depende de la elección de la base $\{x_1, \ldots, x_n\}$ de L). Resumiendo estos últimos resultados podemos enunciar la siguiente proposición:

Proposición 14 *Sea $\phi : L \to \mathfrak{gl}(V)$ una representación fiel de un álgebra semisimple de dimensión finita L. Sea $\beta : L \times L \to F$ la forma bilineal simétrica no degenerada dada por $\beta(x, y) := Tr(\phi(x)\phi(y))$. Fijada una base $\{x_1, \ldots, x_n\}$ de L podemos considerar su base dual $\{y_1, \ldots, y_n\}$ y definir $c_\phi(\beta) := \sum_i \phi(x_i)\phi(y_i)$. Entonces $c_\phi(\beta)$ es un endomorfismo de V denominado* elemento de Casimir *de ϕ, que conmuta con todos los de $\phi(L)$. Su traza coincide con la dimensión de L. Si la representación es irreducible, entonces $c_\phi(\beta) = (\dim(L)/\dim(V))1$.*

Definición 16 *Denominaremos* forma traza de la representación ϕ *a la forma $\beta : L \times L \to F$ definida por $\beta(x, y) := Tr(\phi(x)\phi(y))$.*

Lema 21 *Sea $\phi : L \to \mathfrak{gl}(V)$ una representación de un álgebra de Lie semisimple (de dimensión finita) L. Entonces $\phi(L) \subset \mathfrak{sl}(V)$. En particular L actúa trivialmente sobre los espacios de dimensión uno.*

Dem. Se tiene $L = [L, L]$, $\mathfrak{sl}(V) = [\mathfrak{gl}(V), \mathfrak{gl}(V)]$ luego $\phi(L) = [\phi(L), \phi(L)] \subset [\mathfrak{gl}(V), \mathfrak{gl}(V)] = \mathfrak{sl}(V)$. ■

Lema 22 *Sea $\phi : L \to \mathfrak{gl}(V)$ una representación de un álgebra semisimple de dimensión finita L. Supongamos que W es un L-submódulo de V de codimensión uno (como F-espacio vectorial). Entonces existe un L-submódulo W_1 de V tal que $V = W \oplus W_1$.*

Dem. Demostremos primero el lema en el caso de que W sea irreducible. Previamente demostraremos que la representación puede suponerse fiel. Si $\phi : L \to \mathfrak{gl}(V)$ es la representación, su núcleo $\ker(\phi)$ es un ideal de L y por lo tanto $L = \ker(\phi) \oplus L'$ donde L' es también un ideal de L que visto como álgebra es semisimple. La restricción $\phi' : L' \to \mathfrak{gl}(V)$ de ϕ a L' es ahora fiel y los L'-submódulos de V son exactamente los L-submódulos de V: trivialmente cada L-submódulo de V es un L'-submódulo, por otra parte si X es un L'-submódulo de V, entonces la aplicación $L \times X \to X$ dada por $(a + b)x := bx$ con $a \in \ker(\phi)$, $b \in L$, $x \in X$ define una estructura única de L módulo en X de la que se obtiene la estructura de L'-módulo de X por restricción. Supondremos pues que la representación ϕ de partida es fiel. Sea $c = c_\phi(\beta)$ un elemento de Casimir de ϕ. Como c conmuta con los elementos de $\phi(L)$, se tiene que $c(x \cdot v) = c(\phi(x)(v)) = \phi(x)c(v) = x \cdot c(v)$, es decir, c es un endomorfismo de L-módulos de V. Por otra parte $c = \sum_i \phi(x_i)\phi(y_i)$ para cierta base $\{x_i\}$ de V y su dual $\{y_i\}$ respecto a la forma traza de ϕ. Como $\phi(L)(W) \subset W$ se tiene que $c(W) \subset W$. Además $\ker(c)$ es un L-submódulo de V. Según el Lema 21, L actúa trivialmente sobre V/W lo que quiere decir que $\phi(L)$ transforma V en W. También c transforma V en W (por ser suma de composiciones $\phi(x_i)\phi(y_i)$). Por otra parte c actúa como un múltiplo escalar de la identidad sobre el submódulo irreducible W (aplíquese el Lema de Schur). Este escalar no puede ser nulo pues de serlo se tendría que la traza de c (como endomorfismo de V en V) sería nula (en contra de que dicha traza es la dimensión de L). Como consecuencia, $\ker(c) \cap W = 0$ y necesariamente $\dim(\ker(c)) = 1$, y $V = W \oplus \ker(c)$.

Podemos hacer la demostración en el caso general por inducción sobre la dimensión de V. La dimensión más pequeña de V que podemos considerar es dos. En este caso W es irreducible y aplicamos lo que acabamos de demostrar. Supongamos pues la propiedad cierta para los espacios de dimensión menor que la de V. Sea U el L-módulo (de dimensión uno) que hace exacta la sucesión $0 \to W \to V \to U \to 0$. Suponiendo W no irreducible, sea W' un submódulo propio no nulo de W. Este W' proporciona la posibilidad de considerar la nueva sucesión exacta $0 \to W/W' \to V/W' \to U \to 0$. Aplicando la hipótesis de inducción existe un L-submódulo unidimensional de V/W' (denotémosle $\hat{W}/W'$) tal que $V/W' = W/W' \oplus \hat{W}/W'$. Podemos considerar ahora otra sucesión exacta $0 \to W' \to \hat{W} \to U \to 0$. Aplicando de nuevo la hipótesis de inducción obtenemos un L-submódulo unidimensional X de $\hat{W}$ tal que $\hat{W} = W' \oplus X$. Ahora bien $X \cap W \subset \hat{W} \cap W \subset W'$ y como $X \cap W \subset X$ tenemos $X \cap W \subset W' \cap X = 0$. Por lo tanto $X \cap W = 0$ pero $\dim(X) + \dim(W) = \dim(V)$ (esto se sigue de tomar dimensiones en la fórmula $V/W' = W/W' \oplus \hat{W}/W'$, teniendo en cuenta que $\hat{W}/W' \cong X$). Finalmente concluimos que $V = W \oplus X$. ■

Teorema 23 (Teorema de Weyl). *Toda representación (de dimensión finita) de un álgebra de Lie semisimple (también de dimensión finita) es completamente reducible.*

Dem. Sea $\phi : L \to \mathfrak{gl}(V)$ la representación. Si V es irreducible tenemos la conclusión que buscamos demostrar. En caso contrario supongamos que W es un L-submódulo no nulo, y escribamos la sucesión exacta

$$0 \to W \to V \to V/W \to 0.$$

Consideremos la estructura de L-módulo de $\hom(V, W)$ que introdujimos en el problema 87. Recordemos que si $x \in L$, $f \in \hom(V, W)$, $v \in V$, dicha estructura venía dada por $(x \cdot f)(v) = x \cdot f(v) - f(x \cdot w)$. Sea ahora $\mathcal{V}$ el subespacio de $\hom(V, W)$ formado por los elementos cuya restricción a W consista en la multiplicación por algún escalar. Este subespacio $\mathcal{V}$ es un L-submódulo pues si $f \in \mathcal{V}$ y $x \in L$, entonces $f|_W = a1$ para algún escalar a, y $(x \cdot f)(w) = x \cdot f(w) - f(x \cdot w) = ax \cdot w - ax \cdot w = 0$. Así $x \cdot f$ es la multiplicación por el escalar cero lo que demuestra que $x \cdot f \in \mathcal{V}$. Consideremos ahora el subespacio $\mathcal{W}$ de $\hom(V, W)$ formado por todas las aplicaciones f cuya restricción a W es nula. El cálculo anterior demuestra que $\mathcal{W}$ es también un L-módulo y de hecho, un submódulo de $\mathcal{V}$. Además hemos visto que $L \cdot \mathcal{V} \subset \mathcal{W}$. Veamos que $\mathcal{V}/\mathcal{W}$ tiene dimensión uno: la aplicación $\mathcal{V} \to F$ tal que asocia a cada $f \in \mathcal{V}$ el único escalar a tal que $f|_W = a1$, es lineal y de núcleo $\mathcal{W}$. Así hemos llegado precisamente a la situación

$$0 \to \mathcal{W} \to \mathcal{V} \to U \to 0$$

que se consideró en el lema precedente.

El módulo $\mathcal{V}$ tiene entonces un subespacio unidimensional, que es un L-submódulo, y que complementa a $\mathcal{W}$. Si tomamos un generador f de dicho complemento, podemos suponer que la restricción de f a W es la identidad (multiplicando por conveniente escalar

no nulo). Así $f|_W = 1_W$. Como L actúa trivialmente sobre ese complemento unidimensional, tenemos $x \cdot f = 0$ para cada $x \in K$. Pero esto es equivalente a escribir $x \cdot f(v) = f(x \cdot v)$, es decir f es un homomorfismo de L-módulos. Por consiguiente su núcleo es un L-submódulo de V que satisface $\ker(f) \cap W = 0$. Además $V/\ker(f) \cong W$ (ya que f actúa como la identidad cuando se restringe a W). Así $\dim(V) = \dim(\ker(f)) + \dim(W)$ lo que implica $V = W \oplus \ker(f)$. ■

5.9. Problemas.

Problema 75 *Sea V un espacio vectorial de dimensión arbitraria sobre un cuerpo F (sin restricción sobre su característica). Sea $f : V \times V \to F$ una forma bilineal simétrica y S un subespacio de V de dimensión finita y no degenerado (lo quiere decir que la restricción de f a $U \times U$ es no degenerada). Demuéstrese que entonces $V = S \oplus S^{\perp}$. Sugerencia: demuéstrese que la aplicación $S \to S^*$ tal que $s \mapsto f(s, \_)$ es un isomorfismo de espacios vectoriales. Para ver que $V = S + S^{\perp}$, tómese $v \in V$ y demuéstrese que existe $s \in S$ tal que $f(v, \_) = f(s, \_)$.*

Problema 76 *Certifíquese que $\forall x, y, z \in \mathfrak{gl}(V)$ se tiene $[x, yz] = [x, y]z + y[x, z]$.*

Problema 77 *Sea F es algebraicamente cerrado y V un F-espacio de dimensión finita. Tomemos $x \in \mathfrak{gl}(V)$ semisimple. Demuéstrese que $\mathrm{ad}(x) : \mathfrak{gl}(V) \to \mathfrak{gl}(V)$ es semisimple. Sugerencia: sea $\{v_1, \ldots, v_n\}$ una base de V que diagonaliza a x, de modo que $x(v_i) = a_i v_i$ con $a_i \in F$. Constrúyase la base de $\mathfrak{gl}(V)$ definida por las relaciones $e_{ij}(v_k) = \delta_{ki} v_j$, y demuéstrese que $\mathrm{ad}(x)e_{ij} = (a_j - a_i)e_{ij}$.*

Problema 78 *Demuéstrese la fórmula de la demostración del Lema 17.*

Problema 79 *Sean x, y, z endomorfismos de un espacio vectorial de dimensión finita V. Demuéstrese que $Tr([x, y]z) = Tr(x[y, z])$.*

Problema 80 *Demuéstrese que si L es álgebra de Lie tal que $[L, L]$ es nilpotente, entonces L es soluble.*

Problema 81 *Sea V un F-espacio de dimensión finita, W un subespacio suyo y $f : V \to V$ un endomorfismo que transforma V en W. Demuéstrese que $Tr(f) = Tr(f|_W)$. Sugerencia: estúdiese la traza de f con relación a una base de V que sea el resultado de extender una base de W.*

Problema 82 *Calcúlese la forma Killing del álgebra de Lie $L := \mathfrak{sl}(2, F)$. Sugerencia: considérese la base $\{x, h, y\}$ de L formada por las matrices $x = E_{12}$, $y = E_{21}$, $h = E_{11} - E_{22}$*

donde como es habitual la matriz E_{ij} es la que tiene un uno en la posición (i,j) y cero en las demás. Compruébese que entonces

$$\mathrm{ad}(h) = diag(2,0,-2), \mathrm{ad}(x) = \begin{pmatrix} 0 & 0 & 0 \\ -2 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \mathrm{ad}(y) = \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix},$$

y determínese ahora la forma de Killing que deberá salir de matriz:

$$\begin{pmatrix} 0 & 0 & 4 \\ 0 & 8 & 0 \\ 4 & 0 & 0 \end{pmatrix}.$$

Problema 83 *Sea I un ideal de un álgebra de Lie de dimensión finita L. Demuéstrese que $I^{\perp}$ definido como el conjunto de elementos $x \in L$ tales que $k(x,I) = 0$ es un ideal de L (k es la forma Killing de L).*

Problema 84 *En el ambiente del problema anterior, aplíquese el Criterio de Cartan para demostrar que $I \cap I^{\perp}$ es un ideal soluble.*

Problema 85 *Sea V un F-espacio vectorial de dimensión finita y consideremos el álgebra $L = \mathfrak{sl}(V)$. Sea $x \in L$ y $x = x_s + x_n$ su descomposición de Jordan-Chevalley.*

1. *Demuéstrese que $x_n \in L$ usando el hecho de que todos sus autovalores son nulos. Conclúyase que $x_s \in L$.*

2. *Aplíquese el Lema 16 para concluir que $ad(x_s) : \mathfrak{gl}(V) \to \mathfrak{gl}(V)$ es semisimple. Demuéstrese que $\mathrm{ad}(x_s) : L \to L$ es semisimple.*

3. *Análogamente demuéstrese que $\mathrm{ad}(x_n) : L \to L$ es nilpotente.*

4. *Como $[\mathrm{ad}(x_s), \mathrm{ad}(x_n)] = \mathrm{ad}([x_s, x_n]) = 0$, la unicidad de la descomposición de Jordan-Chevalley abstracta implica que $x = x_s + x_n$ es también la descomposición abstracta de Jordan-Chevalley.*

Problema 86 *Sea V un módulo (de dimensión finita) del álgebra de Lie L. Pruébese que V es completamente reducible si y sólo si cada submódulo de V posee un complemento (es decir, para cada W submódulo de V, existe otro submódulo W' tal que $V = W \oplus W'$). Sugerencia: suponiendo $V = \oplus_i S_i$ para una familia $\{S_i\}$ de L-módulos irreducibles, si W es un submódulo propio y no nulo, no todos los S_i están contenidos en W. Aquellos S_i no contenidos en W tienen intersección nula con W. Consideremos pues un submódulo X de V maximal respecto a la propiedad de tener intersección nula con W. Si $W \oplus X$ no coincide con V,...*

Problema 87 *Sean V y W dos F-espacios vectoriales (de dimensión finita). Compruébese que la aplicación $\theta : V^* \otimes_F W \to \hom_F(V, W)$ que transforma el elemento $f \otimes w$ en la aplicación F-lineal de V a W tal que $v \mapsto f(v)w$, es un isomorfismo de F-espacios vectoriales. Compruébese que definiendo para cada $x \in L$, $f \in \hom_F(V, W)$ el endomorfismo $x \cdot f : V \to W$ tal que $(x \cdot f)(v) := x \cdot f(v) - f(x \cdot v)$, se dota de estructura de L-módulo a $\hom_F(V, W)$. Demuéstrese que entonces θ es un isomorfismo de L-módulos considerando en $V^* \otimes_F W$ la estructura de L-módulo tensorial descrita al final de la sección 5.8.*

Problema 88 *Sea $L = \mathfrak{sl}(2, F)$, $V = F^2$ y $\phi : L \to \mathfrak{gl}(V)$ la inclusión. Consideremos la base $\{x, h, y\}$ de L dada por $x = E_{12}$, $h = E_{11} - E_{22}$, $y = E_{21}$. Determínese la forma traza β de ϕ así como la base dual de la anterior respecto a β. Calcúlese el elemento de Casimir de ϕ.*

Capítulo 6

Estructura de las álgebras de Lie semisimples

6.1. Descomposición de Jordan-Chevalley revisitada.

En el capítulo anterior definimos la descomposición de Jordan-Chevalley de un elemento $x \in \mathfrak{gl}(V)$ (para V finito-dimensional). Vimos que para un elemento de un álgebra de Lie de derivaciones, sus componentes nilpotente y semisimples, pertenecen a dicha álgebra de derivaciones. Después, vimos que se podía definir una noción abstracta de descomposición de Jordan-Chevalley en un álgebra de Lie semisimple L (en dimensión finita), gracias al hecho de que toda derivación es interior. Así si $\mathrm{ad}(x)$ se descompone en partes semisimples y nilpotentes en $\mathfrak{gl}(L)$, tenemos asegurado que estas partes están en $\mathrm{Der}(L)$ luego en $\mathrm{ad}(L)$. Por tanto existen elementos únicos $\mathrm{ad}(x_s)$ y $\mathrm{ad}(x_n)$ que conmutan, $\mathrm{ad}(x) = \mathrm{ad}(x_s)+\mathrm{ad}(x_n)$, y siendo $\mathrm{ad}(x_s)$ semisimple y $\mathrm{ad}(x_n)$ nilpotente. Entonces la descomposición $x = x_s + x_n$ se llama la descomposición abstracta de Jordan-Chevalley de x.

Habíamos advertido del peligro que se corre cuando L es una subálgebra de $\mathfrak{gl}(V)$, pues en este caso podríamos considerar las dos descomposiciones de Jordan-Chevalley: la que tiene cada elemento como endomorfismo de V, y su descomposición abstracta. En esta sección demostraremos que no hay ambigüedad: las descomposiciones coinciden. Para ello será de vital importancia el Teorema de Weyl sobre la completa reducibilidad de las representaciones de dimensión finita de un álgebra semisimple.

Teorema 24 *Sea $L \subset \mathfrak{gl}(V)$ una subálgebra de Lie semisimple de $\mathfrak{gl}(V)$ con V de dimensión finita. Entonces L contiene las partes semisimple y nilpotente de todos sus elementos. En particular la descomposición de Jordan-Chevalley usual, y la abstracta coinciden.*

Dem. Sea $x \in L$ arbitrario, y $x = x_s + x_n$ su descomposición de Jordan-Chevalley en $\mathfrak{gl}(V)$. Tenemos que demostrar que $x_s, x_n \in L$. Como $\mathrm{ad}(x)L \subset L$ y $\mathrm{ad}(x_s)$, $\mathrm{ad}(x_n)$ son polinomios en $\mathrm{ad}(x)$, se tiene $\mathrm{ad}(x_s)L \subset L$, $\mathrm{ad}(x_n)L \subset L$. Por lo tanto $x_s, x_n \in N := \{a \in \mathfrak{gl}(V) : [a, L] \subset L\}$. Es fácil ver que N es una subálgebra de $\mathfrak{gl}(V)$ que contiene a L (como ideal).

Para cada L-submódulo W de V definamos $L_W := \{y \in \mathfrak{gl}(V) : y(W) \subset W, Tr(y|_W = 0\}$. Como L es semisimple, $L = [L, L]$ luego $L \subset L_W$ para todo W. Definamos

$$L' = N \cap \left(\bigcap_W L_W \right).$$

Se demuestra fácilmente que L' es una subálgebra de N que contiene a L como ideal. De hecho: $[L, L'] \subset [L, N] \subset L$ por definición de N. Por otra parte $x_s, x_n \in L_W$ para cada W: en efecto, como $x \in L = [L, L]$ entonces x tiene traza nula, como $V = W \oplus W'$ donde W' es otro L-submódulo, entonces $x(W) \subset W$, $x(W') \subset W'$ luego W y W' son x_s y x_n-invariantes. Ahora bien, $x_n|_W$ tiene traza nula (siendo además nilpotente) y por lo tanto $x_s|_W$ tiene traza nula. En consecuencia $x_s, x_n \in L_W$ para cada W. En resumen, $x_s, x_n \in L'$. Veamos finalmente que $L' = L$ lo que acabará la demostración. Como L' es un L-módulo de dimensión finita se debe tener $L' = L \oplus M$ para cierto L-submódulo M de L'. Pero $[L, L'] \subset L$ luego $[L, M] \subset L \cap M = 0$. Para ver que $M = 0$ tomemos un elemento cualquiera $y \in M$ y consideremos cualquier submódulo irreducible W de V. Al tenerse $[L, y] = 0$ el Lema 20 implica entonces que y actúa sobre W como un múltiplo de la identidad. Por ser $y|_W$ de traza nula, se tiene finalmente que ese múltiplo es cero. Por tanto $y(W) = 0$ para cada submódulo irreducible W de V. Como V es suma de tales submódulos, se tiene finalmente que $y = 0$. ■

Corolario 14 *Sea L semisimple (de dimensión finita) y $\phi : L \to \mathfrak{gl}(V)$ una representación de dimensión finita de L. Si $x = s + n$ es la descomposición de Jordan-Chevalley abstracta de $x \in L$, entonces $\phi(x) = \phi(s) + \phi(n)$ es la descomposición usual de Jordan-Chevalley de $\phi(x)$.*

Dem. Como $\mathrm{ad}(s) : L \to L$ es diagonalizable existe una base $\{e_i\}_{i=1}^n$ de L formada por vectores propios de $\mathrm{ad}(s)$. Entonces $\phi(L)$ esta generada por $\phi(e_i)$, $i = 1, \ldots, n$. Si suponemos que $\mathrm{ad}(s)e_i = k_i e_i$, entonces

$$\mathrm{ad}(\phi(s))\phi(e_i) = \phi([s, e_i]) = k_i \phi(e_i),$$

luego $\mathrm{ad}(\phi(s))$ es semisimple. De forma similar $\mathrm{ad}(\phi(n))$ es nilpotente y ambos operadores conmutan. Por lo tanto $\phi(x) = \phi(s) + \phi(n)$ es la descomposición de Jordan-Chevalley abstracta de $\phi(x)$ en $\mathfrak{gl}(V)$. Aplicando el Teorema anterior, esta es también su descomposición usual. ■

6.2. Representaciones de $\mathfrak{sl}(2, F)$.

En esta sección, todos los módulos se supondrán de dimensión finita. El cuerpo base F se supondrá algebraicamente cerrado y de característica cero. Denotemos por L el álgebra

$\mathfrak{sl}(2,F)$ con base $\{x,y,h\}$ dada por

$$x=\begin{pmatrix}0&1\\0&0\end{pmatrix},\quad y=\begin{pmatrix}0&0\\1&0\end{pmatrix}\quad h=\begin{pmatrix}1&0\\0&-1\end{pmatrix}.$$

Esta base se llamará *la base estandar* de L. Sabemos que la tabla de multiplicar de los elementos de esta base viene dada por las relaciones $[h,x]=2x$, $[h,y]=-2y$, $[x,y]=h$.

Sea V un L-módulo cualquiera, como h es un elemento semisimple de L, de acuerdo con el Corolario 14, h debe actuar diagonalmente sobre V. Tenemos entonces una descomposición $V=\oplus_\lambda V_\lambda$ donde $V_\lambda=\{x\in V:[h,v]=\lambda v\}$, $(\lambda\in F)$. Cuando λ no sea un autovalor del endomorfismo de V que representa a h escribiremos $V_\lambda=0$. Si $\lambda\in F$ es tal que V_λ es no nulo, diremos que λ es un *peso* de h en V. Llamaremos a V_λ un espacio-peso.

Lema 23 *Si $v\in V_\lambda$, entonces $xv\in V_{\lambda+2}$, y $yv\in V_{\lambda-2}$.*

Dem. En efecto:

$$h(xv)=[h,x]v+x(hv)=2xv+\lambda xv=(\lambda+2)xv.$$

Análogamente se demuestra que $yv\in V_{\lambda-2}$. ■

Como la dimensión de V es finita y $V=\oplus_\lambda V_\lambda$, debe existir algún $\lambda\in F$ tal que $V_\lambda\neq 0$, $V_{\lambda+2}=0$. Para un tal λ, los elementos no nulos de V_λ se llamarán *vectores maximales* de peso λ.

Lema 24 *Sea V un L-módulo irreducible. Sea $v_0\in V_\lambda$ un vector maximal. Definamos $v_{-1}:=0$, $v_i:=(1/i!)y^iv_0$, $(i\geq 0)$. Se tiene entonces:*

a) $hv_i=(\lambda-2i)v_i$.

b) $yv_i=(i+1)v_{i+1}$.

c) $xv_i=(\lambda-i+1)v_{i-1}$.

Dem. El primer apartado es corolario del lema anterior mientras que el segundo proviene directamente de la definición de los v_i. Veamos el apartado c). Para $i=0$ tenemos que demostrar que $xv_0=0$. Esto es consecuencia del hecho de que v_0 es un vector maximal, es decir $v_0\in V_\lambda\neq 0$ pero $V_{\lambda+2}=0$. Aplicando el lema anterior, se tendría $xv_0\in V_{\lambda+2}=0$. Supongamos que la fórmula se cumple para i. Entonces

$$xv_{i+1}=\frac{1}{(i+1)!}xy^{i+1}v_0=\frac{1}{i+1}xyv_i=\frac{1}{i+1}\left([x,y]v_i+yxv_i\right)=$$

$$=\frac{1}{i+1}\left(hv_i+(\lambda-i+1)yv_{i-1}\right)=\frac{1}{i+1}\left((\lambda-2i)v_i+(\lambda-i+1)iv_i\right)=$$

$$=\frac{1}{i+1}\left((i+1)\lambda-2i-i^2+i\right)v_i=\frac{1}{i+1}\left((i+1)\lambda-i(i+1)\right)v_i=$$

$$= (\lambda - i)v_i.$$

■

Aplicando la fórmula del primer apartado del lema anterior, el lector puede demostrar sin dificultad que los vectores v_i son linealmente independientes. Tomemos el menor entero m tal que $v_m \neq 0$, $v_{m+1} = 0$. Entonces $v_{m+i} = 0$ para todo $i \geq 1$. Gracias a las formulas del lema anterior, tenemos que el subespacio de V generado por $v_0, \ldots, v_m$ es un L-submódulo de V (no nulo). Por el carácter irreducible de V se tiene entonces $V = \langle v_0, \ldots, v_m \rangle$. Se deja como ejercicio al lector el escribir explícitamente las matrices de los endomorfismos de V que representan a x, y y h en la base $\{v_0, \ldots, v_m\}$. Nótese que la matriz asociada a h es diagonal, mientras que las asociadas a x e y son triangulares una de ellas superior, y la otra inferior (aunque ambas nilpotentes).

La fórmula del apartado c) aplicada para $i = m + 1$ nos dice que $0 = (\lambda - m)v_m$ y como $v_m \neq 0$ tenemos $\lambda = m$. Es decir, el peso de un vector maximal es precisamente m, un entero no negativo que coincide con $\dim(V) - 1$. Este peso se llamará en lo sucesivo *peso máximo*. Además la fórmula a) del lema anterior demuestra que si $V_\mu \neq 0$, entonces $\dim(V_\mu) = 1$. En particular, un vector maximal de V es único salvo múltiplos escalares no nulos. Resumiéndolo todo:

Teorema 25 *Sea V un L-módulo irreducible.*

1. *Con relación a h, V admite una descomposición en suma directa de espacios pesos V_μ, con $\mu = m, m-2, \ldots, -(m-2), -m$ donde $m = \dim(V) - 1$, y $\dim(V_\mu) = 1$ para cada μ.*

2. *V tiene un único vector maximal (salvo múltiplos escalares no nulos), cuyo peso es m y se llama peso máximo.*

3. *La acción de L sobre V viene dada explícitamente por las fórmulas de los apartados a)-c) del lema anterior. En particular existe (salvo isomorfismos) un único L-módulo irreducible para cada posible dimensión $m + 1$ con $m \geq 0$.*

Corolario 15 *Sea V un L-módulo. Entonces los autovalores del endomorfismo de V que representa a h, son todos enteros y cada uno de ellos aparece junto con su opuesto (igual número de veces). En cualquier descomposición de V como suma directa de submódulos irreducibles, el número de sumandos es precisamente* $\dim(V_0) + \dim(V_1)$.

Dem. Teniendo en cuenta el Teorema de Weyl, Lo único que falta por demostrar es la segunda afirmación. Para ello téngase en cuenta que cada submódulo irreducible, tiene el peso 0 o el peso 1 (pero no ambos). ■

6.3. Descomposición en espacios raíces.

En toda esta sección L denotará una F-álgebra de Lie (no nula) semisimple de dimensión finita. Recordemos que el cuerpo F es algebraicamente cerrado y de característica cero. Vamos a estudiar en detalle la estructura de L a través de su representación adjunta. Nuestras principales herramientas serán por un lado la forma Killing y los teoremas 24 y 25 (ambos apoyándose de forma especial en el Teorema de Weyl).

Definición 17 *Sea M una F-álgebra de Lie y H una subálgebra cuyos elementos son todos semisimples (*ad*-semisimples). Entonces diremos que H es una subálgebra* toral.

Así como L es un álgebra no nilpotente, debe existir un elemento que no sea ad-nilpotente (Teorema de Engel). Por lo tanto si x es un tal elemento, su parte semisimple x_s en la descomposición abstracta de Jordan-Chevalley, nos proporciona la subálgebra Fx_s cuyos elementos son todos semisimples. Esta sería pues una subálgebra toral.

Lema 25 *Cualquier subálgebra toral es abeliana.*

Dem. Sea T la subálgebra toral y $x \in T$. Como $\mathrm{ad}_T(x) : T \to T$ es semisimple, será diagonalizable. Lo que se va a demostrar es que $\mathrm{ad}(x)T = 0$ para lo cual bastará demostrar que los autovalores de una matriz diagonal de $\mathrm{ad}_T(x)$ son todos nulos. Supongamos por el contrario que existe $y \in T$ tal que $\mathrm{ad}(x)y = \lambda y \neq 0$. Existe entonces una base de vectores propios de $\mathrm{ad}_T(y)$ o si se quiere una descomposición $T = \oplus T_i$ donde los T_i son los espacios unidimensionales generados por cada uno de los vectores de la base de vectores propios. Si descomponemos $x = \sum_i x_i$ con $x_i \in T_i$, entonces $\mathrm{ad}(y)x_i = \lambda_i x_i$, además

$$0 \neq \lambda y = -\mathrm{ad}(y)x = -\sum_i \lambda_i x_i \tag{6.1}$$

y también

$$0 = \mathrm{ad}(y)\lambda y = -\sum_i \lambda_i \,\mathrm{ad}(y)x_i = -\sum_i \lambda_i^2 x_i$$

de donde se tiene $\lambda_i = 0$ lo que contradice (6.1). ■

Fijemos ahora una subálgebra toral maximal H. Como H es abeliana, $\mathrm{ad}(H)$ es una familia de endomorfismos diagonalizables de L que conmutan entre sí. Un resultado de álgebra lineal relativamente elemental establece que si disponemos de una familia de endomorfismos de un espacio vectorial V que conmutan entre sí, y cada uno de los cuales diagonaliza al espacio V, entonces existe para V una descomposición en suma directa de subespacios tales que cada endomorfismo de la familia actúa como un múltiplo de la identidad, sobre cada uno de dichos sumandos directos. Podemos aplica este resultado a la familia $\mathrm{ad}(H)$ de endomorfismos semisimples de L que conmutan entre sí. Tenemos entonces que L es una suma directa de subespacios S_i tales que cada $\mathrm{ad}(h)$ $(h \in H)$ restringido a S_i es múltiplo escalar de la identidad. Para una base adecuada de L, obtenido mediante la unión

de bases de cada uno de los S_i, tenemos que la matriz de cada $\mathrm{ad}(h)$ con $h \in H$ es del tipo $\mathrm{diag}(B_i : i = 1, \ldots, k)$ donde cada B_i es un múltiplo escalar de la matriz identidad de orden $\dim(S_i)$. Si tomamos una base cualquiera $B = \{h_1, \ldots, h_r\}$ de H, entonces la matriz de cada $\mathrm{ad}(h_i)$ será:

$$\begin{pmatrix} \lambda_{i1}Id & 0 & \cdots & 0 \\ 0 & \lambda_{i2}Id & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & \lambda_{ik}Id \end{pmatrix}$$

Podemos ahora considerar la sucesiónes (finitas) de escalares $\lambda_{i1}, \ldots, \lambda_{ik}$ (una para cada i) y aprovecharla para definir las aplicaciones lineales $\alpha_j : H \to F$ (con $j = 1, \ldots, k$) dadas por $\alpha_j(h_i) := \lambda_{ij}$. Para un elemento $x \in S_j$ se tiene $[h_i, x] = \lambda_{ij}x = \alpha_j(h_i)x$, para cada i. Por lo tanto S_j está contenido en el conjunto

$$L_{\alpha_j} := \{x \in L : [h, x] = \alpha_j(h)x \forall h \in H\}.$$

Si para j y k fijos, ocurriera que $\lambda_{ij} = \lambda_{ik}$ para todo i, entonces también S_k estaría contenido en L_{α_j}. Recíprocamente, si $x \in L_{\alpha_j}$ entonces $[h_i, x] = \alpha_j(h_i)x = \lambda_{ij}x$ para todo i. Si se utiliza la matriz de arriba, se observa que entonces x debe pertenecer a la suma de los S_k para los que $\lambda_{ik} = \lambda_{ij}$ (para todo i). En definitiva cada $L_{\alpha_j} = \oplus_k S_k$ donde la suma está extendida a los k para los que $\lambda_{ik} = \lambda_{ij}$ para todo i (por ejemplo, esta suma siempre tiene el sumando S_j). Así pues la suma de los subespacios L_{α_j} es directa y coincide con L, pues no es más que una redistribución (y posible reagrupamiento) de los sumandos S_k. Podemos pues poner

$$L = \oplus_j L_{\alpha_i}.$$

Además dado que $L_{\alpha_j} \supset S_j$ siempre existe un vector no nulo (cualquier $x \in S_j - \{0\}$) tal que $[h, x] = \alpha_j(h)x$ (para todo $h \in H$). Supongamos ahora que $\alpha : H \to F$ es cualquier aplicación para la que existe un $x \neq 0$ verificando $[h, x] = \alpha(h)x$ para todo $h \in H$. El lector puede demotrar que entonces α coincide con algunas de las aplicaciones lineales α_j definidas antes (en particular α es lineal luego un elemento del espacio dual H^*).

De este modo la descomposición de L que hemos mencionado antes se puede describir del siguiente modo $L = \oplus L_\alpha$ donde

$$L_\alpha = \{x \in L : [h, x] = \alpha(h)x \forall\ h \in H\}$$

y $\alpha \in H^*$. Obsérvese que L_0 estaría formada por los elementos $x \in L$ tales que $[H, x] = 0$, es decir, $L_0 = C_L(H)$ es el centralizador de H en L y contiene a H por el Lema que asegura el carácter abeliano de H. Notemos también que la suma directa $L = \oplus L_\alpha$ está extendida a las $\alpha \in H^*$ para las que $L_\alpha \neq 0$. El conjunto

$$\Phi = \{\alpha \in H^* - \{0\} : L_\alpha \neq 0\}$$

se llamará *sistema de raíces*, y cada uno de sus elementos: *raíces* de L relativas a H. La descomposición

$$L = \oplus_\alpha L_\alpha = C_L(H) \oplus \left(\bigoplus_{\alpha \in \Phi} L_\alpha \right),$$

es lo que se llama la *descomposición de Cartan* de L relativa a H. Los subespacios L_α con $\alpha \neq 0$ se denominan *espacios raíces* de L con relación a H.

Nuestro próximo objetivo es demostrar que $C_L(H) = H$. Para ello necesitaremos algunas propiedades de los espacios raíces:

Lema 26 *Para cualesquiera $\alpha, \beta \in H^*$, se tiene $[L_\alpha, L_\beta] \subset l_{\alpha+\beta}$. Si $\alpha \neq 0$ y $x \in L_\alpha$, entonces* $\mathrm{ad}(x)$ *es nilpotente. Si $\alpha, \beta \in H^*$, $\alpha + \beta \neq 0$, entonces L_α es ortogonal a L_β respecto a la forma Killing k de L.*

Dem. Si tomamos $x \in L_\alpha$, $y \in L_\beta$, entonces

$$[h,[x,y]] = -[x,[y,h]] - [y,[h,x]] = \beta(h)[x,y] - \alpha(h)[y,x] = (\alpha+\beta)(h)[x,y].$$

Lo que demuestra que $[x,y] \in L_{\alpha+\beta}$. El carácter nilpotente de $\mathrm{ad}(x)$ para $x \in L_\alpha$ (con $\alpha \neq 0$) se tiene del siguiente modo: entre los subespacios del conjunto $\{L_{k\alpha+\beta} : k = 1, 2, \ldots\}$ no puede haber una cantidad infinita de ellos no nulos (pues L es de dimensión finita y la suma de los subespacios no nulos del citado conjunto es directa). Por lo tanto no todas las aplicaciones $k\alpha + \beta$ son raíces. Aquellas que no lo sean satisfacen $L_{k\alpha+\beta} = 0$. Ahora bien $\mathrm{ad}(x)^k L_\beta \subset L_{k\alpha+\beta} = 0$. Como L es una suma de espacios L_β tenemos que $\mathrm{ad}(x)^n$ se anula para conveniente $n \geq 1$. Veamos finalmente la ortogonalidad de L_α y L_β respecto de k cuando $\alpha + \beta \neq 0$. Sea $h \in H$ tal que $(\alpha+\beta)(h) \neq 0$. Tomemos $x \in L_\alpha$, $y \in L_\beta$, y efectuemos el siguiente cálculo:

$$\alpha(h)k(x,y) = k([h,x],y) = -k([x,h],y) = -k(x,[h,y]) - \beta(h)k(x,y).$$

Por lo tanto $(\alpha+\beta)(h)k(x,y) = 0$ implicando $k(x,y) = 0$. ■

Corolario 16 *La restricción de la forma Killing k de L a $L_0 = C_L(H)$ es no degenerada.*

Dem. Sabemos que k es no degenerada por ser L semisimple. Además L_0 es ortogonal a cada L_α con $\alpha \neq 0$. Como la no degeneración pasa a sumandos directos ortogonales, el corolario está demostrado. ■

Proposición 15 *Sea H una subálgebra toral maximal de L. Entonces $H = C_L(H)$.*

Dem. Sea $C = C_L(H)$. La demostración se hará en una serie de pasos.

1. C contiene las partes semisimple y nilpotente de cada uno de sus elementos. En efecto, $x \in C$ si y sólo si $[x,H] = 0$. Las partes semisimple y nilpotente de $\mathrm{ad}(x)$ en $\mathfrak{gl}(L)$ vamos a denotarlas por $(\mathrm{ad}(x))_s$ y $(\mathrm{ad}(x))_n$ respectivamente. Entonces, como $(\mathrm{ad}(x))_s$ y $(\mathrm{ad}(x))_n$ se escriben como polinomios en $\mathrm{ad}(x)$ (sin término independiente), resulta que $(ad(x))_s H = 0$, $(\mathrm{ad}(x))_n H = 0$. Como $(\mathrm{ad}(x))_s = \mathrm{ad}(x_s)$, $(\mathrm{ad}(x))_n = \mathrm{ad}(x_n)$ resulta entonces que $x_s, x_n \in C$.

2. Todos los elementos semisimples de C están en H. Si $x \in C$ es semisimple consideremos el subespacio $H + Fx \supset H$. Este subespacio es en realidad una subálgebra de elementos semisimples (la suma de elementos semisimples que conmutan es semisimple). Por maximalidad de H se tiene $H = H + Fx$ lo que implica $x \in H$.

3. La restricción de k a H es no degenerada. Supongamos que $k(h, H) = 0$. Demostremos que también $k(h, C) = 0$ (lo que implicará $h = 0$ en vista del Corolario 16). Sea $c = x + s \in C$, donde x es la parte nilpotente de c y s es la semisimple. Sabemos que $x, s \in C$ y además $s \in H$. Por lo tanto $k(h, c) = k(h, x) = \mathrm{Tr}(\mathrm{ad}(h)\,\mathrm{ad}(x))$. Como $\mathrm{ad}(x)$ es nilpotente, y los endomorfismos $\mathrm{ad}(x)$ y $\mathrm{ad}(h)$ conmutan, el endomorfismo $\mathrm{ad}(h)\,\mathrm{ad}(x)$ es nilpotente y su traza es nula. Así $k(h, x) = 0$ y hemos demostrado que $k(h, C) = 0$.

4. C es nilpotente. Si $x \in C$ es semisimple, entonces $x \in H$ luego $\mathrm{ad}_C(x) : C \to C$ es la aplicación nula. Sea ahora $x \in C$ arbitrario, entonces consideremos la descomposición de Jordan-Chevalley (abstracta) de x dada por $x = x_s + x_n$. Podemos escribir entonces $\mathrm{ad}_C(x) = \mathrm{ad}_C(x_n)$ que es nilpotente. El Teorema de Engel implica entonces que C es nilpotente.

5. $H \cap [C, C] = 0$. Como k es asociativa $k(H, [C, C]) = 0$. Si $z \in H \cap [C, C]$ se tiene entonces $k(H, z) = 0$ y por la no degeneración de la restricción de k a H, tenemos $z = 0$.

6. C es abeliana. En caso contrario $[C, C] \neq 0$, pero siendo C nilpotente, el Lema 15 implica que $Z(C) \cap [C, C] \neq 0$. Sea pues z un elemento no nulo de esta intersección. Si z fuera semisimple, sería elemento de H y como $H \cap [C, C] = 0$ llegaríamos al absurdo de que $z = 0$. Por lo tanto la parte nilpotente n de z es no nula y está en C por el primer apartado de esta demostración. Sabemos también que $\mathrm{ad}(n)$ anula a cada subespacio que sea anulado por $\mathrm{ad}(z)$ (ya que $\mathrm{ad}(n)$ es la parte nilpotente de $\mathrm{ad}(z)$). Como $\mathrm{ad}(z)C = 0$ se tiene entonces $\mathrm{ad}(n)C = 0$, es decir, $n \in \mathrm{Z}(C)$. Pero $\mathrm{ad}(n)\,\mathrm{ad}(C)$ es nilpotente (composición de un nilpotente con otro endomorfismo que conmuta con el primero). Por lo tanto $k(n, C) = \mathrm{Tr}(\mathrm{ad}(n)\,\mathrm{ad}(C)) = 0$. Como la restricción de k a C es no degenerada tenemos $n = 0$ lo cual es una contradicción.

7. $C = H$. En caso contrario hay un elemento no semisimple en C (luego su parte nilpotente es un elemento no nulo de C). Sea entonces $0 \neq x \in C$ (nilpotente). Tenemos otra vez que $\mathrm{ad}(x)\,\mathrm{ad}(y)$ es nilpotente para $y \in C$ luego $k(x, y) = 0$. Como $k|_{C \times C}$ es no degenerada $x = 0$ contradiciendo nuestra suposición inicial.

■

Conviene resaltar de la demostración de este teorema, el hecho de que la restricción de la forma Killing k de L a H es no degenerada. Esto permite un identificación de H y H^* en el sentido de que a cada $\phi \in H^*$ (no nula) corresponde un único $t_\phi \in H$ tal que $\phi(t) = k(t_\phi, t)$ para todo $t \in H$.

Definición 18 *Dada $0 \neq \phi \in H^*$, denotaremos por t_ϕ al único elemento de H tal que $\phi(t) = k(t_\phi, t)$ para todo $t \in H$.*

Es elemental observa que $t_\phi \neq 0$. Extenderemos esta definición al caso $\phi = 0$, escribiendo $t_\phi := 0$.

6.4. Propiedades de los espacios raíces.

En esta sección seguiremos con las hipótesis ya habituales para L (semisimple de dimensión finita) y para el cuerpo base (algebraicamente cerrado de característica cero). Supondremos que H es una subálgebra toral maximal, y Φ el conjunto de elementos $\alpha \in H^* - \{0\}$ tales que $L_\alpha \neq 0$, es decir, el conjunto de raíces de L respecto a H. En la sección anterior hemos demostrado que L_α y L_β son ortogonales respecto a la forma Killing de L cuando $\alpha + \beta \neq 0$. En particular H es ortogonal a cada espacio raíz L_α.

Proposición 16 *Bajo las condiciones de ambiente descritas arriba, se tiene:*

(a) Φ genera H^*.

(b) Si $\alpha \in \Phi$, entonces $-\alpha \in \Phi$.

(c) Sea $\alpha \in \Phi$, $x \in L_\alpha$, $y \in L_{-\alpha}$. Entonces $[x, y] = k(x, y)t_\alpha$ (véase la definición 18).

(d) Si $\alpha \in \Phi$, entonces $[L_\alpha, L_{-\alpha}]$ es de dimensión uno con base $\{t_\alpha\}$.

(e) $\alpha(t_\alpha) = k(t_\alpha, t_\alpha) \neq 0$ para $\alpha \in \Phi$.

(f) Si $\alpha \in \Phi$, y $x_\alpha \neq 0$ es un elemento de L_α, entonces existe $y_\alpha \in L_{-\alpha}$ tal que $\{x_\alpha, y_\alpha, h_\alpha := [x_\alpha, y_\alpha]\}$ genera una subálgebra tridimensional simple de L isomorfa a $\mathfrak{sl}(2, F)$ mediante $x_\alpha \mapsto e_{12}$, $y_\alpha \mapsto e_{21}$, $h_\alpha \mapsto e_{11} - e_{22}$.

(g) $h_\alpha = 2t_\alpha / k(t_\alpha, t_\alpha)$ y $h_{-\alpha} = h_\alpha$.

Dem. (a) Consideremos un subconjunto Φ_0 de Φ, linealmente independiente y que genere el mismo subespacio de H^* que Φ (es decir $< \Phi_0 >=< \Phi >$). Si Φ no genera H^*, ampliemos el conjunto Φ_0 a una base $B^* := \Phi_0 \cup \Phi'$ de H^*. Si consideramos la base dual B de B^*, entonces existen elementos de B que son anulados por todas las aplicaciones de Φ_0 (luego por todas las de Φ). Supongamos pues que $h \in H$ es un elemento (no nulo) tal que $\alpha(h) = 0$ para toda $\alpha \in \Phi$. Esto implica que $[h, L_\alpha] = 0$ (para cada $\alpha \in \Phi$. Por consiguiente $[h, L] = 0$ y $h \in \mathrm{Z}(L) = 0$ lo que es absurdo.

(b) Tomemos $\alpha \in \Phi$ y supongamos que $-\alpha$ no es una raíz. Como $L_{-\alpha} = 0$, entonces $k(L_\alpha, L_\beta) = 0$ para toda $\beta \in H^*$. Esto implica que $k(L_\alpha, L) = 0$ contradiciendo la no degeneración de k.

(c) Sean $\alpha \in \Phi$, $x \in L_\alpha$, $y \in L_{-\alpha}$. Sea $h \in H$ arbitrario. Entonces

$$k(h, [x, y]) = k([h, x], y) = \alpha(h)k(x, y) = k(t_\alpha, h)k(x, y) = k(k(x, y)t_\alpha, h) =$$

$$= k(h, k(x,y)t_\alpha)$$

luego $[x,y] - k(x,y)t_\alpha$ es un elemento de H ortogonal a todo H lo que implica $[x,y] = k(x,y)t_\alpha$.

(d) El apartado anterior muestra que si $[L_\alpha, L_{-\alpha}] \neq 0$ entonces tiene dimensión uno. Para demostrar la no nulidad del anterior producto de espacios, supongamos que $x \in L_\alpha$ es tal que $[x, L_{-\alpha}] = 0$. Entonces aplicando la fórmula del apartado anterior $0 = [x, L_{-\alpha}] = k(x, L_{-\alpha})t_\alpha$ lo que quiere decir que $k(x, L_{-\alpha}) = 0$, es decir, $k(x, L) = 0$ lo que por no-degeneración de k implica $x = 0$. Así $[L_\alpha, L_{-\alpha}] \neq 0$.

(e) Supongamos que $\alpha(t_\alpha) = k(t_\alpha, t_\alpha) = 0$, entonces $[t_\alpha, x] = 0 = [t_\alpha, y]$ para cualesquiera $x \in L_\alpha$, $y \in L_{-\alpha}$. Aplicando el apartado (d) podemos encontrar $x \in L_\alpha$, $y \in L_{-\alpha}$ tales que $k(x,y) \neq 0$. Multiplicando por un escalar conveniente, podemos suponer que $k(x,y) = 1$. Entonces $[x,y] = t_\alpha$. El subespacio S de L generado por $\{x, y, t_\alpha\}$ es un álgebra tridimensional soluble (su tabla de multiplicar vendría dada por las relaciones $[t_\alpha, x] = [t_\alpha, y] = 0$, $[x,y] = t_\alpha$ luego $[S,S] = Ft_a$ y $[[S,S],[S,S]] = 0$. El Corolario 11 nos dice que entonces $\mathrm{ad}(s)$ es nilpotente para cada $s \in [S,S] = Ft_\alpha$. De este modo $\mathrm{ad}(s)$ es a la vez nilpotente y semisimple lo que implica su nulidad. Ahora bien, decir que $ad(t_\alpha) = 0$ es lo mismo que asegurar que $t_\alpha \in \mathrm{Z}(L) = 0$ una contradicción.

(f) Dado $0 \neq x_\alpha \in L_\alpha$, existe $y \in l_{-\alpha}$ tal que $k(x_\alpha, y) \neq 0$. Multiplicando por un escalar conveniente podemos decir que existe $y_\alpha \in L_{-\alpha}$ de modo que $k(x_\alpha, y_\alpha) = 2/k(t_\alpha, t_\alpha)$. Definamos $h_\alpha = 2t_\alpha/k(t_\alpha, t_\alpha)$. Entonces $[x_\alpha, y_\alpha] = k(x_\alpha, y_\alpha)t_\alpha = h_\alpha$. Más aún,

$$[h_\alpha, x_\alpha] = \frac{2}{k(t_\alpha, t_\alpha)}[t_\alpha, x_a] = \frac{2\alpha(t_\alpha)}{k(t_\alpha, t_\alpha)}x_\alpha = 2x_a,$$

ya que $\alpha(t_\alpha) = k(t_\alpha, t_\alpha)$. Del mismo modo se demuestra que $[h_\alpha, y_\alpha] = -2y_\alpha$. Por lo tanto $\{h_\alpha, x_\alpha, y_\alpha\}$ es una subálgebra tridimensional de L con la misma tabla de multiplicar que $\mathfrak{sl}(2, F)$.

(g) Solo falta demostrar que $h_\alpha = -h_{-\alpha}$. Pero es evidente que $t_{-\alpha} = -t_\alpha$ y por lo tanto

$$h_{-\alpha} = \frac{2t_{-\alpha}}{k(t_{-\alpha}, t_{-\alpha})} = -\frac{2t_\alpha}{k(t_\alpha, t_\alpha)} = -h_\alpha.$$

■

Para cada par de raíces $\alpha, -\alpha \in \Phi$, sea $S_\alpha \cong \mathfrak{sl}(2, F)$ la subálgebra de L construida como en el apartado (f) de la Proposición 16. Gracias al Teorema de Weyl, disponemos de una descripción completa de todos los S_α-módulos de dimensión finita. En particular, disponemos de información sobre $\mathrm{ad}(S_\alpha)$. Esto será útil en la demostración de la siguiente proposición.

Proposición 17 *Bajo las condiciones de ambiente descritas arriba, se tiene:*

(a) Si $\alpha \in \Phi$, $\dim(L_\alpha) = 1$. En particular $S_\alpha = L_\alpha + L_{-\alpha} + H_\alpha$ (donde $H_\alpha = [L_\alpha, L_{-\alpha}]$). Para un elemento no nulo dado $x_\alpha \in L_\alpha$ existe un único $y_\alpha \in L_{-\alpha}$ tal que $[x_\alpha, y_\alpha] = h_\alpha$.

(b) Si $\alpha \in \Phi$ los únicos múltiplos escalares de α que son raíces son α y $-\alpha$.

(c) Si $\alpha, \beta \in \Phi$, entonces $\beta(h_\alpha) \in \mathbb{Z}$, $\beta - \beta(h_\alpha)\alpha \in \Phi$ (los números $\beta(h_\alpha)$ se llaman **enteros de Cartan**.

(d) Si $\alpha, \beta, \alpha + \beta \in \Phi$, entonces $[L_\alpha, L_\beta] = L_{\alpha+\beta}$.

(e) Sean $\alpha, \beta \in \Phi$, $\beta \neq \pm\alpha$. Sean r y q los mayores enteros para los que $\beta - r\alpha$ y $\beta + q\alpha$ son raíces. Entonces todas las aplicaciones $\beta + i\alpha \in \Phi$ para $-r \leq i \leq q$. Además $\beta(h_\alpha) = r - q$.

(f) L está generada como álgebra de Lie por los espacios raíces L_α.

Dem. (a) Sea M el subespacio de L generado por H y por todos los espacios raíces $L_{c\alpha}$ con $c \in F^*$. Es evidente que M es un S_α-submódulo de L para la acción $sm = \mathrm{ad}(s)m$ para todo $s \in S_\alpha$, $m \in M$. Los pesos de M bajo la acción de S_α son 0 y los escalares $c\alpha(h_\alpha) = 2c$ donde c varía en el conjunto de elementos de F^* tales que $L_{c\alpha} \neq 0$. Como los pesos son todos enteros (véase el Corolario al Teorema 25), entonces c debe ser múltiplo entero de $1/2$. Como $M = H \oplus (\oplus_c V_{c\alpha}$, la restricción de $\mathrm{ad}(h_\alpha)$ a H se representa diagonalmente como la matriz nula de orden $r := \dim(H)$. Por otra parte la restricción $\mathrm{ad}(h_\alpha)$ a cada $V_{c\alpha}$ se representa por una matriz que es un múltiplo escalar de la identidad (el múltiplo es $c\alpha(h_\alpha) = 2c \neq 0$). En resumen el número de veces que aparece el peso 0 para $\mathrm{ad}(h_\alpha)$, es justamente $r = \dim(H)$. Por otra parte una descomposición de M como suma directa de S_α-módulos irreducibles es

$$M = Fh_1 \oplus \cdots Fh_{r-1} \oplus S_\alpha \oplus R$$

donde $\{h_1, \ldots, h_{r-1}, h_\alpha\}$ es una base de H y R es nulo, o una suma directa de submódulos irreducibles. Como el peso 0 aparece una vez para cada sumando Fh_i y otra vez para el sumando S_α, resulta que en los sumandos directos irreducibles cuya suma es R (si hay alguno), no aparece el peso 0. En consecuencia los pesos de estos submódulos son todos impares y hemos demostrado que los únicos pesos pares de M para $\mathrm{ad}(h_\alpha)$ son 0 y ± 2. Una implicación directa de este hecho es que 2α nunca puede ser raíz (pues de serlo, cualquier vector no nulo de $L_{2\alpha}$ produciría el peso 4). Por lo tanto $\alpha/2$ no es tampoco raíz (si lo fuera, $2\alpha/2 = \alpha$ no podría ser raíz). Si $\alpha/2$ no es raíz, el peso 1 no puede aparecer para $\mathrm{ad}(h_\alpha)$. Esto quiere decir que $R = 0$ pues en caso contrario, cualquier sumando irreducible suyo, tendría el peso 1. En definitiva $M = H + S_\alpha = H \oplus L_\alpha \oplus \ L_{-\alpha}$ lo que implica que $\dim(L_\alpha) = 1$. Como corolario $S_\alpha = L_\alpha + L_{-\alpha} + [L_\alpha, L_{-\alpha}]$. En resumen hemos demostrado los apartados (a) y (b) de esta proposición. Para demostrar los restantes vamos a construir otro S_α-módulo interesante. Vamos a estudiar como actúa S_α sobre los espacios raíces L_β con $\beta \neq \pm\alpha$. Definamos $K := \sum_{i\in\mathbb{Z}} L_{\beta+i\alpha}$. Cada sumando de K es de dimensión uno según acabamos de demostrar. Por otra parte para ningún i puede ocurrir $\beta + i\alpha = 0$. Está claro entonces, que K es un S_α-módulo con espacios peso de dimensión uno para los distintos pesos $\beta(h_\alpha) + 2i$ (con $i \in \mathbb{Z}$ tal que $\beta + i\alpha \in \Phi$) de $\mathrm{ad}(h_\alpha)$. Obviamente los pesos 0 y 1 no pueden aparecer simultáneamente (la diferencia entre dos pesos es siempre par). Aplicando

el Corolario 15 el número de componente irreducibles en la descomposición de K como submódulos irreducibles es $\dim(K_0)$ o $\dim(K_1)$ (ambos valen 1 por ser los espacios pesos de dimensión uno). Así K es irreducible. Supongamos que el peso máximo es $\beta(h_\alpha)+2q$ y el mínimo $\beta(h_\alpha)-2r$. Entonces q es la máximo entero tal que $\beta+q\alpha$ es una raíz y r el máximo entero tal que $\beta-r\alpha$ es una raíz. Además los pesos de $\mathrm{ad}(h_\alpha)$ sobre K forman un progresión aritmética de diferencia 2 (recuérdese el Teorema 25). Por lo tanto las raíces del tipo $\beta+i\alpha$ forman una cadena

$$\beta-r\alpha,\ldots,\beta,\ldots,\beta+q\alpha,$$

que se llama *la α-cadena por β*. Como consecuencia también del Teorema 25, $\beta(h_\alpha)+2q=-(\beta(h\alpha)-2r)$, es decir, $\beta(h_\alpha)=r-q$. Para demostrar el apartado (d), téngase en cuenta que si $\alpha,\beta,\alpha+\beta\in\Phi$, $ad(L_\alpha)$ transforma L_β en $L_{\alpha+\beta}$ sobreyectivamente (véase el Lema 24). Esto demuestra que $[L\alpha,L_\beta]=L_{\alpha+\beta}$. Finalmente el apartado (f) se puede ver así: $L=[L,L]$ (esto es obvio para el caso en que L es simple pero se extiende fácilmente al caso semisimple). Haciendo uso de la descomposición de Cartan $L=H\oplus V$ donde V es la suma de los espacios raíces, tenemos

$$L=[L,L]=[H+V,H+V]\subset V+[V,V]$$

lo que confirma que L está generada como álgebra de Lie por los espacios raíces. ■

Como corolario del hecho de que L está generado como álgebra de Lie por los espacios raíces, observaremos que H esta generada por los elementos t_α con $\alpha\in\Phi$. En efecto sabemos que $L=V+[V,V]$ donde V es la suma de los espacios raíces. Entonces los únicos elementos de H que están en dicha suma son los de la intersección $H\cap[V,V]$, pero estos son precisamente los del tipo $[L_\alpha,L_{-\alpha}]$ con $\alpha\in\Phi$. Es decir H está generada (como espacio vectorial) por los t_α.

Por otra parte como la restricción de la forma Killing k a H es no degenerada, podemos definir en el dual H^* una forma bilineal simétrica dada por $(\ ,\ ):H^*\times H^*\to F$, con $(\alpha,\beta):=k(t_\alpha,t_\beta)$ para cualesquiera $\alpha,\beta\in H^*$. La no degeneración de $(\ ,\ )$ se demuestra así: si $(\alpha,H^*)=0$ entonces $k(t_\alpha,t_\beta)=0$ para todo $\beta\in H^*$. Como H está generada por los t_β tenemos entonces $k(t_\alpha,H)=0$ lo que implica (por la no degeneración de $k|_{H\times H}$) que $t_\alpha=0$. Pero entonces $\alpha(h)=k(t_\alpha,h)=0$ para todo h. Es decir $\alpha=0$.

Fijemos ahora una base $\{\alpha_1,\ldots,\alpha_l\}$ de H^* formada enteramente por raíces (esto es posible ya que Φ genera a H^*). Dados dos elementos α_i y α_j de dicha base, vamos a demostrar que el escalar

$$\frac{2(\alpha_i,\alpha_j)}{(\alpha_j,\alpha_j)}$$

es un entero. Según el apartado (c) de la Proposición 17, $\alpha_i(h_{\alpha_j})\in\mathbb{Z}$ para cualesquiera i,j. Pero

$$\alpha_i(h_{\alpha_j})=\frac{2\alpha_i(t_{\alpha_j})}{k(t_{\alpha_j},t_{\alpha_j})}=\frac{2k(t_{\alpha_i},t_{\alpha_j})}{k(t_{\alpha_j},t_{\alpha_j})}=\frac{2(\alpha_i,\alpha_j)}{(\alpha_j,\alpha_j)}.$$

Teorema 26 *El $\mathbb{Q}$-subespacio $E_{\mathbb{Q}}$ de H^* formado por las combinaciones lineales con coeficientes racionales de las α_i, tiene Q-dimensión $l = \dim_F(H^*)$. Ademas $E_{\mathbb{Q}}$ contiene a Φ.*

Dem. Como $\{\alpha_1, \ldots, \alpha_l\}$ es una base de H^* y la forma bilineal $(\ ,\ )$ es no degenerada, la matriz $((\alpha_i, \alpha_j))_{i,j=1}^{l}$ tiene determinante no nulo. Lo mismo le ocurre entonces a la matriz cuyo coeficiente (i, j) es $(\alpha_i, \alpha_j)/(\alpha_j, \alpha_j)$. Para demostrar que $\dim_{\mathbb{Q}}(E_{\mathbb{Q}}) = \dim_F(H^*)$, bastara comprobar que $\{\alpha_1, \ldots, \alpha_l\}$ es una $\mathbb{Q}$-base de $E_{\mathbb{Q}}$. Evidentemente dicho conjunto es linealmente independiente sobre $\mathbb{Q}$ (pues es F-linealmente independiente). Así pues, lo único que nos falta por demostrar es que $\Phi \subset E_{\mathbb{Q}}$. Dada $\beta \in \Phi$ arbitraria, sabemos que $\beta = \sum_{i=1}^{l} c_i\alpha_i$ donde $c_i \in F$. Vamos a demostrar que en realidad $c_i \in \mathbb{Q}$. Obsérvese que para cada j se tiene $(\beta, \alpha_j) = \sum_i c_i(\alpha_i, \alpha_j)$ y por lo tanto

$$2\frac{(\beta, \alpha_j)}{(\alpha_j, \alpha_j)} = \sum_i \frac{2(\alpha_i, \alpha_j)}{(\alpha_j, \alpha_j)} c_i.$$

Esto se puede considerar como un sistema de l ecuaciones con l incógnitas (las c_i), con coeficientes racionales. Como la matriz cuyo coeficiente (i, j) es (α_i, α_j) es no singular, la matriz del sistema también lo es. Así la Regla de Cramer implica que el sistema tiene solución única sobre $\mathbb{Q}$, en las c_i. ■

Finalicemos esta sección con algunas consideraciones. Si $\lambda, \mu \in H^*$, se tiene $(\lambda, \mu) = k(t_\lambda, t_\mu) = \sum_\alpha k(t_\lambda, t_\alpha)k(t_\alpha, t_\mu)$ (véase el problema 89). Entonces $(\lambda, \mu) = \sum_{\alpha\in\Phi}(\lambda, \alpha)(\alpha, \mu)$. En particular $(\beta, \beta) = \sum_\alpha(\alpha, \beta)^2$ para $\beta \in \Phi$. Equivalentemente, $1/(\beta, \beta) = \sum_{\alpha\in\Phi}(\alpha, \beta)^2/(\beta, \beta)^2$. Como

$$2(\alpha, \beta)/(\beta, \beta) \in \mathbb{Z},$$

tenemos que $(\beta, \beta) \in \mathbb{Q}$ (implicando $(\alpha, \beta) \in \mathbb{Q}$). En definitiva todos los productos escalares de vectores de $E_{\mathbb{Q}}$ son racionales y por lo tanto $(\ ,\ )$ es una forma bilineal simétrica en $E_{\mathbb{Q}}$. Como además $(\lambda, \lambda) = \sum(\lambda, \alpha)^2$, esta forma es definida positiva. Extendamos ahora escalar a $\mathbb{R}$, es decir, consideremos el espacio vectorial real $E = E_{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathbb{R}$. El producto escalar $(\ ,\ ) : E_{\mathbb{Q}} \times E_{\mathbb{Q}} \to \mathbb{Q}$ se extiende automáticamente a un producto escalar $E \times E \to \mathbb{R}$ definido positivo. Así E es un espacio euclídeo, Φ contiene una base de E, y $\dim_{\mathbb{R}}(E) = l$. Resumiendo esta serie de resultados podemos enunciar el siguiente teorema.

Teorema 27 *Sean L, H y E como arriba. Entonces:*

(a) Φ genera a E y 0 no pertenece a Φ.

(b) Si $\alpha \in \Phi$ entonces $-\alpha \in \Phi$ y ningún otro múltiplo escalar de α es una raíz.

(c) Si $\alpha, \beta \in \Phi$, entonces $\beta - \frac{2(\beta,\alpha)}{(\alpha,\alpha)}\alpha \in \Phi$.

(d) Si $\alpha, \beta \in \Phi$, entonces $\frac{2(\beta,\alpha)}{(\alpha,\alpha)} \in \mathbb{Z}$.

Utilizando el lenguaje del siguiente capítulo, este último teorema afirma que Φ es un sistema de raíces en el espacio euclídeo E. Hemos establecido una correspondencia entre las parejas (L, H) y los pares (Φ, E). Estos pares (Φ, E) se clasificarán completamente en el siguiente capítulo. Más tarde veremos que esta correspondencia que acabamos de establecer es un realidad una biyección y que la aparente dependencia de Φ de la elección de subálgebra toral maximal H no es esencial.

6.5. Problemas.

Problema 89 *Demuéstrese que bajo las hipótesis habituales (L álgebra de Lie semisimple de dimensión finita sobre un cuerpo algebraicamente cerrado de característica cero), se tiene $k(t_\lambda, t_\mu) = \sum_\alpha k(t_\lambda, t_\alpha)k(t_\alpha, t_\mu)$ donde la suma está extendida a las $\alpha \in \Phi$. Sugerencia: encuéntrese la matriz de $\mathrm{ad}(t_\gamma)$ teniendo en cuenta la descomposición de Cartan de L respecto a su subálgebra toral maximal H).*

Problema 90 *Encuéntrese una subálgebra toral maximal H de $L = \mathfrak{sl}(n, F)$ y realícese la descomposición de Cartan de L respecto a H. Sugerencia: hágase primero para $n = 3$.*

Problema 91 *Encontrar una subálgebra toral maximal de $L = so(3, 1, \mathbb{C})$ (álgebra de Lie del grupo de Lorentz) que llamaremos H y de hacer la descomposición de Cartan de L respecto a H. Después se pide estudiar la simplicidad de L. Se recuerda al lector que el álgebra L es la formada por todas las matrices de la forma*

$$\begin{pmatrix} 0 & x & y & a \\ -x & 0 & z & b \\ -y & -z & 0 & c \\ a & b & c & 0 \end{pmatrix}.$$

Problema 92 *Sea $\mathfrak{g}_2$ el álgebra de derivaciones del álgebra de octoniones complejos (isomorfa al álgebra de matrices de Zorn sobre los complejos). Demuéstrese que es semisimple, calcúlese una subálgebra toral maximal y hágase la descomposición de Cartan de $\mathfrak{g}_2$ respecto a dicha subálgebra toral. Demuéstrese que $\mathfrak{g}_2$ es simple y de dimensión catorce.*

Problema 93 *En el espacio complejo $V = \mathbb{C}^4$ se considera la forma bilineal alternada $f : V \times V \to \mathbb{C}$ tal que $f(x, y) = xFy^t$ donde F es la matriz diagonal por bloques $F = diag(S, S)$ siendo S la matriz simpléctica dos por dos ($S = e_{12} - e_{21}$). Sea L el álgebra de Lie formada por todas las $T \in \mathfrak{gl}(V)$ tales que $f(T(x), y) + f(x, T(y)) = 0$ para cualesquiera $x, y \in V$. Encuéntrese una forma matricial de L, una subálgebra toral maximal H, así como la descomposición de Cartan de L respecto de H (justificando su existencia). ¿Es L simple?*

Problema 94 *Demostrar que $so(4, \mathbb{C})$ es semisimple y encuéntrese una descomposición de Cartan para este álgebra. ¿Es simple?*

Problema 95 *Sea L un álgebra de Lie semisimple y de dimensión finita sobre un cuerpo F algebraicamente cerrado de característica cero. Supongamos que $L = I \oplus J$ donde $0 \neq I, J \lhd L$. Sabemos que entonces, tanto I como J son álgebras semisimples. Existen entonces subálgebras torales maximales H_I y H_J de I y J respectivamente. Supongamos dadas las descomposiciones en espacios raíces de I y J:*

$$I = H_I \oplus (\oplus_{\alpha \in \Phi_I} I_\alpha), \quad J = H_J \oplus (\oplus_{\beta \in \Phi_J} J_\beta).$$

Demuéstrese que entonces $H := H_I \oplus H_J$ es una subálgebra toral maximal de L y que la descomposición en espacios raíces de L con relación a H es

$$L = H \oplus (\oplus_{\alpha \in \Phi_I} I_\alpha) \oplus (\oplus_{\beta \in \Phi_J} J_\beta),$$

por lo tanto el sistema de raíces de L respecto de H es $\Phi = \Phi_I \dot{\cup} \Phi_J$. Compruébese que entonces $\alpha \perp \beta$ para cualesquiera $\alpha \in \Phi_I$, $\beta \in \Phi_J$.

Problema 96 *Sea L como en el problema anterior y H una subálgebra toral maximal de modo que la descomposición en espacios raíces de L respecto de H es $L = H \oplus (\oplus_{\alpha \in \Phi} L_\alpha)$. Supongamos que hay una partición no trivial del sistema de raíces Φ de la forma $\Phi = \Phi_1 \dot{\cup} \Phi_2$ donde cada raíz de Φ_1 es ortogonal a todas las de Φ_2. Definamos $H_i = \sum_{\alpha \in \Phi_i} Ft_\alpha$ para $i = 1, 2$. Compruébese que entonces*

$$L_i := H_i \oplus (\oplus_{\alpha \in \Phi_i} L_\alpha) \tag{6.2}$$

$(i = 1, 2)$ son dos ideales propios de L, tales que $L = L_1 \oplus L_2$. Compruébese que H_i es una subálgebra toral maximal de L_i induciendo la descomposición en espacios raíces dada por (6.2).

Capítulo 7

Sistemas de raíces

7.1. Preliminares.

En todo este capítulo trabajaremos con un espacio euclídeo E sobre los reales (es decir un $\mathbb{R}$-espacio de dimensión finita provisto de una forma bilineal simétrica definida positiva o producto escalar). Denotaremos por (α, β) el producto escalar de los elementos $\alpha, \beta \in E$.

Recordemos que una reflexión en E es un automorfismo del espacio vectorial E tal que fija punto a punto a un hiperplano de E y transforma un vector no nulo ortogonal al hiperplano en su opuesto. Cada reflexión es un elemento del grupo ortogonal[1] $O(E, (\ ,\ ))$. Dado un vector no nulo $\alpha \in E$ podemos considerar el hiperplano $\alpha^{\perp}$. Denotaremos entonces por σ_α la reflexión en el hiperplano $\alpha^{\perp}$ cuya expresión es

$$\sigma_\alpha(\beta) = \beta - \frac{2(\beta, \alpha)}{(\alpha, \alpha)}\alpha,$$

para cada $\beta \in E$. Como el escalar $2(\alpha, \beta)/(\alpha, \alpha)$ va a aparecer frecuentemente en lo sucesivo, vamos a denotarlo por $< \beta, \alpha >$. Obsérvese que la aplicación que cada pareja de vectores $(\alpha, \beta) \in E \times E$ le asigna el real $< \alpha, \beta >$, sólo es lineal en α.

Lema 27 *Sea Φ un conjunto finito que genera E tal que todas las reflexiones σ_α con $\alpha \in \Phi$ dejan Φ invariante. Si $\sigma \in GL(E)$ es tal que:*

1. *Deja invariante a Φ,*
2. *Fija punto a punto un hiperplano P de E,*
3. *Transforma un α no nulo de Φ en su opuesto,*

entonces $\sigma = \sigma_\alpha$ y P es el hiperplano fijo de σ.

[1] Formado por los automorfismos f del vectorial subyacente a E tales que $(f(x), f(y)) = (x, y)$ con $x, y \in E$.

Dem. Definamos $\tau = \sigma\sigma_\alpha$, entonces $\tau(\Phi) = \Phi$, y $\tau(\alpha) = \alpha$. Por lo tanto τ actúa como la identidad sobre la recta $\mathbb{R}\alpha$. Consideremos la aplicación lineal $\bar{\tau} : E/\mathbb{R}\alpha \to E/\mathbb{R}\alpha$ tal que $\bar{z} \mapsto \overline{\tau(z)}$ (donde $\bar{z}$ denota la clase de equivalencia de z). Sea $P_\alpha = \alpha^\perp$, como $E = \mathbb{R}\alpha \oplus P_\alpha = \mathbb{R}\alpha \oplus P$, para cualquier $x \in P_\alpha$ se tiene $\tau(x) = \sigma\sigma_\alpha(x) = \sigma(x)$. Teniendo en cuenta la descomposición $E = \mathbb{R}\alpha \oplus P$, sabemos que $x = \lambda\alpha + y$ con $\lambda \in \mathbb{R}$, $y \in P$. Por lo tanto $\tau(x) = \sigma(x) = \lambda\sigma(\alpha) + \sigma(y) = -\lambda\alpha + y$. En consecuencia $\tau(x) - x = -\lambda\alpha + y - \lambda\alpha - y = -2\lambda\alpha \in \mathbb{R}\alpha$. Tenemos entonces $\bar{\tau}(\bar{x}) = \overline{\tau(x)} = \bar{x}$ lo que implica que $\bar{\tau}$ es la identidad. Ahora bien el hecho de que $\bar{\tau}$ sea la identidad junto con la igualdad $\tau(\alpha) = \alpha$ implica que el polinomio minimal de τ es divisor de $(T-1)^l$ donde l es la dimensión de E. Además dada la finitud de Φ, fijado un $\beta \in \Phi$, no todos los elementos del conjunto $\{\beta, \tau(\beta), \ldots, \tau^k(\beta)\}$ (con $k \geq |\Phi|$) pueden ser distintos. Esto implica que alguna potencia de τ fija a β. Podemos entonces considerar una potencia de τ^k suficientemente grande para que fije a todos los elementos de Φ (que es un sistema de generadores de E). Por lo tanto, dicha potencia sería la identidad. Así $\tau^k = 1$. El polinomio minimal de τ divide entonces tanto a $(T-1)^l$ como a $T^k - 1$ y como el máximo común divisor de estos dos polinomios es $T - 1$ resulta que $\tau = 1$ lo que implica $\sigma = \sigma_\alpha$. ■

Definición 19 *Un subconjunto Φ del espacio euclídeo E se dice un* sistema de raíces *si:*

R1 Φ es finito, genera E y $0 \notin \Phi$.

R2 Si $\alpha \in \Phi$ los únicos múltiplos de α en Φ son $\pm\alpha$.

R3 Si $\alpha \in \Phi$, la reflexión σ_α deja Φ invariante.

R4 Si $\alpha, \beta \in \Phi$, entonces $< \alpha, \beta > \in \mathbb{Z}$.

Dado un sistema de raíces Φ denotaremos por $\mathcal{W}$ el subgrupo de $\mathrm{GL}(E)$ generado por las reflexiones σ_α con $\alpha \in \Phi$. Teniendo en cuenta la propiedad R3 de los sistemas de raíces, el grupo $\mathcal{W}$ permuta los elementos de Φ. Esto nos permite identificar el grupo $\mathcal{W}$ con un grupo de permutaciones. En particular el grupo $\mathcal{W}$ es finito y se llama *el grupo de Weyl* de Φ.

Lema 28 *Sea Φ un sistema de raíces en E con grupo de Weyl $\mathcal{W}$. Si $\sigma \in GL(E)$ deja a Φ invariante, entonces $\sigma\sigma_\alpha\sigma^{-1} = \sigma_{\sigma(\alpha)}$ para cada $\alpha \in \Phi$. Además $< \beta, \alpha > = < \sigma(\beta), \sigma(\alpha) >$ para cualesquiera $\alpha, \beta \in \Phi$.*

Dem. Por un lado $\sigma\sigma_\alpha\sigma^{-1}(\sigma(\beta)) = \sigma\sigma_\alpha(\beta) \in \Phi$ ya que $\sigma_\alpha(\beta) \in \Phi$. Por lo tanto $\sigma\sigma_\alpha\sigma^{-1}$ deja a Φ invariante. Además $\sigma_\alpha(\beta) = \beta - < \alpha, \beta > \alpha$, lo que implica $\sigma\sigma_\alpha(\beta) = \sigma(\beta) - < \alpha, \beta > \sigma(\alpha)$. Por otra parte $\sigma\sigma_\alpha\sigma^{-1}$ deja invariante (punto por punto) el hiperplano $\sigma(P_\alpha)$ (donde P_α es el plano invariante punto a punto de σ_α). Aplicando el Lema 27 tenemos $\sigma\sigma_\alpha\sigma^{-1} = \sigma_{\sigma(\alpha)}$. Comparando la expresión para $\sigma\sigma_\alpha\sigma^{-1}(\sigma(\beta))$ encontrada antes con $\sigma_{\sigma(\alpha)}(\sigma(\beta)) = \sigma(\beta) - < \sigma(\alpha), \sigma(\beta) > \sigma(\alpha)$ se tiene la segunda afirmación del Lema. ■

Dados dos sistema de raíces (Φ, E) y (Φ', E') en sus respectivos espacios euclídeos E y E', diremos que una aplicación $\phi : E \to E'$ es un isomorfismo de (Φ, E) a (Φ', E') si:

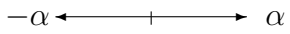


Figura 7.1: Sistema de raíces $A_1 = \{\pm\alpha\}$.

$<\alpha,\beta>$	$<\beta,\alpha>$	θ	$\|\beta\|^2/\|\alpha\|^2$
0	0	$\pi/2$	?
1	1	$\pi/3$	1
-1	-1	$2\pi/3$	1
1	2	$\pi/4$	2
-1	-2	$3\pi/4$	2
1	3	$\pi/6$	3
-1	-3	$5\pi/6$	3

Figura 7.2: Posibilidades para dos raíces independientes.

1. Es un isomorfismo de E a E' que transforma Φ en Φ'.

2. Para cada par de elementos $\alpha, \beta \in \Phi$ se tiene $<\phi(\alpha), \phi(\beta)>=<\alpha, \beta>$.

Se comprueba inmediatamente que $\phi\sigma_\alpha = \sigma_{\phi(\alpha)}\phi$. Por lo tanto el isomorfismo ϕ induce un isomorfismo entre los grupos de Weyl $\mathcal{W}$ y $\mathcal{W}'$ (de Φ y Φ') dado por $\sigma_\alpha \mapsto \sigma_{\phi(\alpha)}$. Como consecuencia del Lema anterior, un automorfismo de Φ no es más que un isomorfismo de E que deja Φ invariante.

Definición 20 *Sea Φ un sistemas de raíces en el espacio euclídeo E. Llamaremos* rango *de Φ al número $l = \dim(E)$.*

Cuando $l \leq 2$ podemos describir Φ mediante un sencillo dibujo. Para $l = 1$, la única posibilidad es la de la figura 7.1,

que es desde luego un sistema de raíces. Este es el sistema de raíces del álgebra de Lie $\mathfrak{sl}(2, F)$. Para $l = 2$ tenemos más posibilidades. La propiedad R4 que deben satisfacer los sistemas de raíces, limitan mucho las posibilidades para el ángulo que pueden formar dos vectores del sistema de raíces. Como $<\beta,\alpha>= 2(\alpha,\beta)/(\alpha,\alpha)$, se tiene de inmediato que $<\alpha,\beta><\beta\alpha>= 4\cos(\theta)$ donde θ es el ángulo que forman α y β. Como $0 \leq \cos\theta \leq 1$, se tiene entonces $0 \leq <\alpha,\beta><\beta\alpha> \leq 4$. Si suponemos que $\beta \neq \pm\alpha$ y $\|\beta\| \geq \|\alpha\|$ entonces queda descartada la posibilidad $\cos\theta = 1$ luego el número $<\alpha,\beta><\beta\alpha>$ solo puede valer 0, 1, 2 o 3. Así los dos números $<\alpha,\beta>$ y $<\beta,\alpha>$ tienen el mismo signo (o son ambos nulos). Las únicas posibilidades son las que quedan reflejadas en la tabla:

Podemos representar gráficamente los únicos sistemas de raíces posibles de rango dos, en las figuras 7.3, 7.4, 7.5, y 7.6.

Como se puede ver, el caso en que $\theta = \pi/3$ es esencialmente el mismo que el caso $\theta = 2\pi/3$, por lo tanto en el conjunto de figuras 7.3,7.4,7.5,7.6 solo hemos representado uno de ellos. Lo mismo se aplica a las parejas de valores $\theta = \pi/4, 3\pi/4$ y $\theta = \pi/6, 5\pi/6$.

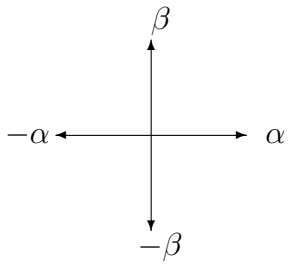


Figura 7.3: Sistema de raíces $A_1 \times A_1 = \{\pm\alpha, \pm\beta\}$.

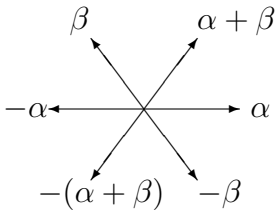


Figura 7.4: Sistema de raíces $A_2 = \{\pm\alpha, \pm\beta \pm (\alpha + \beta)\}$.

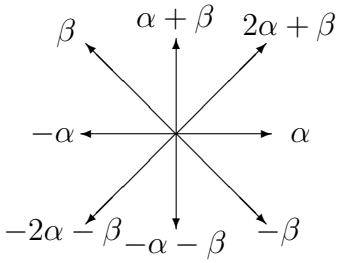


Figura 7.5: Sistema de raíces $B_2 = \{\pm\alpha, \pm\beta \pm (\alpha + \beta), \pm(\alpha - \beta)\}$.

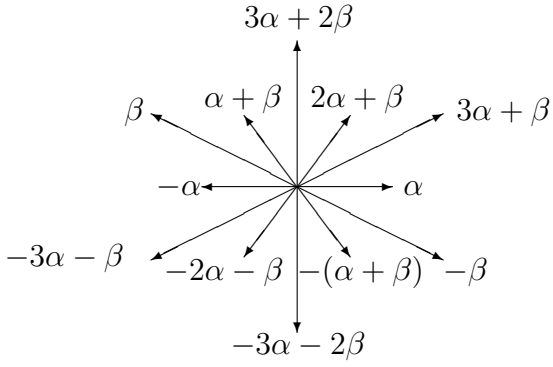


Figura 7.6: $G_2 = \{\pm\alpha, \pm\beta \pm (\alpha + \beta), \pm(2\alpha + \beta), \pm(3\alpha + \beta), \pm(3\alpha + 2\beta)\}$.

Lema 29 *Sean α y β raíces no proporcionales. Si $(\alpha,\beta)>0$, entonces $\alpha-\beta$ es una raíz. Si $(\alpha,\beta)<0$, entonces $\alpha+\beta$ es una raíz.*

Dem. Si $(\alpha,\beta)>0$ entonces $<\alpha,\beta>$ también es positivo luego según la tabla de arriba tenemos que $<\alpha,\beta>=1$ o $<\beta,\alpha>=1$. Si por ejemplo $<\alpha,\beta>=1$ entonces $\sigma_\beta(\alpha)=\alpha-<\alpha,\beta>\beta=\alpha-\beta\in\Phi$. Similarmente si $<\beta,\alpha>=1$. Aplicando lo que acabamos de demostrar a α y $-\beta$ se obtiene la otra afirmación. ■

Veamos una aplicación de esto. Sean $\alpha,\beta\in\Phi$ no proporcionales. Consideremos la α-cadena que contiene a β, es decir el conjunto de raíces de la forma $\beta+i\alpha$ con $i\in\mathbb{Z}$. Sean $r,q\in\mathbb{Z}$ $r,q>0$ los mayores enteros tales que $\beta-r\alpha,\beta+q\alpha\in\Phi$. Veamos que en este caso, para todo $i\in\mathbb{Z}$ tal que $-r\leq i\leq q$, se tiene $\beta+i\alpha\in\Phi$. Para ello supongamos que por el contrario existen enteros i entre r y q, tales que $\beta+i\alpha$ no está en Φ. Entonces existen p,s enteros tales que $-r\leq p,s\leq q$, $p<s$, $\beta+p\alpha\in\Phi$, $\beta+(p+1)\alpha\notin\Phi$, $\beta+s\alpha\in\Phi$, $\beta+(s-1)\alpha\notin\Phi$. Aplicando el Lema anterior se tiene $(\alpha,\beta+p\alpha)\geq 0$ (ya que si dicho producto escalar fuera negativo, entonces se tendría $\beta+(p+1)\alpha\in\Phi$). Del mismo modo se deduce que $(\alpha,\beta+s\alpha)\leq 0$. Pero esto es absurdo pues

$$0\geq(\alpha,\beta+s\alpha)=(\alpha,\beta)+s(\alpha,\alpha)>(\alpha,\beta)+p(\alpha,\alpha)=(\alpha,\beta+p\alpha)\geq 0.$$

Concluimos entonces que la α-cadena que contiene a β no se interrumpe desde $\beta-r\alpha$ hasta $\beta+q\alpha$.

De la propia definición de reflexión, $\sigma_\alpha(\xi)=\xi-<\xi,\alpha>\alpha$ se observa que σ_α suma o resta múltiplos de α a cualquier raíz. Por lo tanto la α-cadena que contiene a una raíz β es invariante por la reflexión σ_α. En el problema 98 se pide demostrar que la reflexión realmente invierte el orden de la cadena. En particular $\sigma_\alpha(\beta+q\alpha)=\beta-r\alpha$ y como

$$\sigma_\alpha(\beta+q\alpha)=\sigma_\alpha(\beta)-q\alpha=\beta-<\beta,\alpha>\alpha-q\alpha=\beta-(<\beta,\alpha>+q)\alpha$$

concluimos que $r-q=<\beta,\alpha>$. Por lo tanto como sabemos que los posibles valores positivos de $<\alpha,\beta>$ son 0, 1, 2 o 3, tenemos que la longitud de la α-cadena que contiene a β es a lo sumo 4.

7.2. Raíces simples

Un subconjunto Δ de un sistema de raíces Φ se dice que es una *base* cuando:

(B1) Δ es una base de E.

(B2) Cada raíz $\beta\in\Phi$ se puede escribir de la forma $\sum_{\alpha\in\Delta}k_\alpha\alpha$ con coeficientes enteros k_α todos ellos mayores o iguales que 0 o todos ellos menores o iguales que ≤ 0.

Las raíces de Δ se llaman *simples*. Como corolario de la definición se tiene $|\Delta|=l$ el rango de Φ. Además la expresión de β dada por B2 es única. Esto nos permite definir la *altura* de

una raíz (con relación a Δ) como el número $\mathrm{ht}(\beta) = \sum_\alpha k_\alpha$. Si $k_\alpha \geq 0$ para todo α diremos que la raíz β es positiva. Si $k_\alpha \leq 0$ entonces diremos que la raíz es negativa. Escribiremos en cada caso $\beta \geq 0$ o $\beta \leq 0$. El conjunto de raíces positivas (con relación a Δ) se denotará por Φ^+, mientras que el conjunto de raíces negativas se denotará por $\Phi^- := -\Phi^+$. La base Δ define un orden parcial en E compatible con el carácter positivo de las raíces: diremos que $\alpha \geq \beta$ si $\beta - \alpha$ es una suma de raíces positivas, o $\alpha = \beta$.

Lema 30 *Si Δ es una base de Φ, entonces:*

1. *$(\alpha, \beta) \leq 0$ para $\alpha \neq \beta$ en Δ.*
2. *$\alpha - \beta$ no es una raíz.*

Dem. Si por ejemplo $(\alpha, \beta) > 0$, como $\alpha \neq \beta$, (y obviamente $\alpha \neq -\beta$), el Lema 29 implica que $\alpha - \beta$ es una raíz. Sin embargo esto contradice la propiedad B2 que debe cumplir una base. ■

Para cada vector $\gamma \in E$, definamos $\Phi^+(\gamma) := \{\alpha \in \Phi : (\alpha, \gamma) > 0\}$, es decir el conjunto de raíces que están en la parte 'positiva' respecto del hiperplano ortogonal a γ. Es un hecho elemental de geometría euclídea, que la unión de una colección finita de hiperplanos no puede ser E. Diremos que un elemento $\gamma \in E$ es *regular* cuando $\gamma \in E - \bigcup_{\alpha \in \Phi} P_\alpha$, donde $P_\alpha = \alpha^\perp$. En caso contrario diremos que el elemento γ es *singular* Cuando γ es regular, está claro que $\Phi = \Phi^+(\gamma) \cup (-\Phi^+(\gamma)$. Diremos que un elemento $\alpha \in \Phi(\gamma)$ es *descomponible* cuando $\alpha = \beta_1 + \beta_2$ donde $\beta_i \in \Phi^+(\gamma)$. En caso contrario diremos que α es *indescomponible*.

Teorema 28 *Sea $\gamma \in E$ un elemento regular. Entonces el conjunto $\Delta(\gamma)$ de todas las raíces indescomponibles de $\Phi^+(\gamma)$ es una base de Φ. Cada base se obtiene de esta forma.*

Dem. La demostración se hará dando una serie de resultados parciales.

(1) *Cada raíz de $\Phi^+(\gamma)$ es una $\mathbb{Z}$-combinación lineal no negativa de elementos en $\Delta(\gamma)$.* Supongamos que cierta $\alpha \in \Phi^+(\gamma)$ desmiente la afirmación anterior. De entre todas estas tomemos una tal que (α, γ) tenga el menor valor posible. Trivialmente $\alpha \notin \Delta(\gamma)$ luego es descomponible y podemos escribir $\alpha = \beta_1 + \beta_2$ con $\beta_i \in \Phi^+(\gamma)$. En consecuencia $(\gamma, \alpha) = (\gamma, \beta_1) + (\gamma, \beta_2)$ y cada uno de los sumandos (γ, β_i) es positivo. Así $(\gamma, \beta_i) < (\gamma, \alpha)$ luego β_i es combinación lineal entera con coeficientes no negativos en $\Delta(\gamma)$ $(i = 1, 2)$. Pero entonces el propio α lo es contradiciendo la suposición inicial.

(2) *Si $\alpha, \beta \in \Delta(\gamma)$, entonces $(\alpha, \beta) \leq 0$ a menos que $\alpha = \beta$.* En caso contrario $(\alpha, \beta) > 0$ implicando que $\alpha - \beta$ es una raíz. Como $\alpha \neq -\beta$, alguna de las raíces $\alpha - \beta$ o $\beta - \alpha$ está en $\Phi^+(\gamma)$. En el primer caso $\alpha = \beta + (\alpha - \beta)$ y por lo tanto α es descomponible en contradicción con que es un elemento de $\Delta(\gamma)$. De forma análoga se procede en el segundo caso.

(3) *$\Delta(\gamma)$ es un conjunto linealmente independiente.* Supongamos por el contrario que $\sum r_\alpha a = 0$ con $\alpha \in \Delta(\gamma)$, $r_\alpha \in \mathbb{R}$. Separando los índices para los que $r_\alpha > 0$ de aquellos para los que $r_\alpha < 0$ tenemos una igualdad del tipo $\sum s_\alpha \alpha = \sum r_\beta \beta$ con $s_\alpha, r_\beta > 0$ y siendo disjuntos los conjuntos de los r_β y los s_α. Si llamamos $e := \sum s_\alpha \alpha$, entonces

$(e,e) = \sum s_\alpha s_\beta(\alpha,\beta) \leq 0$ (por el apartado (2)). Entonces como $(e,e) \geq 0$ sólo queda la posibilidad $(e,e) = 0$ implicando $e = 0$. Aparte, $0 = (\gamma, e) = \sum s_\alpha(\gamma,\alpha) \geq 0$ lo que obliga a que cada s_α es nulo. Análogamente se llega a que cada t_β es nulo (obsérvese que hemos demostrado un resultado algo más general: cada conjunto de vectores que están a un lado de un hiperplano de E y forman dos a dos, ángulos obtusos, es linealmente independiente).

(4) $\Delta(\gamma)$ *es una base de* Φ. Dado que $\Phi = \Phi^+(\gamma) \cup -\Phi^+(\gamma)$, la propiedad B2 se satisface gracias a lo demostrado en el primer paso. Por otra parte, hemos demostrado también en (1) que cada elemento de $\Phi^+(\gamma)$ es combinación lineal de elementos de $\Delta(\gamma)$. Por lo tanto lo mismo se aplica a los elementos de $-\Phi^+(\Delta)$ y así, a todos los de Φ. Como Φ es un sistema de generadores de E, resulta que $\Delta(\gamma)$ lo es. El carácter linealmente independiente de este conjunto demostrado en (3), completa pues la demostración de que $\Delta(\gamma)$ es una base de E.

(5) *Cada base de* Φ *es de la forma* $\Delta(\gamma)$ *para algún elemento regular* γ *de* E. Dada una base Δ, seleccionemos un $\gamma \in E$ tal que $(\gamma,\alpha) > 0$ para todo $\alpha \in \Delta$ (esto es posible gracias al resultado que se pide demostrar en el Problema 99). La propiedad B2 implica entonces que γ es regular. Por otra parte $\Phi^+ \subset \Phi^+(\gamma)$ ya que si $\alpha \in \Phi^+$, se tiene $\alpha = \sum k_i a_i$ con $k_i > 0$, $\alpha_i >= 0$, $\alpha_i \neq 0$. Entonces $(\gamma,\alpha) = \sum k_i(\gamma,\alpha_i) > 0$ al ser algún $k_i \neq 0$. De forma simétrica $\Phi^- \subset -\Phi^+(\Delta)$. Al tratarse de conjuntos finitos, se tiene $\Phi^+ = \Phi^+(\gamma)$, $\Phi^- = -\Phi^+(\gamma)$. Además $\Delta \subset \Phi^+(\gamma)$. Veamos ahora el contenido $\Delta \subset \Delta(\gamma)$. Si $\alpha \in \Delta$ es descomponible, tenemos $\alpha = \beta_1 + \beta_2$ con $\beta_i \in \Phi^+(\gamma) = \Phi^+$. Por otro lado $\beta_i = \sum_{\lambda\in\Delta} h_{i\lambda}\lambda$ con $h_{i\lambda} \geq 0$ para todos i, λ. En definitiva $\alpha = \sum_{i,\lambda} h_{i\lambda}\lambda$ lo que implica $1 = \sum_i h_{i\alpha}$, $0 = \sum_i h_{i\lambda}$ (para $\lambda \neq \alpha$). Como $h_{i\alpha}, h_{i\lambda} \geq 0$, tenemos por ejemplo la solución $h_{1\alpha} = 1$, $h_{2\alpha} = 0$, $h_{i\lambda} = 0$ (para todo i y $\lambda \neq \alpha$). De este modo $\beta_2 = h_{2\alpha}\alpha + \sum_{\lambda\neq\alpha} h_{2\lambda}\lambda = 0$ en contra de que β_2 es una raíz. En consecuencia α es indescomponible y $\Delta \subset \Delta(\gamma)$ Como ambos son bases de E, tienen el mismo cardinal y por lo tanto $\Delta = \Delta(\gamma)$. ■

Los hiperplanos $P_\alpha = \alpha^\perp$ ($\alpha \in \Phi$) descomponen al espacio E en un número finito de regiones. Las componentes conexas de $E - \cup_\alpha P_\alpha$ reciben el nombre de *cámaras de Weyl* (abiertas). Cada elemento regular $\gamma \in E$ pertenece a exactamente una cámara de Weyl que se denotará por $\mathfrak{G}(\gamma)$. Si $\gamma, \gamma' \in E$ y $\mathfrak{G}(\gamma) = \mathfrak{G}(\gamma')$, entonces los vectores γ y γ' están en el mismo semiespacio en que cada hiperplano P_α ($\alpha \in \Phi$) divide a E. Por lo tanto $\Phi^+(\gamma) = \Phi^+(\gamma')$, y también $\Delta(\gamma) = \Delta(\gamma')$. Por lo tanto dada una base Δ de Φ sabemos que existe un elemento regular $\gamma \in E$ tal que $\Delta = \Delta(\gamma)$, entonces llamamos a $\mathfrak{G}(\gamma)$ la *cámara de Weyl fundamental* con relación a Δ. Esta cámara de Weyl vamos a denotarla por $\mathfrak{G}(\Delta)$.

Proposición 18 *La cámara de Weyl fundamental* $\mathfrak{G}(\Delta)$ *coincide con el conjunto de elementos* $\delta \in E$ *tales que* $(\delta,\alpha) > 0$ *para cada* $\alpha \in \Delta$.

Dem. Sea $\delta \in \mathfrak{G}(\Delta) = \mathfrak{G}(\gamma)$ para un adecuado elemento γ tal que $\Delta = \Delta(\gamma)$. Entonces para cada $\alpha \in \Delta \subset \Phi^+(\gamma)$ se tiene $(\gamma,\alpha) > 0$. Como δ y γ están en la misma cámara de Weyl, $(\delta,\alpha) > 0$ para cada $\alpha \in \Delta$. Recíprocamente, supongamos que δ es un elemento del espacio tal que $(\delta,\alpha) > 0$ para cada $\alpha \in \Delta$. Como $(\gamma,\alpha) > 0$ también para cada

$\alpha \in \Delta$ (por ser $\Delta \subset \Phi^+(\gamma)$), entonces para cada raíz $\beta \in \Phi$ se tendrá $(\delta, \beta) = \sum_i k_i(\delta, \alpha_i)$ donde $\beta = \sum_i k_i \alpha_i$ con los k_i enteros todos positivos o todos negativos, y $\alpha_i \in \Delta$. Así $(\delta, \beta) > 0$ si todos los k_i son positivos y $(\delta, \beta) < 0$ en caso de ser todos los k_i negativos. Lo mismo se aplica al producto escalar (γ, β) con lo cual tienen el mismo signo y por lo tanto $\delta \in \mathfrak{G}(\gamma) = \mathfrak{G}(\Delta)$. ■

Como ilustración de estas nociones se recomienda en este punto resolver el Problema 100.

Si $\gamma \in E$ es un elemento regular y $\sigma \in \mathcal{W}$ (el grupo de Weyl), entonces $\sigma(\mathfrak{G}(\gamma)) = \mathfrak{G}(\sigma(\gamma))$. Por lo tanto el grupo de Weyl transforma cámaras de Weyl en cámaras de Weyl. Por otra parte para cada base Δ, y cada elemento $\sigma \in \mathcal{W}$ se tiene que $\sigma(\Delta)$ es una base. Además $\sigma(\Delta(\gamma)) = \Delta(\sigma(\gamma))$.

Lema 31 *Si α es una raíz positiva pero no simple, entonces $\alpha - \beta$ es raíz (necesariamente positiva) para algún $\beta \in \Delta$.*

Dem. Supongamos que $(\alpha, \beta) \leq 0$ para cada $\beta \in \Delta$. Entonces como hicimos constar en el apartado (3) de la demostración del Teorema 28, cada conjunto de vectores que están a un lado de un hiperplano de E y forman dos a dos, ángulos obtusos, es linealmente independiente. Así $\Delta \cup \{\alpha\}$ es linealmente independiente contradiciendo el carácter de base de Δ. Por lo tanto $(\alpha, \beta) > 0$ para algún $\beta \in \Delta$. Aplicando el Lema 29 $\alpha - \beta \in \Phi$ (obsérvese que β no puede ser proporcional a α). Para ver que $\alpha - \beta$ es positiva, escribamos $\alpha = \sum_{\gamma \in \Delta} k_\gamma \gamma$ con todos los $k_\gamma \geq 0$ y necesariamente algún k_γ positivo con $\gamma \neq \beta$. Al restar β obtenemos una combinación lineal entera de raíces simples con al menos un coeficiente positivo. Esto obliga a que todos sean positivos gracias a B2. ■

Corolario 17 *Cada $\beta \in \Phi^+$ se puede escribir de la forma $\alpha_1 + \ldots + \alpha_k$ con $\alpha_i \in \Delta$ (no necesariamente distintos) de modo que cada suma parcial $\alpha_1 + \ldots + \alpha_i$ es una raíz.*

Dem. Aplíquese inducción sobre la altura $\mathrm{ht}(\beta)$. ■

Lema 32 *Sea α una raíz simple, entonces σ_α permuta las raíces positivas distintas de α.*

Dem. Sea $\beta \in \Phi^+ - \{\alpha\}$, $\beta = \sum_{\gamma \in \Delta} k_\gamma \gamma$, con $k_\gamma \in \mathbb{Z}^+$. Claramente β no puede ser proporcional a α. Por consiguiente hay algún k_γ no nulo con $\gamma \neq \alpha$. Si pensamos en el coeficiente que lleva ese γ en la expresión de $\sigma_\alpha(\beta) = \beta - < \beta, \alpha > \alpha$, resulta que es el mismo k_γ lo que implica que $\sigma_\alpha(\beta)$ tiene algún coeficiente positivo con relación a Δ. Esto fuerza a $\sigma_\alpha(\beta)$ a ser una raíz positiva. Además $\sigma_\alpha(\beta) \neq \alpha$ ya que α es $\sigma_\alpha(-\alpha)$. ■

Corolario 18 *Sea $\delta = \frac{1}{2} \sum_{\beta \geq 0} \beta$ y $\alpha \in \Delta$ cualquiera. Entonces $\sigma_\alpha(\delta) = \delta - \alpha$.*

Por un lado

$$\delta - \alpha = \sum_{\beta \geq 0, \beta \neq \alpha} \beta - \frac{1}{2}\alpha$$

y por el otro la acción de σ_α sobre cada sumando de δ distinto de $\frac{1}{2}\alpha$, consiste en dejarlo invariante, mientras que su acción sobre $\frac{1}{2}\alpha$ es transformarlo en su opuesto. Esto demuestra la igualdad. ■

Lema 33 *Sean $\alpha_1, \ldots, \alpha_t \in \Delta$ no necesariamente distintas. Denotemos $\sigma_i := \sigma_{\alpha_i}$. Si $\sigma_1 \cdots \sigma_{t-1}(\alpha_t)$ es negativa, entonces para algún índice s tal que $1 \leq s < t$ se tiene $\sigma_1 \cdots \sigma_t = \sigma_1 \cdots \sigma_{s-1}\sigma_{s+1} \cdots \sigma_{t-1}$.*

Dem. Sea $\beta_i = \sigma_{i+1} \cdots \sigma_{t-1}(\alpha_t)$ para $0 \leq i \leq t-2$, y hagamos $\beta_{t-1} := \alpha_t$. Como $\beta_0 \leq 0$ y $\beta_{t-1} \geq 0$, existe el menor s para el cual $\beta_s \geq 0$. Entonces $\sigma_s(\beta_s) = \beta_{s-1} \leq 0$ lo que en virtud del Lema 32 nos lleva a la igualdad $\beta_s = \alpha_s$. El Lema 28 nos dice que si $\sigma \in \mathcal{W}$, entonces $\sigma_{\sigma(\alpha)} = \sigma\sigma_\alpha\sigma^{-1}$, así es que en nuestro caso $\sigma_s = (\sigma_{s+1} \cdots \sigma_{t-1})\sigma_t(\sigma_{t-1} \cdots \sigma_{s+1})$ lo que convenientemente trastocado nos da la igualdad que proclama el Lema. ■

Corolario 19 *Si $\sigma = \sigma_1 \cdots \sigma_t$ es una expresión de $\sigma \in \mathcal{W}$ en términos de reflexiones correspondientes a raíces simples, con t tan pequeño como sea posible, entonces $\sigma(\alpha_t) \leq 0$.*

Dem. Si $\sigma_1 \cdots \sigma_{t-1}(\alpha_t) \leq 0$ se podría expresar σ como composición de menos de t reflexiones correspondientes a a raíces simples (aplicando el Lema precedente). Por lo tanto $\sigma_1 \cdots \sigma_{t-1}(\alpha_t) \geq 0$ y entonces $\sigma(\alpha_t) = -\sigma_1 \cdots \sigma_{t-1}(\alpha_t) \leq 0$. ■

Vamos a demostrar ahora que el grupo de Weyl $\mathcal{W}$ permuta las bases de Φ de forma transitiva y que $\mathcal{W}$ está generado por las reflexiones σ_α con $\alpha \in \Delta$.

Teorema 29 *Sea Δ una base de Φ. Entonces:*

(a) Si $\gamma \in E$ es regular, existe $\sigma \in \mathcal{W}$ tal que $(\sigma(\gamma), \alpha) > 0$ para cada $\alpha \in \Delta$, dicho de otro modo $\mathcal{W}$ actúa transitivamente sobre las cámaras de Weyl.

(b) Si Δ' es otra base de Φ entonces $\sigma(\Delta') = \Delta$ para algún $\sigma \in \mathcal{W}$, es decir, $\mathcal{W}$ actúa transitivamente sobre las bases.

(c) Si $\alpha \in \Phi$, existe $\sigma \in \mathcal{W}$ tal que $\sigma(\alpha) \in \Delta$.

(d) $\mathcal{W}$ está generado por las reflexiones σ_α con $\alpha \in \Delta$.

(e) Si $\sigma(\Delta) = \Delta$ con $\sigma \in \mathcal{W}$, entonces $\sigma = 1$.

Dem. Sea $\mathcal{W}'$ el subgrupo de $\mathcal{W}$ generado por las reflexiones σ_α con $\alpha \in \Delta$. Vamos a demostrar las propiedades (a)-(c) para $\mathcal{W}'$ en vez de para $\mathcal{W}$. Después veremos que se tiene la coincidencia $\mathcal{W}' = \mathcal{W}$.

(a) Sea $\delta = \frac{1}{2}\sum_{\alpha\geq 0}\alpha$ y tomemos $\sigma \in \mathcal{W}$ de modo que el producto escalar $(\sigma(\gamma), \delta)$ sea máximo. Si la raíz α es simple, entonces $\sigma_\alpha\sigma \in \mathcal{W}'$ y tenemos

$$(\sigma(\gamma), \delta) \geq (\sigma_\alpha\sigma(\gamma), \delta) = (\sigma(\gamma), \sigma_\alpha(\delta)) = (\sigma(\gamma), \delta - \alpha)$$

(en virtud del Corolario 18). Pero entonces concluimos que $(\sigma(\gamma), \delta) \geq (\sigma(\gamma), \delta) - (\sigma(\gamma), \alpha)$. Esto implica $(\sigma(\gamma), \alpha) \geq 0$ para cada $\alpha \in \Delta$. Como γ es regular no puede ocurrir $(\sigma(\gamma), \alpha) = 0$ para ninguna raíz simple α (de tenerse la nulidad de dicho producto escalar, se tendría $\sigma(\gamma) \in P_\alpha$ o equivalentemente γ sería ortogonal a $\sigma^{-1}(\alpha) \in \Phi$). Por lo tanto $(\sigma(\gamma), \alpha) > 0$ para cada raíz de Φ y $\sigma(\gamma)$ pertenece a la cámara de Weyl fundamental $\mathfrak{G}(\Delta)$. Así, σ transforma $\mathfrak{G}(\gamma)$ en $\mathfrak{G}(\Delta)$.

(b) Como $\mathcal{W}'$ permuta las cámaras de Weyl, por el apartado anterior, también permuta las bases de Φ transitivamente, pues cada base es el conjunto de elementos indescomponibles de una cierta cámara $\mathfrak{G}(\gamma)$ para un elemento regular γ.

(c) Demostremos primero que cada raíz pertenece a al menos una base de Φ. Como las únicas raíces proporcionales a α son $\pm\alpha$, los hiperplanos P_β con $\beta \neq \pm\alpha$ son distintos de P_α. Por lo tanto podemos afirmar la no vacuidad del conjunto

$$P_\alpha - \bigcup_{\beta\neq\pm\alpha} P_\beta.$$

Tomemos por lo tanto algún elemento γ en dicho conjunto. Sea ahora γ' suficientemente cercano a γ como para que $(\gamma', \alpha) = \epsilon > 0$ y $|(\gamma', \beta)| > \epsilon$ para cada $\beta \neq \pm\alpha$. Entonces $\alpha \in \mathfrak{G}(\gamma')$ pero α es indescomponible pues si $\alpha = \alpha_1 + \alpha_2$ con $\alpha_i \in \mathfrak{G}(\gamma')$, se tendría $(\gamma', \alpha_i) \geq 0$, $|(\gamma', \alpha_i)| > \epsilon > 0$ luego $(\gamma', \alpha_i) > \epsilon$ y entonces $\epsilon = (\gamma', \alpha) = (\gamma', \alpha_1) + (\gamma', \alpha_2) > 2\epsilon$. Por lo tanto α es un elemento indescomponible de $\mathfrak{G}(\gamma 0')$, es decir, un elemento de la base $\Delta(\gamma')$. Por el apartado anterior sabemos la existencia de un elemento $\sigma \in \mathcal{W}'$ que transforma $\Delta(\gamma')$ en Δ. En particular $\sigma(\alpha) \in \Delta$.

(d) Basta demostrar que cada reflexión σ_α con $\alpha \in \Phi$ pertenece a $\mathcal{W}'$. Usando el apartado (c) sabemos que existe $\sigma \in \mathcal{W}'$ tal que $\beta := \sigma(\alpha) \in \Delta$. Entonces $\sigma_\beta = \sigma_{\sigma(\alpha)} = \sigma\sigma_\alpha\sigma^{-1}$ de forma que $\sigma_\alpha = \sigma^{-1}\sigma_\beta\sigma \in \mathcal{W}'$.

(e) Supongamos que $\sigma(\Delta) = \Delta$ pero $\sigma \neq 1$. Podemos expresar σ como un producto de una o varias reflexiones asociadas a raíces de Δ. Elijamos una tal expresión mínima y apliquemos el Corolario 19. Se tiene entonces $\sigma(\alpha_t) < 0$ pero $\sigma(\alpha_t) \in \Delta$ es una raíz simple y por lo tanto positiva. Esta contradicción demuestra el apartado (e). ■

Llamaremos *reflexión simple* (relativa a Δ), a una reflexión σ_α para $\alpha \in \Delta$. Cuando un elemento σ del grupo de Weyl $\mathcal{W}$ se expresa como una composición de reflexiones $\sigma = \sigma_{\alpha_1} \cdots \sigma_{\alpha_t}$ con $\alpha_i \in \Delta$ y t mínimo, diremos que hemos escrito una *expresión reducida* del elemento en cuestión (relativa a Δ). Diremos también que la *longitud* de σ relativa a Δ es t (denotado $l(\sigma) = t$). Completaremos la definición de longitud poniendo $l(1) = 0$.

Lema 34 *Sea $n(\sigma)$ el número de raíces positivas α tales que $\sigma(\alpha) < 0$. Entonces para cada $\sigma \in \mathcal{W}$ se tiene $l(\sigma) = n(\sigma)$.*

Dem. Hagamos inducción sobre $l(\sigma)$. Para $l(\sigma) = 0$, se tiene $\sigma = 1$ y por lo tanto $n(\sigma) = 0$. Supongamos ahora un elemento $\sigma \in \mathcal{W}$ escrito en forma reducida $\sigma = \sigma_{\alpha_1} \cdots \sigma_{\alpha_t}$. Aplicando el Corolario 19 sabemos que $\sigma(\alpha_t) < 0$. Pero entonces el Lema 32 implica que $n(\sigma\sigma_{\alpha_t}) = n(\sigma) - 1$. Por otra parte $l(\sigma\sigma_{\alpha_t}) = l(\sigma) - 1 < l(\sigma)$ luego aplicando la hipótesis de inducción $n(\sigma\sigma_{\alpha_t}) = l(\sigma\sigma_{\alpha_t})$ y en consecuencia $n(\sigma) = (\sigma)$. ■

Lema 35 *Sea $\lambda, \mu \in \overline{\mathfrak{G}(\Delta)}$. Supongamos que $\sigma(\lambda) = \mu$ para algún $\sigma \in \mathcal{W}$, entonces σ es un producto de reflexiones simples que fijan λ. En particular $\lambda = \mu$.*

Dem. Nuevamente procederemos por inducción sobre el número $l(\sigma)$. El caso $l(\sigma) = 0$ está claro. Supongamos pues $l(\sigma) > 0$ lo que implica la existencia de una raíz positiva que se transforma por σ es una raíz negativa. No puede ocurrir entonces que σ transforme todas las raíces simples en positivas luego $\exists \alpha \in \Delta : \sigma(\alpha) < 0$. Como $\lambda, \mu \in \overline{\mathfrak{G}(\Delta)}$ se tiene $(\lambda, \Delta), (\mu, \Delta) \geq 0$. Entonces

$$0 \geq (\mu, \sigma(\alpha)) = (\sigma(\mu), \alpha) = (\lambda, \alpha) \geq 0$$

y esto nos lleva a que $(\lambda, \alpha) = 0$ implicando $\sigma_\alpha(\lambda) = \lambda$ y $\sigma\sigma_\alpha(\lambda) = \mu$. Gracias al Lema 32 y al Lema 34, podemos asegurar que $l(\sigma\sigma_\alpha) = l(\sigma) - 1$ y podemos aplicar la hipótesis de inducción para obtener que $\sigma\sigma_\alpha$ es un producto de reflexiones simples que fijan λ (luego lo mismo puede decirse de σ). ■

Definición 21 *Diremos que un sistema de raíces Φ es* irreducible *si no puede partir en la unión de dos subconjuntos propios tales que cada raíz de uno de los subconjuntos es ortogonal a todas las del otro.*

Los sistemas de raíces A_1, A_2, B_2 y G_2 son irreducibles mientras que $A_1 \times A_1$ no lo es.

Lema 36 *Sea Φ un sistema de raíces y Δ una base suya. Entonces Φ es irreducible si y sólo si su base Δ no se puede partir en subconjuntos propios ortogonales.*

Dem. Supongamos que $\Phi = \Phi_1 \cup \Phi_2$ siendo estos conjuntos disjuntos y ortogonales. Si $\Delta \subset \Phi_1$ entonces $(\Delta, \Phi_2) = 0$ y por lo tanto $(E, \Phi_2) = 0$ lo que es absurdo. Así $\Delta \not\subset \Phi_i$, $i = 1, 2$ y tenemos una partición $\Delta = \Delta_1 \cup \Delta_2$ en dos subconjuntos propios ortogonales. Recíprocamente, supongamos ahora que Φ es irreducible siendo $\Delta = \Delta_1 \cup \Delta_2$ una partición de Δ es subconjuntos propios ortogonales. Cada raíz es conjugada a una raíz de Δ (Teorema 29 (c)). De este modo podemos partir Φ de la formas $\Phi = \Phi_1 \cup \Phi_2$ siendo Φ_i el conjunto de raíces que tienen un conjugado en Δ_i $(i = 1, 2)$. Recordemos que $(\alpha, \beta) = 0$ implica $\sigma_\alpha\sigma_\beta = \sigma_\beta\sigma_\alpha$, y que $\mathcal{W}$ está generado por reflexiones simples. Si tomamos una raíz ρ cualquiera en un Φ_i, entonces $\rho = \sigma(\delta_i)$ para algún $\delta_i \in \Delta_i$, y $\sigma \in \mathcal{W}$. Ahora bien, σ es

una composición de reflexiones simples cada una de las cuales suma a δ_i un múltiplo de una raíz de Δ_i. Así, ρ está en el subespacio E_i de E generado por Δ_i. Por lo tanto $\Phi_i \subset E_i$ y vemos que $(\Phi_1, \Phi_2) = 0$. Esto obliga a $\Phi_1 = \emptyset$ o $\Phi_2 = \emptyset$ de donde $\Delta_1 = \emptyset$ o $\Delta_2 = \emptyset$. ■

Recordemos que habíamos ordenado las raíces mediante un orden parcial (relativo a Δ) tal que $\alpha \geq \beta$ si $\beta - \alpha$ es una suma de raíces positivas, o $\alpha = \beta$.

Lema 37 *Sea Φ irreducible. Con relación al orden parcial $\geq$ hay una única raíz maximal β. En particular para $\alpha \neq \beta$ se tiene $ht(\alpha) < ht(\beta)$, y $(\alpha, \beta) \geq 0$ para cada $\alpha \in \Delta$. Si $\beta = \sum k_\alpha \alpha$, entonces $k_\alpha > 0$ para toda α.*

Dem. Sea $\beta = \sum_{\alpha \in \Delta} k_\alpha \alpha$ maximal y por lo tanto $\beta \geq 0$. Si $\Delta_1 := \{\alpha \in \Delta : k_\alpha > 0\}$ y $\Delta_2 := \{\alpha \in \Delta : k_\alpha = 0\}$, entonces $\Delta = \Delta_1 \cup \Delta_2$ es una partición. Supongamos que Δ_2 no es vacío. Para cada $\alpha \in \Delta_2$ se tiene $(\beta, \alpha) \leq 0$ (véase el Lema 30). Siendo Φ irreducible, al menos un elemento $\alpha \in \Delta_2$ no es ortogonal a Δ_1. Por lo tanto $(\alpha, \alpha') < 0$ para cierto $\alpha' \in \Delta_1$. Entonces obligatoriamente $(\alpha, \beta) < 0$ (el coeficiente $k_{\alpha'}$ es no nulo y $(\alpha, \alpha') < 0$). El Lema 29 implica que entonces $\alpha + \beta$ es una raíz, pero esto contradice la maximalidad de β. Por consiguiente $\Delta_2 = \emptyset$ y $k_\alpha > 0$ para todo $\alpha \in \Delta$. Además $(\alpha, \beta) \geq 0$ para cada $\alpha \in \Delta$ (ya que si para algún producto escalar $(\alpha, \beta) < 0$, entonces $a + b$ es raíz contradiciendo de nuevo el carácter maximal de β). Más aún, se debe tener $(\alpha, \beta) > 0$ para al menos un $\alpha \in \Delta$ (pues Δ genera E). Sea ahora β' otra raíz maximal. Aplicando a β' lo recién demostrado se tiene $(\alpha, \beta') \geq 0$, $\forall \alpha \in \Delta$, y además $(\alpha, \beta') > 0$ para alguna $\alpha \in \Delta$. Pero entonces $(\beta, \beta') = \sum_\alpha k_\alpha (\alpha, \beta') > 0$ lo que nos obliga a afirmar que $\beta - \beta'$ es una raíz o bien $\beta = \beta'$. Si $\beta - \beta'$ es raíz, se tiene que $\beta \leq \beta'$, o bien $\beta' \leq \beta$ lo que sólo se puede conciliar dado las maximalidades de β y β' escribiendo $\beta = \beta'$. ■

Lema 38 *Sea Φ un sistema de raíces irreducibles. Entonces el grupo de Weyl $\mathcal{W}$ actúa de forma irreducible sobre E. En particular la órbita de cada raíz α genera E.*

Dem. El subespacio generado por la órbita de cada raíz es no nulo y $\mathcal{W}'$-invariante. Por lo tanto la segunda afirmación del Lema se sigue de la primera. Sea E' un subespacio no nulo de E invariante bajo $\mathcal{W}'$. El ortogonal $E'' := E'^{\perp}$ de E' es también W-invariante y $E = E' \oplus E''$. Aplicando el Problema 97 se tiene $\alpha \in E'$ o $E' \subset P_\alpha$. Por lo tanto en caso de que $\alpha \notin E'$ se tendría $\alpha \in P_\alpha^{\perp} \subset E'^{\perp} = E''$. De este modo cada raíz estaría en E' o en E''. Esto partiría Φ en dos subconjuntos ortogonales, luego no pueden ser ambos propios. Uno de los dos es vacío pero si se tuviera $\Phi \subset E''$, entonces $E = E''$ entonces $E' = 0$ en contra de que E' es no nulo desde el principio. Por lo tanto $\Phi \subset E'$ y $E = E'$. ■

Lema 39 *Sea Φ irreducible. Entonces el conjunto $\{\|\alpha\| : \alpha \in \Phi\}$ tiene cardinal dos a lo sumo. Todas las raíces de una longitud dada son conjugadas bajo el grupo de Weyl.*

Dem. Dadas dos raíces arbitrarias α, β, no todas la raíces de la órbita de α (el conjunto $\{\sigma(\alpha) : \sigma \in \mathcal{W}\}$) pueden ser ortogonales a β (ya que dicha órbita genera E por el Lema precedente). Existe entonces una raíz $\sigma(\beta)$ tal que α y $\sigma(\beta)$ no son ortogonales. Como $\|\beta\| = \|\sigma(\beta)\|$ podemos suponer de entrada que disponemos de dos raíces no ortogonales α y β. Sabemos que entonces los posibles valores de $\|\beta\|^2/\|\alpha\|^2$ son 1, 1/2, 2, 3, y 1/3. A partir de este hecho se sigue fácilmente que si tomamos ahora otra raíz γ, o bien: (1) Si $\|\alpha\| \neq \|\beta\|$ entonces $\|\gamma\|$ es igual a $\|\alpha\|$ o a $\|\beta\|$, o (2) Si las normas de α y β coinciden, entonces la de γ puede ser distinta. A partir de este hecho se concluye sin dificultad que los elementos del sistema de raíces se clasifican en dos conjuntos disjuntos donde los elementos de cada conjunto tienen la misma norma.

Supongamos ahora que disponemos de dos raíces α y β con la misma norma. Se puede sustituir una de las raíces por otra conjugada suya que no sea ortogonal a la primera (como al principio de la demostración). Supondremos pues que $\alpha, \beta \in \Phi$ con $\|\alpha\| = \|\beta\|$, $(\alpha, \beta) \neq 0$, $\beta \neq \pm\alpha$. Sabemos que en este caso obligatoriamente $< \alpha, \beta >=< \beta, \alpha >= \pm 1$. Si $< \beta, \alpha >= -1$ podemos sustituir β por $-\beta$ de modo que se tenga $< \alpha, \beta >=< \beta, \alpha >= 1$. Entonces

$$(\sigma_\alpha\sigma_\beta\sigma_\alpha)(\beta) = \sigma_\alpha\sigma_\beta(\beta - \alpha) = \sigma\alpha(-b - (\alpha - \beta)) = \sigma_\alpha(-\alpha) = \alpha.$$

Así, α es conjugada de β.■

Si Φ es irreducible con raíces de dos longitudes, hablaremos de *raíces largas* y *raíces cortas* para referirnos a ellas. En caso de ser todas las longitudes iguales, convendremos en llamar largas a todas las raíces.

Lema 40 *Sea Φ irreducible con raíces de dos longitudes. Entonces la raíz maximal de Φ es larga.*

Dem. Sea β la raíz maximal y α cualquier otra raíz. Vamos a demostrar que entonces $\|\beta\| \geq \|\alpha\|$. Para estudiar esta acotación sustituiremos α por un conjugado suyo que este en el cierre de la cámara de Weyl fundamental relativa a Δ (esto es posible pues el grupo de Weyl $\mathcal{W}$ actúa transitivamente sobre las cámaras de Weyl, por otra parte si un elemento no es regular pertenecerá al cierre de alguna cámara de Weyl). Por ser β maximal se tiene $\beta - \alpha \geq 0$, esto implica que para todo $\gamma \in \overline{\mathfrak{G}(\Delta)}$, se tiene $(\gamma, \beta - \alpha) \geq 0$. Ahora podemos sustituir γ por β y por α ya que β es raíz positiva y α está en el cierre de la cámara de Weyl fundamental. Haciendo $\gamma = \beta$ se tiene $(\beta, \beta) \geq (\beta, \alpha)$ y haciendo $\gamma = \alpha$ se tiene $(\beta, \alpha) \geq (\alpha, \alpha)$ de donde $\|\beta\| \geq \|\alpha\|$. ■

7.3. Matrices de Cartan, grafos de Coxeter y Diagramas de Dynkin.

Fijemos una ordenación $\Delta = \{\alpha_1, \ldots, \alpha_l\}$ de las raíces simples, es decir, consideremos una base ordenada Δ del sistema de raíces Φ. Consideremos entonces la matriz $(< \alpha_i, \alpha_j >)$

cuyos coeficientes son los enteros de Cartan. Esta se llamará la *matriz de Cartan* de Φ relativa a Δ. La matriz de Cartan depende de la ordenación elegida en la base pero esto no es un gran inconveniente. Por otra parte la matriz no depende de la base elegida ya que el grupo de Weyl $\mathcal{W}$ actúa transitivamente sobre el conjunto de las bases (Teorema 29). La matriz de Cartan es inversible pues la base Δ genera a Φ (luego a E) y la matriz de productos escalares $((\alpha_i, \alpha_j))$ es inversible (es la matriz del producto escalar que dota a E de estructura de espacio euclídeo, respecto a la base Δ). Demostremos a continuación que la matriz de Cartan determina a Φ completamente:

Proposición 19 *Sean $\Phi \subset E$ y $\Phi' \subset E'$ sistemas de raíces con bases $\Delta = \{\alpha_1, \ldots, \alpha_l\}$, y $\Delta' = \{\alpha'_1, \ldots, \alpha'_l\}$ respectivamente. Supongamos que las matrices de Cartan de ambos sistemas coinciden: $< \alpha_i, \alpha_j > = < \alpha'_i, \alpha'_j >$ para cualesquiera i, j. Entonces la biyección $\alpha_i \mapsto \alpha'_i$ se extiende de forma única a un isomorfismo $\varphi : E \to E'$ que transforma Φ en Φ' y que satisface $< \varphi(\alpha), \varphi(\beta) > = < \alpha, \beta >$ para todos $\alpha, \beta \in \Phi$. En consecuencia la matriz de Cartan determina a Φ salvo isomorfismo.*

Dem. Existe un único isomorfismo de espacios vectoriales $\varphi : E \to E'$ tal que $\varphi(\alpha_i) = \alpha'_i$, $i = 1, \ldots, l$. Por otro lado, para cualesquiera $\alpha, \beta \in \Delta$ podemos escribir:

$$\sigma_{\varphi(\alpha)}(\varphi(\beta)) = \sigma_{\alpha'}(\beta') = \beta' - < \beta', \alpha' > \alpha' = \varphi(\beta) - < \beta, \alpha > \varphi(\alpha) =$$

$$= \varphi(\beta - < \beta, \alpha > \alpha) = \varphi\sigma_\alpha(\beta)$$

lo que demuestra la igualdad $\sigma_{\varphi(\alpha)}\ \varphi = \varphi\ \sigma_\alpha$, para $\alpha \in \Delta$. Recordemos en este punto que los grupos de Weyl respectivos $\mathcal{W}$ y $\mathcal{W}'$ están generados por las reflexiones simples σ_α con $\alpha \in \Delta$ ($\alpha \in \Delta'$ para $\mathcal{W}'$). Por lo tanto la aplicación $\sigma \mapsto \varphi\sigma\varphi^{-1}$ es un isomorfismo de $\mathcal{W}$ a $\mathcal{W}'$ que transforma σ_α en $\sigma_{\varphi(\alpha)}$. Sabemos también que cada $\beta \in \Phi$ es conjugada por el grupo de Weyl de algún elemento de Δ, es decir, $\beta = \sigma(\alpha)$ para algún $\sigma \in \mathcal{W}$, y cierto $\alpha \in \Delta$ (véase el Teorema 29). Entonces $\varphi(\beta) = (\varphi\sigma\varphi^{-1})(\varphi(\alpha)) \in \Phi'$ lo que demuestra que $\varphi(\Phi) = \Phi'$. Finalmente señalemos que φ preserva los enteros de Cartan como consecuencia de la fórmula para las reflexiones. ■

Escribamos las matrices de Cartan de los sistemas de raíces de rango dos que hemos estudiado en secciones anteriores. Estas son:

$$A_1 \times A_1 : \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}; A_2 : \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}; B_2 : \begin{pmatrix} 2 & -2 \\ -1 & 2 \end{pmatrix}; G_2 : \begin{pmatrix} 2 & -1 \\ -3 & 2 \end{pmatrix}.$$

Estudiemos ahora como podemos recuperar el sistema de raíces conociendo su matriz de Cartan. Supongamos por ejemplo la matriz de Cartan $\begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$ que nos dice que el sistema de raíces tiene rango dos con una base $\Delta = \{\alpha_1, \alpha_2\}$ tal que $< \alpha_1, \alpha_2 > = < \alpha_2, \alpha_1 > = -1$. Aparte de las raíces $\pm\alpha_1$ y $\pm a_2$ vamos a localizar el resto de ellas (sólo las positivas pues las negativas son las opuestas de las primeras) . Empecemos por las de altura dos. Para ello consideremos la α_1-cadena que contiene a α_2. Si tal cadena es

$\alpha_2 - r\alpha_1, \ldots, \alpha_2 + q\alpha_1$, sabemos que $r - q =< \alpha_2, \alpha_1 >$. Pero $\alpha_2 - \alpha_1$ no es una raíz (todas las raíces son combinaciones lineales enteras de coeficientes todos positivos o todos negativos). Entonces $r = 0$ y tenemos $q = 1$. Esto quiere decir que la α_1-cadena por α_2 es simplemente $\{\alpha_2, \alpha_2 + \alpha_1\}$. Dada la simetría de la matriz de Cartan, la α_2-cadena por α_1 se reduce a $\{\alpha_1, \alpha_1 + \alpha_2\}$ lo que quiere decir que las únicas raíces de altura dos son $\pm(\alpha_1 + \alpha_2)$. ¿Habrá raíces de altura tres? Obsérvese que las únicas posibles raíces positivas de altura tres serían $\alpha_1 + 2\alpha_2$ o $\alpha_2 + 2\alpha_1$ y que si alguna de ellas fuera de verdad raíz, la α_1-cadena por α_2 (o la α_2-cadena por α_1) sería más larga de lo que en realidad es. Así el sistema de raíces es el conjunto $\{\pm\alpha_1, \pm\alpha_2, \pm(\alpha_1 + \alpha_2)\}$, es decir, se trata del sistema A_2.

Hemos ilustrado el modo de recuperar el sistema de raíces completo, a partir de su matriz de Cartan. El ejemplo que hemos tomado es uno de los más sencillos pero esto se puede hacer para cualquier sistema de raíces. Se podría dar incluso un algoritmo que determinará Φ a partir de la matriz de Cartan. Dar la matriz de Cartan de un sistema de raíces, es una forma de comprimir la información aportada por dicho sistema. Existe otra forma de comprimir aún más esta información. Se trata de los *grafos de Coxeter*. Dado un sistema de raíces Φ con base Δ de cardinal l, definimos el grafo de Coxeter como aquel grafo que tiene l vértices (tantos como raíces simples) y cada dos vértices i, j $(i \neq j)$ se unen con tantas aristas como el número $< \alpha_i, \alpha_j >< \alpha_j, \alpha_i >$. Veamos los grafos de Coxeter de los sistemas de raíces de rango dos:

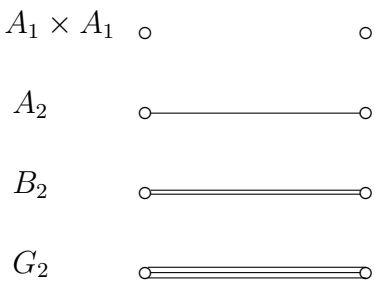
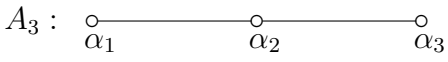


Figura 7.7: Grafos de Coxeter.

Aunque en estos dibujos no lo hemos hecho, normalmente se etiquetan los vértices con los nombres de las raíces. La matriz de Cartan de un sistema de raíces evidentemente determina el grafo de Coxeter. Supongamos dado un grafo de Coxeter, por ejemplo el llamado A_3 que es el siguiente:



entonces $< \alpha_1, \alpha_2 >< \alpha_2, \alpha_1 >= 1$ lo que implica (véase la tabla de la Figura 7.2) que $< \alpha_1, \alpha_2 >=< \alpha_2, \alpha_1 >= -1$. De forma análoga $< \alpha_2, \alpha_3 >=< \alpha_3, \alpha_2 >= -1$ y $<$

$\alpha_1, \alpha_3 >=< \alpha_3, \alpha_1 >= 0$. Por lo tanto la matriz de Cartan del sistema de raíces es

$$\begin{pmatrix} 2 & -1 & 0 \\ -1 & 2 & 1 \\ 0 & -1 & 2 \end{pmatrix}.$$

Sin embargo el grafo de Coxeter no determina del todo la matriz de Cartan cuando hay mas de una arista uniendo dos vértices. Supongamos por ejemplo el grafo

en el que no sabemos cuál es la raíz larga (no pueden tener la misma longitud en virtud de la tabla de la Figura 7.2). Si el lector intentar escribir la matriz de Cartan, verá que hay dos posibilidades

$$\begin{pmatrix} 2 & -1 \\ -2 & 2 \end{pmatrix}, \qquad \text{o} \qquad \begin{pmatrix} 2 & -2 \\ -1 & 2 \end{pmatrix}$$

en función de cuál sea la raíz larga, la de la derecha o la de la izquierda). Para superar este cierto grado de incertidumbre, podemos definir los *diagramas de Dynkin*. Estos se basan en el grafo de Coxeter del sistema de raíces. En el diagrama de Dynkin simplemente se añade un sentido a cada una de las aristas que unen vértices, cuando estos están unidos por más de una arista. Por ejemplos los diagramas de Dynkin de $A_1 \times A_1$ o de A_2 son exactamente iguales a sus grafos de Coxeter. Sin embargo los diagramas de Dynkin de B_2 y de G_2 son los dados en la Figura 7.8

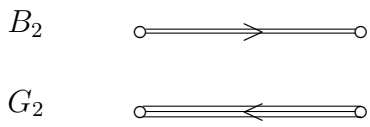


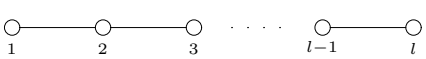
Figura 7.8: Diagramas de Dynkin.

Por lo tanto en el diagrama de Dynkin de B_2 se supone que la raíz larga es la de la derecha mientras que en el de G_2 se supone que es la de la izquierda.

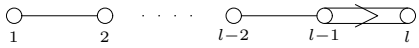
Finalmente, nos gustaría acabar este capítulo clasificando los diagramas de Dynkin de los sistemas de raíces irreducibles.

Teorema 30 *Si ϕ es un sistema de raíces irreducible de rango l, su diagrama de Dynkin es uno de los siguientes (en cada caso hay l vértices):*

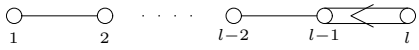
1. *A_l ($l \geq 1$):*



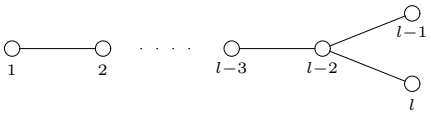
2. *B_l ($l \geq 2$):*



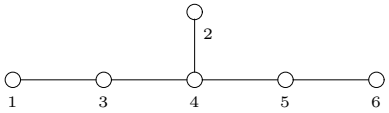
3. C_l $(l \geq 3)$:



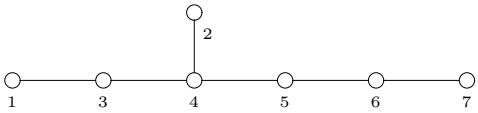
4. D_l $(l \geq 4)$:



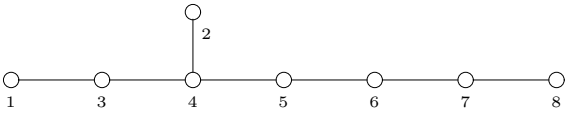
5. E_6:



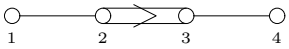
6. E_7:



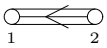
7. E_8:



8. F_4:



9. G_2:



Las restricciones sobre l se imponen para que los nueve casos sean excluyentes.

Dem. La idea de la demostración es clasificar primero los posibles diagramas de Coxeter y luego ver qué diagramas de Dynkin resultan. De hecho se clasifican unas estructuras más generales, que se denotarán en general por el nombre *conjunto admisible* y que no es más que un conjunto $\mathfrak{U} = \{e_1, \ldots, e_n\} \subset E$,donde E es un espacio euclideo, de vectores linealmente independiente de norma uno que satisfacen

$$(e_i, e_j) \leq 0 \quad y \quad 4(e_i, e_j)^2 \in \{0, 1, 2, 3\} \quad (i \neq j)$$

Al igual que se hacía con las raíces simples de un sistema de raíces simples, a cada *conjunto admisible* le asociaremos un grafo, Γ con n vértices donde los vértices i, j están unidos por $4(e_i, e_j)^2$ aristas. Nuestra tarea consiste en encontrar todos los posibles grafos asociados a un *conjunto admisible* dado. Vamos a demostrarlo por etapas:

(1) Si eliminamos algún e_i del conjunto $\mathfrak{U}$ sigue siendo un *conjunto admisible*, cuyo grafo se obtiene del anterior quitando el vértice correspondiente al e_i y las aristas que parten de él.

(2) El número de pares de vértices en Γ unidos por al menos una arista, es estrictamente menor que n. Veamos:
Sea $e = \sum_{i=1}^{n} e_i$, como los e_i son linealmente independientes se tiene que $e \neq 0$. Luego

$$0 < (e, e) = n + 2 \sum_{i<j} (e_i, e_j)$$

Sean $i \neq j$ dos índices tales que $(e_i, e_j) \neq 0$, es decir tales que sus vértices asociados están unidos por alguna arista. Como formaban parte de un *conjunto admisible* sólo nos quedan tres posibilidades para $4(e_i, e_j)^2$, es decir $4(e_i, e_j)^2 = 1, 2, 3$, luego en cualquier caso $|2(e_i, e_j)| \geq 1$ y como por hipótesis los productos son negativos nos queda $2(e_i, e_j) \leq -1$. Si llamamos m al número de pares de vértices conectados por al menos una arista, nos queda que

$$0 < (e, e) = n + 2 \sum_{i<j} (e_i, e_j) = n + \sum_{i<j} 2(e_i, e_j) \leq n + \sum_{i<j} (-1) = n - m$$

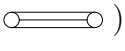
Por tanto $m < n$.

(3) Γ no contiene ciclos. Veamos:
Si tuviera algún ciclo, el subconjunto $\mathfrak{U}'$ de los vectores asociados a los vértices del ciclo sería también un conjunto admisible aplicando (1). Ahora en ese subconjunto el número de pares conectados (por al menos una arista) sería igual al cardinal del conjunto, es decir por cada vector hay un único par conectado (él con el siguiente en el ciclo, por ejemplo). Pero esto contradice lo que dice (2), luego no puede haber ciclos.

(4) No puede haber un vértice en Γ del que partan más de tres aristas. Veamos:
Fijemos un vértice $e \in \mathfrak{U}$ y llamemos $\eta_1, \ldots, \eta_k$ a los vectores de $\mathfrak{U}$ conectados con e, es decir $(e, \eta_i) < 0$ y todos los η_i son distintos y distintos de e. No puede haber dos η_i conectados ya que en ese caso formarían, junto con e, un ciclo, que por (3) es imposible. Tenemos por tanto que $(\eta_i, \eta_j) = 0$ para $i \neq j$. Ahora, como $\mathfrak{U}$ es linealmente independiente debe haber algún vector unitario η_0, en el subespacio generado por $e, \eta_1, \ldots, \eta_k$, ortogonal a todos los η_i. Luego $\eta_0, \eta_1, \ldots, \eta_k$ es un sistema ortonormal que genera el mismo subespacio que los $e, \eta_1, \ldots, \eta_k$ y por tanto, $e = \sum_{i=0}^{k} (e, \eta_i)\eta_i$ si además aplicamos que $e \in \mathfrak{U}$ tenemos

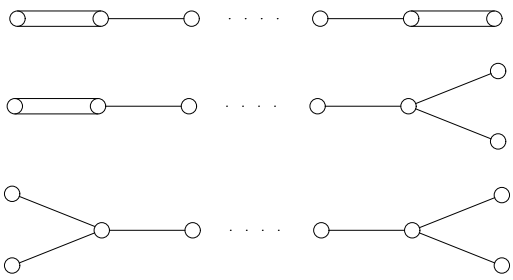
$$1 = (e, e) = \sum_{i=0}^{k} (e, \eta_i)^2$$

claramente $(e, \eta_0) \neq 0$ por lo que la igualdad anterior fuerza que $\sum_{i=1}^{k} (e, \eta_i)^2 < 1$ o equivalentemente $\sum_{i=1}^{k} 4(e, \eta_i)^2 < 4$. Pero $4(e, \eta_i)^2$ es el número de aristas uniendo e con η_i en Γ. Luego, por un cálculo elemental, no puede haber más de tres aristas que partan de e.

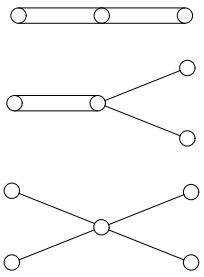
(5) El único grafo conectado Γ posible, para un conjunto admisible $\mathfrak{U}$, que contiene una arista triple (es decir, un par de vértices unidos por tres aristas) es el grafo de Coxeter $\mathbf{G_2}$ (). Esto se deduce trivialmente del apartado anterior.

(6) Sea $\{e_1, \ldots, e_k\} \subset \mathfrak{U}$ tal que el subgrafo asociado sea (una cadena simple en Γ). Si llamamos $\mathfrak{U}' = (\mathfrak{U} - \{e_1, \ldots, e_k\}) \cup \{e\}$, donde $e = \sum_{i=1}^{k} e_i$ entonces $\mathfrak{U}'$ vuelve a ser admisible.
Claramente $\mathfrak{U}'$ es un conjunto independiente por tanto sólo hay que comprobar las condiciones sobre los productos escalares. Veamos:
Por hipótesis $4(e_i, e_{i+1})^2 = 1$ y como además son elementos de un conjunto admisible $2(e_i, e_{i+1}) = -1$, por tanto $(e, e) = k + 2\sum_{i<j} (e_i, e_j) = k - (k-1) = 1$ luego e tiene norma uno. Claramente, si $\eta \in \mathfrak{U} - \{e_1, \ldots, e_k\}$ sólo se puede conectar con un e_i como mucho, ya que en caso de conectarse con dos de ellos, e_i, e_j con $i \neq j$, $\{\eta, e_i, e_j\}$ formaría un ciclo, lo que contradice (3). Tenemos entonces que $(\eta, e) = 0$ si no está conectado con ninguno o $(\eta, e) = (\eta, e_i)$ en el caso de estar conectado sólo con el e_i (por linealidad del producto escalar), en cualquiera de los casos $4(\eta, e)^2 = 0, 1, 2, 3$ y $(\eta, e) \leq 0$. Luego $\mathfrak{U}'$ es también admisible.

(7) Γ no contiene subgrafos de la forma:

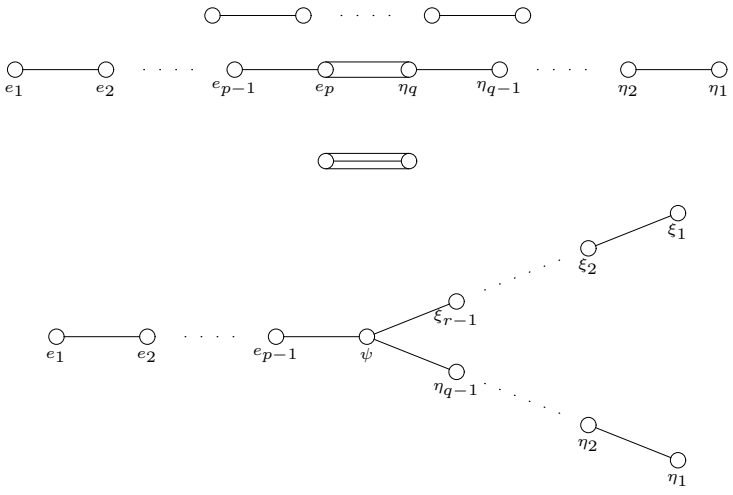


Para ver esto hay que interpretar primero el significado del apartado anterior. Tal y como se ve en la conclusión del apartado el nuevo vértice e está conectado con todos los vértices que estaban conectados con la cadena simple. Lo que hacemos es cambiar la cadena simple por un sólo vértice del que parten todas las aristas que partían de la cadena. En esta caso es fácil ver que de darse alguna de las posibilidades anteriores y aplicando el apartado (6) nos encontraríamos con los siguientes grafos asociados a nuevos conjuntos admisibles:

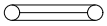


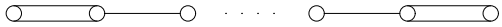
Pero una rápida mirada nos muestra que todos contradicen el apartado (4) ya que tienen vértices con más de tres aristas.

(8) Cualquier grafo conectado Γ de un conjunto admisible tiene una de las siguientes formas.

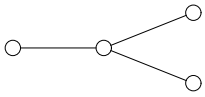


Vamos a ir descartando posibilidades según el tipo de aristas que tenga el grafo.

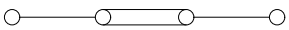
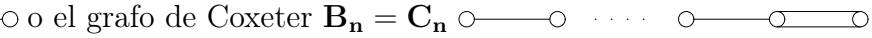
- Si tiene aristas triples, por el apartado (5) sólo puede ser 
- Si tiene aristas dobles por el apartado (7) sólo puede tener una, ya que si tuviera dos contendría un subgrafo de la forma

  lo que contradice (7). Por el mismo motivo tampoco puede contener una bifurcación

  luego sería un grafo del segundo tipo.
- Si tiene alguna bifurcación con el mismo razonamiento que antes deduciríamos que sólo puede tener una y que además no puede tener aristas dobles por lo que tendríamos un grafo del cuarto tipo.
- Por último, si no tiene ni aristas triples, ni dobles, ni bifurcaciones, debe ser una cadena simple, por tanto tendríamos un grafo del primer tipo

(9) Los únicos grafos conectados del segundo tipo en (8) son el grafo de Coxeter $\mathbf{F_4}$  o el grafo de Coxeter $\mathbf{B_n} = \mathbf{C_n}$ 

Sea $e = \sum_{i=1}^{p} ie_i$ y $\eta = \sum_{i=1}^{q} i\eta_i$. Por hipótesis, $2(e_i, e_{i+1}) = -1 = 2(\eta_i, \eta_{i+1})$ y los demás pares son ortogonales (no son adyacentes). Entonces

$$(e,e) = \sum_{i=1}^{p} i^2 - \sum_{i=1}^{p-1} i(i+1) = \frac{p(p+1)}{2} \; y \; (\eta,\eta) = \sum_{i=1}^{q} i^2 - \sum_{i=1}^{q-1} i(i+1) = \frac{q(q+1)}{2}$$

Ahora, como $4(e_p, \eta_q)^2 = 2$ por linealidad $(e,\eta)^2 = p^2q^2(e_p,\eta_q)^2 = p^2q^2/2$. Si escribimos la desigualdad de Schwartz $(e,\eta)^2 < (e,e)(\eta,\eta)$ en términos de p y q nos queda

$$\begin{aligned}
\frac{p^2q^2}{2} &< \frac{p(p+1)q(q+1)}{4} \\
pq &< \frac{(p+1)(q+1)}{2} \\
2pq &< pq+1+q+p \\
pq-p-q &< 1 \\
pq-p-q+1 &< 2 \\
(p-1)(q-1) &< 2
\end{aligned}$$

Las únicas posibilidades son $p = q = 2$ que nos dan $\mathbf{F_4}$ ó $p = 1$ (q arbitrario), $q = 1$ (p arbitrario) que nos da la otra posibilidad.

(10) Los únicos grafos conectados del cuarto tipo en (8) son el grafo de Coxeter $\mathbf{D_n}$ o el grafo de Coxeter $\mathbf{E_n}$ ($n = 6, 7, 8$).
Sea $e = \sum ie_i$, $\eta = \sum i\eta_i$ y $\xi = \sum i\xi_i$. Claramente e, η, ξ son ortogonales dos a dos, linealmente independientes y ψ no es combinación lineal de ellos. Si llamamos e_1, e_2, e_3 a los correspondientes normalizados de e, η, ξ aplicando el mismo razonamiento que en (4) podemos encontrar otro vector, e_0, normal y ortogonal a los demás e_i tal que $\psi = \sum_{i=0}^{3}(e_i, \psi)e_i$ y siguiendo el razonamiento de (4) llegamos a que $\sum_{i=1}^{3}(e_i, \psi)^2 < 1$.
Escribamos ahora cada término de la suma en función de p, q y r.

$$(e_1, \psi)^2 = \left(\frac{e}{\sqrt{(e,e)}}, \psi\right)^2 = \frac{(e,\psi)^2}{(e,e)} = \frac{(p-1)^2(e_{p-1},\psi)^2}{(e,e)} = \frac{(p-1)^2/4}{p(p-1)/2} = \frac{p-1}{2p}$$

análogamente

$$(e_2, \psi)^2 = \frac{q-1}{2q}$$

$$(e_3, \psi)^2 = \frac{r-1}{2r}$$

con lo que la desigualdad nos queda

$$\begin{aligned} \frac{p-1}{2p} + \frac{q-1}{2q} + \frac{r-1}{2r} &< 1 \\ \frac{1}{2}\left(1 - \frac{1}{p} + 1 - \frac{1}{q} + 1 - \frac{1}{r}\right) &< 1 \\ 3 - \left(\frac{1}{p} + \frac{1}{q} + \frac{1}{r}\right) &< 2 \\ \frac{1}{p} + \frac{1}{q} + \frac{1}{r} &> 1 \end{aligned}$$

Vamos a calcular ahora todas las soluciones de esta ecuación. Como el grafo del cuarto tipo es simétrico podemos suponer sin pérdida de generalidad que $p \geq q \geq r$. Además todos son mayores que uno, ya que en ese caso el grafo no tendría sentido. Tenemos entonces

$$\frac{1}{p} \leq \frac{1}{q} \leq \frac{1}{r} \leq \frac{1}{2}$$

en particular

$$\frac{3}{2} \geq \frac{3}{r} > 1$$

por tanto $r = 2$. Veamos qué ocurre con p y q.

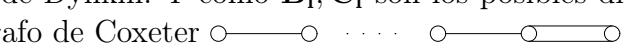
$$\frac{1}{p} + \frac{1}{q} > \frac{1}{2}$$

y por lo mismo que antes

$$1 \geq \frac{2}{q} > \frac{1}{2}$$

luego $2 \leq q < 4$ que nos deja dos posibilidades

- $q = 2$, en este caso $\frac{1}{q} + \frac{1}{r} = 1$ luego el valor de p es superfluo. El grafo correspondería con algún grafo de Coxeter del tipo $\mathbf{D_n}$.
- $q = 3$, entonces $\frac{1}{p} > \frac{1}{6}$ luego $p < 6$. El grafo sería un grafo de Coxeter de tipo $\mathbf{E_{p+3}}$ con $p = 3, 4, 5$ ya que si $p = 2$ estaríamos en el caso anterior, cambiando p por q.

Esto muestra que todos los grafos de conjuntos admisibles de un espacio euclídeo se encuentran entre los grafos de Coxeter de los tipos $\mathbf{A} - \mathbf{G}$. En particular, el grafo de Coxeter de un sistema de raíces debe ser de uno de esos tipos. Además, en todos los casos excepto en los tipos $\mathbf{B_l}, \mathbf{C_l}$ el grafo de Coxeter determina de forma única el diagrama de Dynkin. Y como $\mathbf{B_l}, \mathbf{C_l}$ son los posibles diagramas de Dynkin provenientes del grafo de Coxeter  .■

7.4. Problemas.

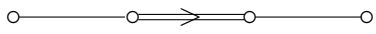
Problema 97 *Sea E' un subespacio del espacio euclídeo E. Demuéstrese que si una reflexión σ_α deja E' invariante, entonces o bien $\alpha \in E'$ o de lo contrario $E' \in P_\alpha$.*

Problema 98 *Demuéstrese que la reflexión σ_α invierte el orden de la α-cadena que contiene a β. Sugerencia: se ha visto antes que la reflexión deja a la tal cadena invariante. Por lo tanto permuta sus elementos. Demuéstrese que esa permutación de elementos invierte el orden,*

Problema 99 *Pruébese que dada una base $\{\gamma_1, \ldots, \gamma_l\}$ de un espacio euclídeo E, la intersección de los semiespacios $S_i := \{x \in E : (x, \gamma_i) > 0\}$ es no vacía. Sugerencia: considérese el elemento $\gamma = \sum r_i \delta_i$ donde los r_i son positivos y cada δ_i es la proyección de γ_i en la recta ortogonal al hiperplano generado por $\{\gamma_1, \ldots, \gamma_{i-1}, \gamma_{i+1}, \ldots, \gamma_l\}$.*

Problema 100 *Determinar en cada uno de los sistemas de raíces de rango dos una base. ¿Cuál es la cámara de Weyl fundamental en cada caso?*

Problema 101 *Dado el diagrama de Dynkin de la figura de abajo, determínese su matriz de Cartan (el correspondiente sistema de raíces se llama F_4).*



Capítulo 8

Álgebras de Lie excepcionales

En este apéndice definiremos las álgebras de Lie de tipo G_2, F_4, y E_i con $i = 6, 7, 8$.

8.1. Resultados preliminares

Recordemos que un álgebra de composición U sobre un cuerpo F es un álgebra no necesariamente asociativa pero con unidad $1 \in U$, provista de una forma cuadrática $n : U \to F$ no degenerada y multiplicativa en el sentido de que $n(xy) = n(x)n(y)$ para cualesquiera $x, y \in U$. En un álgebra de este tipo, podemos definir la aplicación *traza* como aquella aplicación lineal $\tau : U \to F$ dada por $\tau(x) := f(x, 1)$ donde $f : U \times U \to F$ es la forma polar de n, es decir, $f(x, y) := n(x + y) - n(x) - n(y)$, $(x, y \in U)$. En el Capítulo tercero de estos apuntes, se tratan exhaustivamente estas álgebras, obteniéndose una clasificación completa. Si el cuerpo base F es de característica distinta de dos, podemos descomponer el álgebra en una suma directa de subespacios $U = F1 \oplus U_0$, donde $U_0 := \{x \in U : \tau(x) = 0\}$. En efecto para cada $x \in U$, podemos escribir[1] $x = \tau(x) + x - \tau(x)$, siendo $\tau(x) \in F$, y $x - \tau(x) \in U_0$. Por otra parte si $\lambda \in F \cap U_0$, entonces $\lambda = \tau(\lambda) = 0$.

La descomposición anterior $U = F1 \oplus U_0$, garantiza que cada elemento $x \in U$ se descompone de la forma $x = \lambda + x_0$, $\lambda \in F$, $x_0 \in U_0$. Llamaremos *parte escalar de* x a λ (que coincide con $\tau(x)$), y *parte vectorial de* x a x_0. Por otra parte para cada par de elementos $x, y \in U_0$ denotaremos al opuesto de la parte escalar de xy por $-(x, y)$, y a su parte vectorial, por $x * y$. Se tiene entonces que:

$$xy = -(x, y) + x * y, \ \forall x, y \in U_0.$$

Finalmente añadamos que como consecuencia de la clasificación de las álgebras de composición estudiada en el tercer capítulo, podemos afirmar que sobre un cuerpo F algebraicamente cerrado y de característica distinta de dos, las álgebras de composición son (salvo isomorfismos):

$$F, C_s, H_s, O_s,$$

[1] Como es habitual, identificamos $F1$ con F.

donde C_s es isomorfa a $F \times F$ con operaciones por componentes e involución de intercambio, H_s es isomorfa a $\mathcal{M}_2(F)$ con involución

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} d & -b \\ -c & a \end{pmatrix},$$

y O_s es isomorfa al álgebra de matrices de Zorn (véase el Problema 54).

Dada un álgebra de composición[2] U con involución $u \mapsto \overline{u}$. Podemos considerar el álgebra $H_3(U)$ formada por las matrices $(a_{ij}) \in \mathcal{M}_3(U)$, tales que $\overline{a_{ji}} = a_{ij}$. Ésta, es un álgebra de Jordan para la multiplicación $x \circ y = xy + yx$. Recordemos que un álgebra de Jordan sobre un cuerpo de característica distinta de dos, es un álgebra J, cuyo producto (que podemos provisionalmente denotar por $x \circ y$), satisface las identidades:

$$x \circ y = y \circ x, \quad x^2 \circ (y \circ x) = (x^2 \circ y) \circ x, \quad (x^2 := x \circ x).$$

Consideremos entonces un álgebra de Jordan $J = F$, o bien, $J = H_3(U)$ donde U es como en el párrafo anterior. Veníamos denotando al producto de J mediante $\circ$, pero vamos ahora a cambiar de nuevo a la notación habitual en cualquier álgebra: la simple yuxtaposición de elementos de J denotará su producto. En el resto de este apéndice, vamos a exigir al cuerpo base F, el ser algebraicamente cerrado y de característica cero. En cada una de las álgebras J definidas arriba, podemos considerar la aplicación $T : J \to F$ dada por

$$T(x) := \frac{3}{\dim(J)} \text{traza}(R_x).$$

Entonces, se tiene una descomposición en suma directa $J = F1 \oplus J_0$ donde $J_0 = 0$ si $J = F$, y en los otros casos $J_0 = \{x \in J : T(x) = 0\}$. En efecto: si $J \neq F$, la aplicación T aplicada a escalares actúa de la forma $T(\lambda 1) = 3\lambda$, para cada $\lambda \in F$. Entonces, si $\lambda \in F1 \cap J_0$, se tiene $0 = T(\lambda 1) = 3\lambda$ lo que implica $\lambda = 0$. Por otra parte cada elemento $x \in J$ se puede escribir de la forma

$$x = \frac{1}{3}T(x) + (x - \frac{1}{3}T(x)),$$

donde $T(x) \in F$ y $x - \frac{1}{3}T(x) \in J_0$. En forma parecida a como hicimos en U, llamaremos *parte escalar de* x al elemento $T(x) \in F$, y *parte vectorial de* x al sumando $x - \frac{1}{3}T(x)$. Una vez establecido este hecho, para cada pareja de elementos $x, y \in J$, denotaremos por $\langle x, y \rangle$ al triple de la parte escalar de xy; y por $x * y$ a la parte vectorial del producto xy. Por lo tanto podremos escribir

$$xy = \frac{1}{3}\langle x, y \rangle + x * y, \ \forall x, y \in J.$$

Vamos ahora a describir un construcción muy peculiar, que nos proporcionará la definición de todas las álgebras de Lie excepcionales. Si U es cualquiera de las álgebras alternativas F, C_s, H_s, O_s y J cualquiera de las álgebras de Jordan F, $H_3(F)$, $H_3(C_s)$, $H_3(H_s)$, o

[2]Seguimos suponiendo que la característica del cuerpo base es distinta de dos.

$H_3(O_s)$, podemos construir el F-espacio vectorial

$$\mathcal{L} = \mathrm{Der}(U) \oplus U_0 \otimes J_0 \oplus \mathrm{Der}(J).$$

El espacio $\mathcal{L}$ se convierte en un álgebra de Lie con el producto [,] que actúa conforma a las siguientes cláusulas:

$$[\mathrm{Der}(U), \mathrm{Der}(J)] := 0,$$
$$[a \otimes x, D] := D(a) \otimes x,\ a \in U_0,\ x \in J_0,\ D \in \mathrm{Der}(U),$$
$$[a \otimes x, E] := a \otimes E(x),\ a \in U_0,\ x \in J_0,\ E \in \mathrm{Der}(J),$$
$$[a \otimes x, b \otimes y] := \frac{1}{12}\langle x, y\rangle D_{a,b} + (a * b) \otimes (x * y) - (a, b)[R_x, R_y],$$

Donde $D_{x,z} := R_{[x,z]} - L_{[x,z]} - 3[L_x, R_z]$ para cualesquiera $x, z \in U$. El hecho de que $D_{a,b} \in \mathrm{Der}(U)$ se puede ver en [9, p.77], por otra parte $[R_x, R_y] \in \mathrm{Der}(J)$ por [9, p. 92].

Con las definiciones que hemos introducido podemos definir las álgebras de Lie excepcionales. Para ello, tomaremos U como el álgebra O_s de las matrices de Zorn, y dejaremos que J varíe en el conjunto de álgebras de Jordan:

$$\{F, H_3(F), H_3(C_s), H_3(H_s), H_3(O_s)\}.$$

Así, podemos escribir:

$$\begin{array}{llll} g_2 := \mathcal{L}, & \text{para} & U = O_s, & J = F, \\ f_4 := \mathcal{L}, & \text{para} & U = O_s, & J = H_3(F), \\ e_6 := \mathcal{L}, & \text{para} & U = O_s, & J = H_3(C_s), \\ e_7 := \mathcal{L}, & \text{para} & U = O_s, & J = H_3(H_s), \\ e_8 := \mathcal{L}, & \text{para} & U = O_s, & J = H_3(O_s), \end{array} .$$

En consecuencia $g_2 = \mathrm{Der}(O_s)$ pues para $J = F$, se tiene $J_0 = 0$ y $\mathrm{Der}(J) = 0$. Ahora debemos comprobar que los nombres de las álgebras están bien puestos, es decir que cada una de las álgebras g_2, f_4, e_i, con $i = 6, 7, 8$ tiene los correspondientes diagramas de Dynkin.

8.2. g_2

En el álgebra de octoniones split O_s sobre F llamaremos como es habitual e_1 y e_2 a los idempotentes ortogonales

$$e_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad e_2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix},$$

cuya suma es la unidad. Para cualquier vector $a \in F^3$ usaremos las notaciones

$$X_{12}(a) = \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix}, \quad X_{21}(a) = \begin{pmatrix} 0 & 0 \\ a & 0 \end{pmatrix}.$$

Si denotamos por $\{i, j, k\}$ la base canónica de F^3, El conjunto

$$\mathcal{B} := \{e_1, e_2, X_{12}(i), X_{12}(j), X_{12}(k), X_{21}(i), X_{21}(j), X_{21}(k)\}$$

es una base de O_s que nos será de utilidad en el futuro. Es de comprobación inmediata que las reglas de multiplicación de estos elementos viene dadas por las relaciones

$$e_i e_j = \delta_{ij} e_i, \quad e_1 X_{12}(a) = X_{12}(a) = X_{12}(a) e_2,$$

$$e_1 X_{21}(a) = X_{21}(a) e_2 = 0, \quad e_1 X_{21}(a) = 0 = X_{21}(a) e_2,$$

$$e_2 X_{21}(a) = X_{21}(a) = X_{21}(a) e_1, \quad X_{12}(a) X_{12}(b) = X_{21}(a \wedge b)$$

$$X_{21}(a) X_{21}(b) = -X_{12}(a \wedge b), \quad X_{12}(a) X_{21}(b) = (a, b) e_1$$

$$X_{21}(a) X_{12}(b) = (a, b) e_2,$$

donde (a, b) denota el producto escalar de F^3 dado por $(a, b) = ab^t$ para todos $a, b \in F^3$.

El álgebra de octoniones split es $\mathbb{Z}_3$-graduada de modo que $O_s = (O_s)_0 \oplus (O_s)_1 \oplus (O_s)_2$ siendo $(O_s)_0 := Fe_1 \oplus F_2$, $(O_s)_1 := X_{12}(F^3)$ y $(O_s)_2 := X_{21}(F^3)$. El problema 102 implica entonces que $L = \mathrm{Der}(O_s)$ es también $\mathbb{Z}_3$-graduada de modo que $L = L_0 \oplus L_1 \oplus L_2$ y para cada $i = 0, 1, 2$ se tiene:

$$L_i = \{D \in \mathrm{Der}(O_s) : D((O_s)_j) \subset (O_s)_{i+j}), \forall j = 0, 1, 2\}.$$

Por lo tanto $D \in L_0$ si y sólo si $D(e_i) \in Fe_1 + Fe_2$, $D(X_{ij}(F^3)) \subset X_{ij}(F^3)$ para $i, j \in \{1, 2\}$, $i \neq j$. Para cada elemento x de un álgebra $\mathbb{Z}_n$-graduada $A = \oplus_i A_i$, vamos a escribir $x = x_0 + \cdots + x_{n-1}$ con $x_i \in A_i$ para indicar la descomposición de x conforme a la descomposición $A = \oplus_i A_i$. Los sumandos x_i reciben el nombre de *componentes homogéneas*.

Proposición 20 *Para toda derivación $D \in L = Der(O_s)$ y cada $i = 1, 2$, se tiene $D(e_i) \in X_{12}(F^3) + X_{21}(F^3)$*

Dem. Supongamos $D(e_1) = \lambda_1 e_1 + \lambda_2 e_2 + X_{12}(a) + X_{21}(b)$. Al ser $e_1^2 = e_1$ se tiene $D(e_1)e_1 + e_1 D(e_1) = D(e_1)$ lo que implica $e_1 D(e_1) e_1 + e_1 D(e_1) = e_1 D(e_1)$ o bien $e_1 D(e_1) e_1 = 0$. Pero $e_1 D(e_1) = \lambda_1 e_1 + X_{12}(a)$ y $0 = e_1 D(e_1) e_1 = \lambda_1 e_1$ implicando $\lambda_1 = 0$. Por otra parte como $e_1 e_2 = 0$ tenemos $D(e_1)e_2 + e_1 D(e_2) = 0$. Además $0 = D(1) = D(e_1) + D(e_2)$ luego $D(e_2) = -D(e_1)$ lo que unido a lo anterior nos dice que

$$D(e_1)e_2 - e_1 D(e_1) = 0. \tag{8.1}$$

Como $D(e_1)e_2 = \lambda_2 e_2 + X_{12}(a)$ y $e_1 D(e_1) = X_{12}(a)$, concluimos de la ecuación (8.1) que $\lambda_2 e_2 = 0$, es decir, $\lambda_2 = 0$. ■

Corolario 20 *Para cada $D \in L_0$ se tiene $D(e_1) = D(e_2) = 0$.*

Tratemos de describir las derivaciones de L_0. Sabemos que tales derivaciones $D \in L_0$ satisfacen $D(e_1) = D(e_2) = 0$. Además $D(X_{12}(a)) = X_{12}(f(a))$ y $D(X_{21}(a)) = X_{21}(g(a))$ para todo $a \in F^3$, siendo $f, g : F^3 \to F^3$ aplicaciones lineales. Vamos a determinar las propiedades de f y g. Al tenerse que $X_{12}(x)X_{12}(y) = X_{21}(x \wedge y)$, si aplicamos D obtenemos $X_{12}(f(x))X_{12}(y) + X_{12}(x)X_{12}(f(y)) = X_{21}(g(x \wedge y))$ o equivalentemente $X_{21}(f(x) \wedge y + x \wedge f(y)) = X_{21}(g(x \wedge y))$ lo que nos lleva a $f(x) \wedge y + x \wedge f(y) = g(x \wedge y)$, para cualesquiera $x, y \in F^3$. Por otra parte sabemos que $X_{12}(x)X_{21}(y) = (x, y)e_1$ para todos $x, y \in F^3$. Si aplicamos D obtenemos: $X_{12}(f(x)X_{21}(y) + X_{12}(x)X_{21}(g(y)) = 0$ o bien $(f(x), y) + (x, g(y)) = 0$, lo que implica que $g = -f^\sharp$ (el exponente 'sostenido' de f indica adjunción de operadores). Si suponemos que la matriz de f en la base canónica $\{i, j, k\}$ de F^3 es (a_{ij}), entonces la de g es $-(a_{ji})$. Por otra parte como caso particular de lo que hemos demostrado antes se tiene $f(i) \wedge j + i \wedge f(j) = g(k)$ o bien

$$(a_{11}i + a_{13}k) \wedge j + i \wedge (a_{22}j + a_{23}k) = -a_{13}i - a_{23}j - a_{33}k,$$

$$a_{11}k - a_{13}i + a_{22}k - a_{23}j = -a_{13}i - a_{23}j - a_{33}k,$$

lo que implica $a_{11} + a_{22} + a_{33} = 0$. Por lo tanto la matriz de D en la base $\mathcal{B}$ es

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & M & 0 \\ 0 & 0 & -M^t \end{pmatrix},$$

donde $M = (a_{ij})$ es una matriz 3×3 de traza nula. Recíprocamente toda aplicación lineal $O_s \to O_s$ cuya matriz en $\mathcal{B}$ sea como arriba, se comprueba sin dificultad que es una derivación de L_0. La aplicación $L_0 \to \mathfrak{sl}(3, F)$ tal que $D \mapsto M$ es trivialmente un isomorfismo de álgebras de Lie.

Investigemos ahora las derivaciones $D \in L_1$. Éstas actúan del siguiente modo: $D(e_i) \in X_{12}(F^3)$, $D(X_{12}(F^3)) \subset X_{21}(F^3)$, y $D(X_{21}(F^3)) \subset Fe_1 + Fe_2$. Supongamos pues que $D(e_1) = X_{12}(a)$ para un $a \in F^3$. Naturalmente $D(e_2) = -D(e_1) = -X_{12}(a)$. Además se debe tener $D(X_{12}(x)) = X_{21}(h(x))$ para alguna aplicación lineal $h : F^3 \to F^3$. Como $e_1X_{12}(x) = X_{12}(x)$, al aplicar D obtenemos $X_{12}(a)X_{12}(x) + e_1X_{21}(h(x)) = X_{21}(h(x))$. Esto equivale a $X_{21}(a \wedge x) = X_{21}(h(x))$ y por lo tanto $h(x) = a \wedge x$ para todo $x \in F^3$. Análogamente como $D(X_{21}(x)) = \alpha(x)e_1 + \beta(x)e_2$ para ciertas aplicaciones lineales $\alpha, \beta : F^3 \to F$, entonces, dado que $X_{21}(x)e_1 = X_{21}(x)$, al aplicar D a esta última igualdad se obtiene

$$[\alpha(x)e_1 + \beta(x)e_2]e_1 + X_{21}(x)X_{12}(a) = \alpha(x)e_1 + \beta(x)e_2$$

de donde $\beta(x) = (x, a)$. De forma parecida, al aplicar D a la identidad $e_2X_{21}(x) = X_{21}(x)$ y simplificar, obtenemos $\alpha(x) = -(x, a)$. en resumen $D \in L_1$ si y sólo si existe $a \in F^3$ tal que $D(e_1) = X_{12}(a) = -D(e_2)$, $D(X_{12}(x)) = X_{21}(a \wedge x)$, $D(X_{21}(x)) = -(x, a)(e_1 - e_2)$. En

este caso, la matriz de D en $\mathcal{B}$ se podría representar del siguiente modo:

$$\begin{pmatrix} 0 & a & 0 & \\ 0 & -a & 0 & \\ 0 & 0 & a\wedge i & \\ 0 & 0 & a\wedge j & \\ 0 & 0 & a\wedge k & \\ -(a,i) & (a,i) & 0 & 0 \\ -(a,j) & (a,j) & 0 & 0 \\ -(a,k) & (a,k) & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & a_1 & a_2 & a_3 & 0 & 0 & 0 \\ 0 & 0 & -a_1 & -a_2 & -a_3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & a_3 & -a_2 \\ 0 & 0 & 0 & 0 & 0 & -a_3 & 0 & a_1 \\ 0 & 0 & 0 & 0 & 0 & a_2 & -a_1 & 0 \\ -a_1 & a_1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -a_2 & a_2 & 0 & 0 & 0 & 0 & 0 & 0 \\ -a_3 & a_3 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Conviene observar que los elementos de L_1 admiten una representación matricial por bloques del tipo:

$$\begin{pmatrix} 0 & A & 0 \\ 0 & 0 & A' \\ -A^t & 0 & 0 \end{pmatrix},\ \text{donde } A = \begin{pmatrix} a_1 & a_2 & a_3 \\ -a_1 & -a_2 & -a_3 \end{pmatrix},\ A' = \begin{pmatrix} 0 & a_3 & -a_2 \\ -a_3 & 0 & a_1 \\ a_2 & -a_1 & 0 \end{pmatrix}.$$

Finalmente dejamos al lector la comprobación de que la matriz de una derivación $D \in L_2$ es de la forma:

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & b_1 & b_2 & b_3 \\ 0 & 0 & 0 & 0 & 0 & -b_1 & -b_2 & -b_3 \\ -b_1 & b_1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -b_2 & b_2 & 0 & 0 & 0 & 0 & 0 & 0 \\ -b_3 & b_3 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & b_3 & -b_2 & 0 & 0 & 0 \\ 0 & 0 & -b_3 & 0 & b_1 & 0 & 0 & 0 \\ 0 & 0 & b_2 & -b_1 & 0 & 0 & 0 & 0 \end{pmatrix},$$

o bien

$$\begin{pmatrix} 0 & 0 & B \\ -B^t & 0 & 0 \\ 0 & B' & 0 \end{pmatrix},\ \text{donde } B = \begin{pmatrix} b_1 & b_2 & b_3 \\ -b_1 & -b_2 & -b_3 \end{pmatrix},\ B' = \begin{pmatrix} 0 & b_3 & -b_2 \\ -b_3 & 0 & b_1 \\ b_2 & -b_1 & 0 \end{pmatrix}.$$

Finalmente la representación matricial por bloques de una derivación arbitraria de L, será del tipo:

$$\begin{pmatrix} 0 & A & B \\ -B^t & M & A' \\ -A^t & B' & -M^t \end{pmatrix}, \tag{8.2}$$

con A, A', B, B' y M como antes. Como consecuencia de todo esto, tenemos además que $\dim(L_0) = \dim(\mathfrak{sl}(3,F)) = 8$, $\dim(L_1) = \dim(L_2) = 3$ y $\dim(L) = \dim(L_0) + \dim(L_1) + \dim(L_2) = 8 + 3 + 3 = 14$.

Teorema 31 *En la descomposición $L = L_0 \oplus L_1 \oplus L_2$ los subespacios L_i con $i = 0, 1, 2$ son L_0-módulos irreducibles no isomorfos.*

Dem. Como $L_0 \cong \mathfrak{sl}(3,F)$ que es simple, resulta que en primer lugar que L_0 es un L_0-módulo irreducible. La irreducibilidad de L_1 y L_2 como L_0-módulos es consecuencia del enunciado del problema 105. Lo único que nos quedaría por demostrar es que $L_1 \ncong L_2$ como L_0-módulos, pero esto se deja como ejercicio al lector. ■

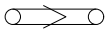
Corolario 21 *El álgebra L es simple.*

Dem. Sea $0 \neq I \lhd L$, si $I \cap L_0 \neq 0$, dado que $L_0 \cong \mathfrak{sl}(3,F)$ es simple y $I \cap L_0 \lhd L_0$ se tendría $L_0 \subset I$ lo que implica $L_1 = [L_0, L_1] \subset [I, L_1] \subset I$ (véase el problema 105). Del mismo modo $L_2 \subset I$ lo que implica $I = L$. Supongamos ahora que $I \cap L_0 = 0$. Como I es un L_0-módulo, aplicando el enunciado del problema 106, las únicas posibilidades que quedan para I son $I = L_1$, $I = L_2$ o $I = L_1 \oplus L_2$. Sin embargo ninguno de los espacios L_1, L_2 o $L_1 + L_2$ es un ideal como se comprueba de inmediato. Por lo tanto la posibilidad $I \cap L_0 = 0$ queda descartada y como $[L, L] \neq 0$, el álgebra L es simple. ■

Corolario 22 *El diagrama de Dynkin de L es g_2.*

Dem. Aplicando el Teorema 30, el diagrama de Dynkin es a_2, b_2, o g_2. Pero si L tiene el diagrama de Dynkin a_2

entonces su sistema de raíces es $\{\pm\alpha, \pm\beta, \pm(\alpha+\beta)\}$ luego $\dim(L) = 2 + 2{,}3 = 8$ en contradicción con que $\dim(L) = 14$. Si el diagrama de Dynkin fuera b_2:



entonces su sistema de raíces sería del tipo $\{\pm a, \pm\beta, \pm(\alpha+\beta), \pm(2\alpha+\beta)\}$, siendo β la raíz larga. En este caso se tendría $\dim(L) = 2 + 2{,}4 = 10$. Por lo tanto el diagrama de Dynkin de L es g_2. ■

Se podría demostrar directamente el hecho de que el diagrama de Dynkin de L es g_2 sin recurrir al Teorema 30. Naturalmente esto requiere algo más de esfuerzo por nuestra parte y dedicaremos el resto de la sección a esta prueba directa. El lector no interesado podría por tanto saltar sin problema hasta la siguiente sección.

Para encontrar el diagrama de Dynkin g_2 es $L = \mathrm{Der}(O_s)$, sin recurrir al teorema de clasificación de los diagramas de Dynkin, el siguiente paso será fijar una subálgebra toral maximal H de L, y determinar las ráices de L respecto de H. Consideremos los elementos h_1 y h_2 de L_0 definidos como sigue: h_1 se obtiene haciendo $M = e_{11} - e_{33}$, $A = B = 0$ en (8.2). Por su parte h_2 se obtiene para $M = e_{22} - e_{33}$, $A = B = 0$. Se comprueba que $H := Fh_1 + Fh_2$ es una subálgebra toral maximal de L (esto se propone como ejercicio en el problema 103).

Consideremos ahora una base de L_0 tomando en primer lugar las matrices h_1 y h_2 y definiendo después las matrices de la forma (8.2) donde $A = B = 0$ mientras que M

va tomando sucesivamente los valores: e_{12}, e_{13}, e_{23}, e_{21}, e_{31} y e_{32}. Un cálculo rutinario demuestra que las matrices de $\mathrm{ad}(h_1)|_{L_0}$ y $\mathrm{ad}(h_2)|_{L_0}$ respecto a dicha base son:

$$\mathrm{ad}(h_1)|_{L_0} \equiv \mathrm{diag}(0,0,1,2,1,-1,-2,-1)$$

$$\mathrm{ad}(h_2)|_{L_0} \equiv \mathrm{diag}(0,0,-1,1,2,1,-1,-2).$$

Podemos ahora tomar en L_1 la base que surge al poner en (8.2) $M = 0$ $B = 0$, $A = I, J, K$ sucesivamente, siendo

$$I = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 0 & 0 \end{pmatrix},\ J = \begin{pmatrix} 0 & 1 & 0 \\ 0 & -1 & 0 \end{pmatrix},\ K = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & -1 \end{pmatrix}.$$

Respecto a esta base las aplicaciones $\mathrm{ad}(h_i)|_{L_1}$, $(i = 1, 2)$ admiten las siguientes representaciones matriciales:

$$\mathrm{ad}(h_1)|_{L_1} \equiv \mathrm{diag}(-1,0,1), \quad \mathrm{ad}(h_2)|_{L_1} \equiv \mathrm{diag}(0,-1,1).$$

Por último definamos en L_2 aquella base formada por las matrices del tipo (8.2) haciendo $M = 0$, $A = 0$, $B = I, J, K$ sucesivamente. Respecto a esta base encontramos las representaciones matriciales:

$$\mathrm{ad}(h_1)|_{L_2} \equiv \mathrm{diag}(1,0,-1), \quad \mathrm{ad}(h_2)|_{L_2} \equiv \mathrm{diag}(0,1,-1).$$

En definitiva podemos construir una base $\mathcal{B}_L$ de L haciendo la unión de las bases que hemos encontrado para L_i $(i = 0, 1, 2)$, de modo que respecto a dicha base los operadores $\mathrm{ad}(h_i)$ $(i = 1, 2)$ se representan del siguiente modo:

$$ad(h_1) \equiv \mathrm{diag}(0,0,1,2,1,-1,-2,-1,-1,0,1,1,0,-1)$$

$$ad(h_2) \equiv \mathrm{diag}(0,0,-1,1,2,1,-1,-2,0,-1,1,0,1,-1).$$

Esto determina completamente la restricción de la forma Killing k de L a H: $k(h_1, h_1) = \mathrm{tr}(\mathrm{ad}(h_1)^2) = 16$, $k(h_1, h_2) = \mathrm{tr}(\mathrm{ad}(h_1)\,\mathrm{ad}(h_2)) = 8$, $k(h_2, h_2) = \mathrm{tr}(ad(h_2)^2) = 16$. Fijémonos entonces en la raíz $\alpha : H \to F$ tal que $\alpha(h_1) = 1$, $\alpha(h_2) = -1$. El hecho de que esta aplicación es raíz se evidencia viendo que el tercer vector de $\mathcal{B}_L$ es un vector propio común de $\mathrm{ad}(h_i)$ con $i = 1, 2$ (luego vector propio común para todos los $\mathrm{ad}(h)$ con $h \in H$). Es fácil calcular el $t_\alpha \in H$ tal que $\alpha = k(t_\alpha, -)$. Se obtiene $t_\alpha = \frac{1}{8}(h_1 - h_2)$. Esto posibilita calcular la longitud de la raíz α que es $\|\alpha\| = \frac{1}{2}$. Por otra parte podemos considerar la raíz $\beta : H \to F$ dada por $\beta(h_1) = -1$, $\beta(h_2) = 0$. En este caso tenemos $t_\beta = -\frac{1}{24}(2h_1 - h_2)$, y $\|\beta\| = \frac{1}{2\sqrt{3}}$. Además ahora es fácil comprobar que el ángulo que forman α y β es $\frac{5\pi}{6}$.

Si denotamos la raíz α mediante el vector $(\alpha(h_1), \alpha(h_2)$ se tendría $\alpha = (1, -1)$, $\beta = (-1, 0)$, el resto de la raíces de L respecto de H se pueden ver en las expresiones matriciales de los operadores $\mathrm{ad}(h_1)$ y $\mathrm{ad}(h_2)$. Estas son (aparte de $\pm\alpha$ y $\pm\beta$) las dadas por $\alpha + \beta = (0, -1)$, $-\alpha - 2\beta = (1, 1)$, $-\alpha - 3\beta = (2, 1)$, $-2\alpha - 3\beta = (1, 2)$ así como sus opuestas. Esto demuestra que el conjunto $\{\alpha, \beta\}$ es una base del sistema de raíces de L relativa a H y el diagrama de Dynkin es precisamente g_2 dado que

$$< \alpha, \beta >< \beta, \alpha >= 4\frac{(\alpha, \beta)^2}{\|\alpha\|^2\|\beta\|^2} = 3.$$

8.3. f_4

8.4. Problemas

Problema 102 *Un álgebra A sobre un cuerpo arbitrario F se dice que es $\mathbb{Z}_n$-graduada (o $n-$ graduada simplemente) cuando A se expresa como una suma directa de subespacios $A = A_0 \oplus \cdots \oplus A_{n-1}$ tales que $A_i A_j \subset A_{i+j}$ (suma módulo n). Observe el lector que A_0 es siempre una subálgebra de A. Demuéstrese que para toda álgebra $\mathbb{Z}_n$-graduada A, el álgebra de Lie $L = Der(A)$ es también $\mathbb{Z}_n$-graduada siendo $L = \oplus_0^{n-1} L_i$, donde*

$$L_i := \{d \in Der(A) : d(A_j) \subset A_{i+j} \forall j\}.$$

Problema 103 *Compruébese que $H := Fh_1 \oplus Fh_2$ es una subálebra toral maximal de $L = Der(O_s)$ (véase la sección relativa a g_2 en este capítulo).*

Problema 104 *Sea $L = L_0 \oplus L_1 \oplus L_2$ una F-álgebra Z_3-graduada de dimensión finita, con forma de Killing k.*

- *Demuéstrese que L_0 es ortogonal a L_1 y a L_2 por la forma Killing k de L. Demuéstrese también que $k(L_i, L_i) = 0$ para $i = 1, 2$. Conclúyase que la matriz de la forma Killing adopta la forma*

$$\begin{pmatrix} A & 0 & 0 \\ 0 & 0 & B \\ 0 & B^t & 0 \end{pmatrix}$$

  para una base conveniente.

- *Conclúyase que L es semisimple si y solo si A es singular y el rango de B coincide con la dimensión de L_1.*

- *Demuéstrese que $L = Der(O_s)$ es semisimple teniendo en cuenta la 3-graduación de L que se explica en la sección relativa a este álgebra.*

Problema 105 *Consideremos el álgebra 3-graduada $L = Der(O_s)$ (véase la sección relativa a g_2 para la graduación). Demuéstrese que $L_i = [L_0, L_i]$ para $i = 1, 2$.*

Problema 106 *Sea L un álgebra de Lie y $M = \oplus_{i \in I} M_i$ un módulo de dimensión finita tal que cada M_i es un L-módulo irreducible y $M_i \ncong M_j$ para $i \neq j$. Demuéstrese que si S es un L-submódulo de M, entonces:*

1. *S contiene una subsuma $\oplus_{i \in J} M_i$ donde $J \subset I$.*

2. *Los L-submódulos de M son las subsumas parciales $\oplus_{i \in J} M_i$ con $J \subset I$.*

Sugerencia: Sea S un L-submódulo de M. Como $S \cap (\oplus_{i \in I} M_i) \neq 0$ debe existir una subsuma $\oplus_{i \in J} M_i$ con $|J|$ mínimo tal que $S \cap (\oplus_{i \in J} M_i) \neq 0$. Tomemos un elemento no nulo $x \in S \cap (\oplus_{i \in J} M_i)$. Entonces la proyección x_i de x en cada M_i $(i \in J)$ es no nula. El conjunto

$$\{t \in M_i : t = x_i, \text{ para algún } x \in S \cap (\oplus_{j \in J} M_j)\}$$

es un submódulo no nulo de M_i luego coincide con M_i. Ahora podemos establecer un isomorfismo de L-módulos $M_i \to M_j$ tal que $x_i \mapsto x_j$. Pero para $i \neq j$ los módulos M_i y M_j no son isomorfos. Esto implica que $|J| = 1$ y por lo tanto $S \cap M_j \neq 0$ para algún j (implicando $M_j \subset S$). Para la segunda parte se puede proceder por inducción sobre el cardinal $|I|$. Si S está contenido en alguna subsuma $\oplus_{i \in J} M_i$ donde $J \subsetneq I$, se aplica la hipótesis de inducción. En caso contrario para cada $i \in I$ existe un $x \in S$ tal que $M_i \ni x_i \neq 0$. Si $x_j \neq 0$ para algún $j \neq i$ podríamos establecer un isomorfismo $M_i \to M_j$ tal que $x_i \mapsto x_j$. Pero sabemos que esto es imposible luego $M_i \subset S$ implicando $S = M$.

Apéndice A

Grupos de Lie lineales

A.1. Preliminares.

Recordemos que un grupo de Lie G es un grupo que además tiene estructura de variedad (analítica por ejemplo) de modo que las operaciones de multiplicación y de inversión de elementos son analíticas. Sin embargo uno puede hasta cierto punto escabullirse del manejo de las variedades limitándose al estudio de los grupos lineales (también conocidos como grupos de Lie de matrices). Estos no son más que los subgrupos cerrados de $\mathfrak{gl}(V)$ para un espacio vectorial real de dimensión finita V. Así pues

Definición 22 *Un grupo de Lie lineal (o de matrices) no es más que un subgrupo cerrado del grupo $GL(V)$ o $GL(n,\mathbb{R})$, estando este grupo dotado de la topología natural que hereda de ser considerado como subespacio de $\mathcal{M}_n(\mathbb{R})$, donde $n = \dim(V)$.*

Lo que para nosotros es una definición, es en realidad un teorema en la teoría general de grupos de Lie. Consideremos ahora un subgrupo uniparamétrico, es decir una aplicación analítica $\varphi : I \to G$, donde I es un intervalo abierto tal que $0 \in I$, $\varphi(0) = 1$ (elemento neutro de G) y $\varphi(s+t) = \varphi(s)\varphi(t)$ para todos $s, t, s+t \in I$. Si derivamos respecto de s en esta última identidad tenemos $\varphi'(s+t) = \varphi'(s)\varphi(t)$ y haciendo $s = 0$ obtenemos $\varphi'(t) = \varphi'(0)\varphi(t)$ con lo que haciendo $a = \varphi'(0)$ tenemos que el subgrupo uniparamétrico φ es solución del problema de contorno:

$$\varphi'(t) = a\varphi(t), \varphi(0) = 1, \varphi'(0) = a. \tag{A.1}$$

Aplicando un teorema adecuado de existencia y unicidad de soluciones para ecuaciones diferenciales, tenemos que:

1. La función $\mathbb{R} \to G$ dada por $t \mapsto \exp(at)$ es una solución de la ecuación que extiende a φ.

2. Dicha solución es única.

Teniendo en cuenta el enunciado del Problema 108, podemos enunciar:

Teorema 32 *Cada subgrupo uniparamétrico $\varphi : I \to G$ de un grupo de Lie lineal G se puede extender a un subgrupo uniparamétrico único $\mathbb{R} \to G$.*

En adelante hablaremos de grupo paramétrico como sinónimo de subgrupo paramétrico. Dado un grupo paramétrico φ de G, el elemento $a = \varphi'(0) \in \mathcal{M}_n(\mathbb{R})$ lo llamaremos generador infinitesimal del grupo ϕ. El espacio tangente de G en 1 es el conjunto

$$\mathfrak{g} = \{\varphi'(0) : \varphi \text{ es un grupo uniparamétrico}\}.$$

Es fácil demostrar que $\mathfrak{g}$ coincide con el conjunto

$$\{a \in \mathcal{M}_n(\mathbb{R}) : \exp(ta) \in G, \forall t \in \mathbb{R}\}.$$

Ahora queremos demostrar que en el conjunto $\mathfrak{g}$ de todos los generadores infinitesimales hay una estructura de espacio vectorial real. Para ello tomemos dos generadores $a = \varphi'(0)$ y $b = \psi'(0)$, donde $\varphi, \psi : \mathbb{R} \to G$ son dos grupos uniparamétricos. Como

$$\varphi(t) = \exp(at) = 1 + ta + \frac{t^2}{2!}a^2 + \cdots$$

$$\psi(t) = \exp(bt) = 1 + tb + \frac{t^2}{2!}b^2 + \cdots,$$

entonces $\exp(at)\exp(bt) = 1 + t(a+b) + O(t^2)$, para todo t real. Por lo tanto

$$\exp(\frac{at}{n})\exp(\frac{bt}{n}) = 1 + \frac{t}{n}(a+b) + \frac{1}{n^2}O(t^2) = 1 + \frac{t(a+b) + \frac{1}{n}O(t^2)}{n},$$

$$\lim_{n\to\infty}\left(\exp(\frac{at}{n})\exp(\frac{bt}{n})\right)^n = \lim_{n\to\infty}\left(1 + \frac{t(a+b) + \frac{1}{n}O(t^2)}{n}\right)^n = \exp(t(x+y)),$$

aplicando el Problema 107. Hemos demostrado pues la fórmula

$$\exp(t(x+y)) = \lim_{n\to\infty}\left(\exp(\frac{at}{n})\exp(\frac{bt}{n})\right)^n, \tag{A.2}$$

para todo $t \in \mathbb{R}$. Observemos que como las exponenciales del miembro de la derecha son elementos de G, y éste, es un grupo cerrado, el límite de la fórmula anterior es un elemento de G por lo que $\exp(t(x+y)) \in G$ para todo $t \in \mathbb{R}$, y por lo tanto $x + y$ es un generador infinitesimal. Así $\mathfrak{g} + \mathfrak{g} \subset \mathfrak{g}$ y obviamente $\mathbb{R}\mathfrak{g} \subset \mathfrak{g}$. Nos gustaría ahora demostrar que $\mathfrak{g}$ es cerrado para el corchete de Lie. Dadas dos matrices cuadradas $a, b \in \mathcal{M}(K)$ (donde K es un cuerpo arbitrario), denotaremos por $[a, b]$ a la nueva matriz $ab - ba$. Este producto se llamara en lo sucesivo el *corchete de Lie*. Entre las identidades que verifica, mencionemos:

1. $[a, a] = 0$ para toda matriz a. Esto implica la anticonmutatividad del producto, y si la característica de K no es dos, equivale a dicha anticonmutatividad.

2. $[[a, b], c] + [[b, c], a] + [[c, a], b] = 0$, para cualesquiera a, b, c.

Lo que queremos demostrar ahora es que $[\mathfrak{g},\mathfrak{g}] \subset \mathfrak{g}$. Para ellos partiremos de las igualdades

$$\exp(at)\exp(bt) = 1 + t(a+b) + \frac{t^2}{2}(a^2+b^2+2ab) + \cdots,$$

$$\exp(-at)\exp(-bt) = 1 - t(a+b) + \frac{t^2}{2}(a^2+b^2+2ab) + \cdots,$$

$$\exp(at)\exp(bt)\exp(at)^{-1}\exp(bt)^{-1} = 1 + t(a+b) - t(a+b) +$$

$$+\frac{t^2}{2}(a^2+b^2+2ab) + \frac{t^2}{2}(a^2+b^2+2ab) - t^2(a+b)^2 + O(t^3) =$$

$$= 1 + t^2(a^2+b^2+2ab-a^2-b^2-ab-ba) = 1 + t^2[a,b] + O(t^3).$$

Podemos pues afirmar que

$$\exp\left(\frac{at}{n}\right)\exp\left(\frac{bt}{n}\right)\exp\left(\frac{at}{n}\right)^{-1}\exp\left(\frac{bt}{n}\right)^{-1} = 1 + \frac{t^2}{n^2}[a,b] + \frac{O(t^3)}{n^3},$$

y tomando límites:

$$\lim_{n\to\infty}\left(\exp\left(\frac{at}{n}\right)\exp\left(\frac{bt}{n}\right)\exp\left(\frac{at}{n}\right)^{-1}\exp\left(\frac{bt}{n}\right)^{-1}\right)^{n^2} =$$

$$= \lim_{n\to\infty}\left(1 + \frac{t^2}{n^2}[a,b] + \frac{O(t^3)}{n^3}\right)^{n^2} = \lim_{n\to\infty}\left(1 + \frac{t^2[a,b] + \frac{O(t^3)}{n}}{n^2}\right)^{n^2} =$$

$$= \exp(t^2[a,b]),$$

aplicando el Problema 107. Tenemos pues

$$\lim_{n\to\infty}\left(\exp\left(\frac{at}{n}\right)\exp\left(\frac{bt}{n}\right)\exp\left(\frac{at}{n}\right)^{-1}\exp\left(\frac{bt}{n}\right)^{-1}\right)^{n^2} = \exp(t^2[a,b]). \tag{A.3}$$

Como las exponenciales que aparecen en esta fórmula son elementos de G y éste es cerrado, concluimos que $\exp(t^2[a,b]) \in G$ para todo $t \in \mathbb{R}$. Esto implica que $\exp(t[a,b]) \in G$ para todo $t \geq 0$. Para los $t < 0$, tenemos $\exp(t[a,b]) = \exp(-t[a,b])^{-1} \in G$. En definitiva $\exp(t[a,b]) \in G$ para todo t y por lo tanto $[a,b] \in g$ para todos $a, b \in \mathfrak{g}$. Hemos demostrado pues que $\mathfrak{g}$ es un álgebra de Lie real a la que llamaremos el *álgebra de Lie* del grupo de Lie G. De hecho $\mathfrak{g}$ y G están estrechamente relacionadas y para muchas tareas podemos sustituir el uno por el otro. Pero sustituir G por $\mathfrak{g}$ tiene la ventaja de que mientras G es un objeto no lineal que puede ser tremendamente retorcido, su álgebra de Lie es un objeto lineal, en general más sencillo de tratar. Para ilustrar la estrecha relación de la que hemos hablado con anterioridad, podemos ver gracias a la fórmula A.3 como ciertas propiedades

pasan de G a $\mathfrak{g}$. Por ejemplo si G es abeliano, la fórmula A.3 implica que $1 = \exp(t[a,b])$ para todo $t \in \mathbb{R}$. Pero entonces

$$1 = 1 + t[a,b] + O(t^2) \Rightarrow t[a,b] + O(t^2) = 0, \forall t,$$

y dividiendo entre t tenemos

$$0 = [a,b] + \lim_{t\to 0} \frac{O(t^2)}{t} = [a,b]$$

por lo tanto $\mathfrak{g}$ es abeliana.

A.2. Algunos ejemplos

Vamos a ilustrar las ideas de la sección anterior con algunos ejemplos. Consideremos en primer lugar el grupo $G = \mathrm{GL}(n,\mathbb{R})$ de todas las matrices inversibles. Entonces su álgebra de Lie $\mathfrak{g}$ consiste en todos los elementos a de $\mathfrak{gl}(n,\mathbb{R}) = \mathcal{M}_n(\mathbb{R})$ tales que $\exp(ta) \in \mathrm{GL}(n,\mathbb{R})$ para todo $t \in \mathbb{R}$. Pero esto se cumple para toda $a \in \mathfrak{gl}(n,\mathbb{R})$ pues $\exp(ta)$ es inversible con inverso $\exp(-ta)$. Otro ejemplo interesante es el grupo lineal $G = \mathrm{O}(n)$ formado por las matrices $a \in \mathcal{M}_n(\mathbb{R})$ tales que $aa^* = 1$ donde $x \mapsto x^*$ denota la transposición matricial. Este es un subconjunto cerrado de $\mathcal{M}_n(\mathbb{R})$ pues está definido como el conjunto de ceros de un sistema de ecuaciones algebraicas. Su álgebra de Lie $\mathrm{o}(n)$, está formada por las matrices a tales que $\exp(ta) \in \mathrm{O}(n)$ para todo $t \in \mathbb{R}$. entonces se debe tener:

$$\begin{aligned} 1 = \exp(ta)\exp(ta)^* = \exp(ta)\exp(ta^*) &= \left(1 + ta + O(t^2)\right)\left(1 + ta^* + O(t^2)\right) \\ &= 1 + t(a + a^*) + O(t^2), \end{aligned}$$

por lo tanto $t(a + a^*) + O(t^2) = 0$ $(t \in \mathbb{R})$. Esto implica que se debe tener $a + a^* = 0$. En otras palabras el álgebra de Lie de $\mathrm{O}(n)$ es el álgebra de Lie $\mathrm{o}(n)$ de las matrices reales $n \times n$ antisimétricas. El grupo $\mathrm{O}(n)$ no es conexo, de hecho se descompone como unión disjunta de dos componentes conexas $\mathrm{O}^+(n)$ y $\mathrm{O}^-(n)$, donde las matrices de $\mathrm{O}^+(n)$ son las ortogonales de determinante 1, mientras que las de $\mathrm{O}^-(n)$ son las de determinante -1. La componente conexa $\mathrm{O}^+(n)$ resulta ser a su vez un grupo lineal que se suele denotar por $\mathrm{SO}(n)$. Toda matriz antisimétrica es semejante a una matriz diagonal por bloques donde cada bloque es de la forma

$$\begin{pmatrix} 0 & t \\ -t & 0 \end{pmatrix}, \qquad t \in \mathbb{R}.$$

La exponencial de dicha matriz es la matriz de una rotación plana:

$$\begin{pmatrix} \cos t & \sin t \\ -\sin t & \cos t \end{pmatrix}.$$

Por lo tanto la exponencial de una matriz antisimétrica es semejante a una matriz diagonal por bloques, siendo cada bloque la matriz de una rotación plana. Como corolario el

determinante de cada matriz $\exp(ta)$ (con a antisimétrica) es 1. Esto demuestra que el álgebra de Lie de $\mathrm{SO}(n)$ (denotada $\mathrm{so}(n)$) coincide con el álgebra de Lie de las matrices antisimétricas reales $n \times n$. Se tiene pues

$$\mathrm{so}(n) = \mathfrak{o}(n).$$

Por lo tanto dos grupos de Lie no isomorfos (uno es conexo y el otro no), pueden tener la misma álgebra de Lie. Para la propiedad recíproca tenemos que exigir a los grupos la propiedad de ser simplemente conexos: dos grupos de Lie (no necesariamente lineales) simplemente conexos G y H son isomorfos si y sólo si sus álgebras de Lie son isomorfas (véase [8, Corollary 8.7, p. 173]).

A.3. Representaciones de SO(2)

Dados dos grupos de Lie lineales G_1 y G_2, diremos que $f : G_1 \to G_2$ es un homomorfismo de grupos de Lie si es un homomorfismo de grupos que es analítico. Un isomorfismo $f : G_1 \to G_2$ será entonces un isomorfismos de grupos que es bianalítico (tanto f como f^{-1} son analíticas). Una representación de un grupo G es un homomorfismo de grupos de Lie $\rho : G \to \mathrm{GL}(V)$ para algún espacio vectorial real V de dimensión finita n. Según nos convenga consideraremos a las representaciones como aplicaciones $G \to \mathrm{GL}(V)$ o bien $G \to \mathrm{GL}(n, \mathbb{R})$. Una representación $\rho : G \to \mathrm{GL}(V)$ se dice que es irreducible cuando para todo subespacio S de V se tiene

$$\rho(G)S \subset S \Rightarrow S = 0, \text{ o } S = V.$$

Se sabe además que toda representación finita (es decir, con $\dim(V) < \infty$), de un grupo de Lie compacto es suma directa de represetaciones irreducibles (véase por ejemplo [6, Theorem 1, p. 90]). Consideremos entonces el grupo (compacto) $\mathrm{SO}(2)$, y sea $\rho : \mathrm{SO}(2) \to \mathrm{GL}(V)$ una representación irreducible con $\dim(V) = n$ (finita). Sea $\alpha : (-\pi, \pi) \to \mathrm{SO}(2)$ la aplicación dada por

$$\alpha(t) = \begin{pmatrix} \cos t & \sin t \\ -\sin t & \cos t \end{pmatrix}.$$

La composición $\varphi := \rho\alpha : (-\pi, \pi) \to \mathrm{GL}(V)$ es entonces un grupo paramétrico (analítico) y podemos asegurar que $\varphi(t) = \exp(tA)$ para algún $A \in \mathfrak{gl}(V)$. Recurriendo a las forma canónica real sabemos que o bien A tiene un autovalor real (y por lo tanto un subespacio invariante de dimensión 1), o bien todos los autovalores de A son complejos (en cuyo caso A tiene un subespacio invariante de dimensión 2). Sea pues S un subespacio de V de dimensión uno o dos invariante por A. Entonces S es invariante por $\exp(tA)$ para todo $t \in \mathbb{R}$. Esto implica que $\rho(\mathrm{SO}(2))S \subset S$ y como la representación ρ es irreducible concluimos que $V = S$ y por lo tanto:

Proposición 21 *Toda representación irreducible finita de SO(2) es de dimensión uno o dos.*

A.4. Ecuaciones diferenciales

Consideremos la ecuación diferencial en derivadas parciales:

$$\frac{\partial^2 f}{\partial x^2} + \frac{\partial^2 f}{\partial y^2} = 0. \tag{A.4}$$

Evidentemente el conjunto de soluciones de la ecuación es un espacio vectorial real del que podemos quedarnos con un subespacio de dimensión finita cualquiera. Sea pues V un subespacio de dimensión finita del espacio de soluciones. Entonces si $f(x,y) \in V$, se demuestra sin dificultad que la nueva función $f(x\cos\theta - y\sin\theta, x\sin\theta + y\cos\theta)$ es también solución de (A.4) luego pertenece a V. De este modo tenemos una aplicación $\sigma : \mathrm{SO}(2) \to \mathrm{GL}(V)$ dada por $r \mapsto \sigma(r)$ donde $\sigma(r) : V \to V$ es el automorfismo (lineal) tal que $\sigma(r)f = f \circ r$. El lector puede comprobar que se trata de una representación del grupo SO(2) en el espacio de soluciones V. Como se trata de una representación finita, es automáticamente suma directa de representaciones irreducibles (que como sabemos son de dimensiones uno o dos). Por lo tanto la ecuación diferencial tiene espacios de soluciones de dimensión uno o dos. Analicemos los dos caso. Sea S un espacio de soluciones unidimensional. Sea $f \in S$ un generador del espacio. Entonces $\sigma(r)f \in S$ para toda rotación $r \in \mathrm{SO}(2)$. En definitiva para cada θ existe un escalar $\lambda(\theta)$ tal que

$$f(x\cos\theta - y\sin\theta, x\sin\theta + y\cos\theta) = \lambda(\theta) f(x,y),$$

para cualesquiera x, y. Haciendo $y = 0$ se tiene $f(x\cos\theta, x\sin\theta) = \lambda(\theta) f(x,0)$ para todos x, θ. Haciendo $\rho = x$ podemos escribir

$$f(\rho\cos\theta, \rho\sin\theta) = \lambda(\theta)\mu(\rho), \tag{A.5}$$

donde $\mu(\rho) = f(\rho, 0)$. De este modo hemos encontrado la forma que deben tener las soluciones de la ecuación (A.4) que pertenezcan a representaciones unidimensionales. Sustituyendo una función genérica del tipo anterior en la ecuación (A.4), esta se transforma en una ecuación diferencial ordinaria. Tomando por ejemplo $\mu(\rho) = 1$ para todo ρ, podemos encontrar soluciones que sólo dependan de θ. El lector puede comprobar trivialmente que dichas soluciones son de la forma

$$f(x,y) = k\arctan(\frac{y}{x}) + h,$$

donde h, k son constantes reales. Si hacemos $\lambda(\theta) = 1$, encontraremos las soluciones que sólo dependan de ρ. El lector puede comprobar que se trata de las funciones:

$$f(x,y) = k\log(\sqrt{x^2+y^2}) + h, \quad h, k \in \mathbb{R}.$$

Podríamos encontrar otras soluciones e incluso la solución general del tipo $\lambda(\theta)\mu(\rho)$. Dejamos al lector comprobar que tales soluciones son

$$\left(b + a\ \arctan(\frac{y}{x})\right)\ \left(\log(\sqrt{x^2+y^2})\, c_1 + c_2\right),$$

donde $a, b, c_1, c_2 \in \mathbb{R}$. Vamos ahora a analizar las soluciones que provienen de espacios de dimensión dos. Si fijamos una base $\alpha(x,y), \beta(x,y)$ de dicho espacio de soluciones, se debe tener $\sigma(r)\alpha = \lambda\alpha + \mu\beta$, y también $\sigma(r)\beta = \lambda'\alpha + \mu'\beta$ siendo λ, λ', μ y μ' reales que dependen de la rotación r. Por lo tanto podemos escribir

$$\alpha(x\cos\theta - y\sin\theta, x\sin\theta + y\cos\theta) = \lambda(\theta)\alpha(x,y) + \mu(\theta)\beta(x,y),$$

$$\beta(x\cos\theta - y\sin\theta, x\sin\theta + y\cos\theta) = \lambda_1(\theta)\alpha(x,y) + \mu_1(\theta)\beta(x,y).$$

Haciendo $x = \rho$, $y = 0$ se tiene

$$\alpha(\rho\cos\theta, \rho\sin\theta) = \lambda(\theta)\delta(\rho) + \mu(\theta)\gamma(\rho),$$

$$\beta(\rho\cos\theta, \rho\sin\theta) = \lambda_1(\theta)\delta(\rho) + \mu_1(\theta)\gamma(\rho),$$

donde $\delta(\rho) = \alpha(\rho, 0)$, $\gamma(\rho) = \beta(\rho, 0)$. En definitiva hemos encontrado la forma general de las soluciones que forman la representación irreducible bidimensional. De hecho no es difícil, a partir de esta información llegar a la solución general de la representación bidimensional. Además la solución general de la ecuación debe ser suma de soluciones de uno u otro tipo por lo que tenemos también un modelo para la solución general de la ecuación.

A.5. Consideraciones finales

Este capítulo no ha sido mas que una breve introducción a las nociones fundamentales de la teoría de grupos de Lie. Nos han quedado muchos aspectos por vislumbrar. Sirva esta sección final para añadir alguna apostilla sobre estos.

Supongamos que $f : G \to G'$ es un homomorfismo de grupos de Lie. Entonces cada subgrupo uniparamétrico $\alpha : I \to G$ nos proporciona un subgrupo uniparamétrico $f \circ \alpha : I \to G'$. Podemos por lo tanto definir una aplicación $T_1(f) : T_1(G) \to T_1(G')$ tal que $\alpha'(0) \mapsto (f \circ \alpha)'(0)$ para cada subgrupo uniparamétrico α. Se comprueba sin dificultad que $T_1(f)$ es una aplicación lineal. Pero resulta que además $T_1(f)$ es un homomorfismo de álgebras de Lie (lo cual resulta algo más complicado de demostrar). El homomorfismo $T_1(f)$ hace comutativo el diagrama:

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ {\scriptstyle \exp}\uparrow & & \uparrow{\scriptstyle \exp} \\ T_1(G) & \xrightarrow[T_1(f)]{} & T_1(G') \end{array}$$

Tenemos así un vínculo muy estrecho entre los grupos de Lie y sus respectivas álgebras. El par de aplicaciones $G \to T_1(G)$, $f \mapsto T_1(f)$ se puede ver como un functor entre la categoría de grupos de Lie lineales y la de álgebras de Lie. En efecto, dados dos homomorfismos de grupos de Lie

$$G \xrightarrow{f} G' \xrightarrow{g} G''$$

las propiedades

$$T_1(g \circ f) = T_1(g) \circ T_1(f)$$
$$T_1(1_G) = 1_{T_1(G)},$$

son de comprobación inmediata. Como se mencionó en secciones anteriores, para grupos de Lie simplemente conexos G y G', se tiene $G \cong G'$ si y sólo si $T_1(G) \cong T_1(G')$ (como álgebras de Lie).

A.6. Problemas.

Problema 107 *Sea A un álgebra de Banach asociativa con unidad $1 \in A$. tomemos una sucesión convergente en A con límite $a \in A$, es decir $\lim_{n\to\infty} a_n = a$. Demuéstrese que entonces*

$$\lim_{n\to\infty} \left(1 + \frac{a_n}{n}\right)^n = \exp(a).$$

Problema 108 *Supongamos dado un grupo uniparamétrico $\varphi : (-\epsilon, \epsilon) \to G$, $(\epsilon \in \mathbb{R})$ en un grupo de Lie lineal, tal que $\varphi(t) = \exp(ta)$, para una cierta matriz a y todo $t \in (-\epsilon, \epsilon)$. Demuéstrese que para todo $t \in \mathbb{R}$, la matriz $\exp(ta) \in G$ lo que permitiría extender φ a un grupo uniparamétrico global $\mathbb{R} \to G$.*

Problema 109 *Demuestrese que la descomposición en unión disjunta $O(n) = O^+(n) \cup O^-(n)$ es de hecho la descomposición del espacio topológico $O(n)$ en sus dos componentes conexas $O^{\pm}(n)$.*

Bibliografía

[1] G.H. Hardy y E.M. Wright, *An Introduction to the Theory of Numbers. Fith Edition.* Oxford Science Publications. Claredon Press, Oxford, 1979.

[2] J. E. Humphreys, *Introduction to Lie Algebras and Representation Theory.* Springer-Verlag. New York Heidelberg Berlin. 1972.

[3] N. Jacobson, *Lie Algebras.* Wiley Interscience. New York-London, 1962.

[4] L. Kadison y M. T. Kromann, *Projective Geometry and Modern Algebra.* Birkhäuser. Boston-Basel-Berlin, 1996.

[5] I. Kaplansky, *Lie Algebras and Locally Compact Groups.* U. of Chicago Press. Chicago-London. 1971.

[6] G. Pichon, *Groupes de Lie, Représentations linéaires et applications.* Hermann Paris, Collection Méthodes.

[7] M. Postnikov. *Lecons de Géométrie. Groupes et algèbres de Lie.* Editions Mir. 1985.

[8] A. A. Sagle y R. E. Walde. *Introduction to Lie groups and Lie algebras.* Academic Press. New York and London. 1973.

[9] R. D. Schafer, *An Introduction to Nonassociative Algebras.* Academic Press, NY-San Francisco-London, 1966.

[10] K. A. Zhevlakov, A. M. Slin'ko, I. P. Shestakov, A. I. Shirshov. *Rings that are nearly associative.* Academic Press, NY-San Francisco-London, 1982.