# Álgebras, Grupos y Representaciones

Universidad de Granada

Curso 2019/2020

José Gómez Torrecillas

gomezj@ugr.es

Notas para el curso homónimo.

# Índice general

# 1. Módulos y Álgebras

En este curso, la noción de anillo es central. Supondremos que este concepto, y algunos hechos fundamentales alrededor del mismo, son conocidos, tal y como deben de estudiarse en la asignatura *Álgebra I*. La información necesaria puede encontrarse en el Capítulo 2 de [1]. Subrayemos que, como allí, nuestros anillos no tiene por qué ser conmutativos.

También se suponen conocimientos básicos de Álgebra Lineal. Aquellos que necesitemos[1], y que puedan no estar cubiertos por las asignaturas correspondientes del Grado en Granada, se incluyen en el presente texto.

El material expuesto aquí se encuentra, en su mayor parte, y más desarrollado, aunque no siempre de la misma forma, en los excelentes libros [2] y [3].

## 1.1 Homomorfismos de anillos y módulos

Sea $M$ un grupo aditivo, es decir, un grupo abeliano en el que usamos notación aditiva. Así, la operación binaria de grupo será denotada por $+$ y el elemento neutro por 0. Consideremos el conjunto

$$\mathrm{End}(M) = \{f : M \to M \mid f \text{ es homomorfismo de grupos}\}.$$

Para $f, g \in \mathrm{End}(M)$ definimos $f+g : M \to M$ por

$$(f+g)(m) = f(m) + g(m), \qquad \forall m \in M.$$

Una comprobación rutinaria muestra que $f+g \in \mathrm{End}(M)$. De esta manera, tenemos definida una operación binaria en $\mathrm{End}(M)$. Esto debe ser comprobado por el alumno, así como que, con esta operación, $\mathrm{End}(M)$ resulta ser un grupo aditivo. Nótese que el elemento neutro será la aplicación $0 : M \to M$ definida por $0(m) = 0$ para todo $m \in M$ que, a todas

[1] Fundamentalmente, teoría seria de diagonalización de endomorfismos.

luces, pertenece a $\mathrm{End}(M)$. También es recomendable comprobar que si $f,g \in \mathrm{End}(M)$, entonces $g \circ f \in \mathrm{End}(M)$. De esta manera, la composición dota a $\mathrm{End}(M)$ de una segunda operación binaria. Obviamente, la aplicación identidad $id_M : M \to M$ es un elemento neutro para la composición.

**Proposición 1.1.1** Si $M$ es un grupo aditivo, entonces $(\mathrm{End}(M), +, 0, \circ, id_M)$ es un anillo.

*Demostración.* De nuevo, es un ejercicio que, si bien puede resultar aburrido, es recomendable hacer. ■

**Definición 1.1.1** El anillo definido obtenido en la Proposición 1.1.1 se llama *anillo de endomorfismos de M*.

R Si $M = \{0\}$, entonces $\mathrm{End}(M) = \{0\}$. En este caso, $id_M = 0$, claro.

▪ **Ejercicio 1.1** Sea $A$ un anillo. Diremos que $A$ es *trivial* si $A = \{0\}$. Demostrar que $A$ es trivial si, y sólo si, $1 = 0$. (Aquí, " 1" denota el elemento neutro de $A$ para el producto).

Estamos preparados para dar una definición fundamental en este curso.

**Definición 1.1.2** Sea $A$ un anillo y $M$ un grupo aditivo. Una estructura de *$A$–módulo* sobre $M$ es un homomorfismo de anillos $\varphi : A \to \mathrm{End}(M)$. Diremos entonces que $M$ es un $A$–módulo. Dicho módulo se dice *fiel* si $\varphi$ es inyectivo.

**Ejemplo 1.1** Sea $V$ un espacio vectorial sobre un cuerpo $K$. Definimos $\varphi : K \to \mathrm{End}(M)$ por $\varphi(k)(v) = kv$ para todo $k \in K$ y $v \in V$. De los axiomas de espacio vectorial se deduce de manera rutinaria, pero recomendable para principiantes, que $\varphi$ es un homomorfismo de anillos. Por tanto, $V$ es un $K$–módulo. ▪

**Ejemplo 1.2** Sea $M$ un grupo aditivo y $\chi : \mathbb{Z} \to \mathrm{End}(M)$ el único homomorfismo de anillos. Recordemos que este homomorfismo de anillos está determinado por la condición $\chi(1) = id_M$. Vemos, así, que $M$ tiene una (única) estructura de $\mathbb{Z}$–módulo. ▪

Gran parte de la literatura define los módulos de manera distinta a como lo hemos hecho aquí. Distinta, pero equivalente, según vamos a discutir seguidamente.

**Proposición 1.1.2** Sea $M$ un grupo aditivo y $A$ un anillo. Existe una biyección entre

1. Estructuras de $A$–módulo sobre $M$.
2. Operaciones binarias $\cdot : A \times M \to M$ sujetas a las siguientes condiciones:
   a) $a \cdot (m + m') = a \cdot m + a \cdot m'$ para todo $a \in A, m, m' \in M$.
   b) $(a + a') \cdot m = a \cdot m + a' \cdot m$ para todo $a, a' \in A, m \in M$.
   c) $(aa') \cdot m = a \cdot (a' \cdot m)$ para todo $a, a' \in A, m \in M$.
   d) $1 \cdot m = m$ para todo $m \in M$.

*Demostración.* Vamos a describir la correspondencia biyectiva mencionada en el enunciado. Si $\varphi : A \to \mathrm{End}(M)$ es un homomorfismo de anillos, definimos

$$a \cdot m = \varphi(a)(m), \qquad \text{para } a \in A, m \in M.$$

Esto define una operación binaria $\cdot : A \times M \to M$. Que la misma satisface las condiciones listadas en 2 se deduce de una comprobación rutinaria. Comprobemos, por ejemplo, $2c$): dados $a, a' \in A, m \in M$, tenemos

$$(aa') \cdot m = \varphi(aa')(m) = (\varphi(a) \circ \varphi(a'))(m) = \varphi(a)(\varphi(a')(m)) = a \cdot (a' \cdot m),$$

donde, en la segunda igualdad, hemos usado que $\varphi$ es multiplicativa (esto es, preserva productos).

Recíprocamente, dada una operación binaria como la descrita en 2, definimos $\varphi : A \to \mathrm{End}(M)$ por

$$\varphi(a)(m) = a \cdot m, \qquad \text{para } a \in A, m \in M.$$

Ahora, partiendo de las condiciones $2a$, $2b$, $2c$ y $2d$ se comprueba sin dificultad que $\varphi$ ciertamente define un homomorfismo de anillos. Por ejemplo, que $\varphi(a) \in \mathrm{End}(M)$ para todo $a \in A$ se deduce de $2a$. ■

R De la misma forma que el producto de dos elementos de un anillo, si el contexto lo permite, se denota por yuxtaposición, así, para un $A$–módulo $M$, usaremos la notación $am = a \cdot m$ para $a \in A$, $m \in M$. Lo que hace los cálculos más legibles y fáciles de manejar.

**Módulo regular.** Dado un anillo $A$, tenemos el homomorfismo de anillos

$$\lambda : A \to \mathrm{End}(A)$$

que asigna a cada $a \in A$ el endomorfismo $\lambda(a) : A \to A$ definido por

$$\lambda(a)(a') = aa'$$

para todo $a' \in A$. Así, $A$ es un $A$–módulo, gracias a su multiplicación. Este es el llamado "módulo regular".

**Restricción de escalares.** Consideremos $M$ un módulo sobre un anillo $A$ y un homomorfismo de anillos $\rho : R \to A$, donde $R$ es, claro, un anillo. Si

$$\varphi : A \to \mathrm{End}(M)$$

es el homomorfismo de anillos que da estructura de $A$–módulo a $M$, entonces

$$\varphi \circ \rho : R \to \mathrm{End}(M)$$

es un homomorfismo de anillos. Por tanto, dota a $M$ de estructura de $R$–módulo. Este proceso se llama *restricción de escalares*.

**Ejemplo 1.3** Dado un homomorfismo de anillos $\rho : R \to A$, tenemos que, por restricción de escalares, $A$ resulta ser un $R$–módulo. Concretamente, la acción de $R$ sobre $A$ viene dada, a la luz de la Proposición 1.1.2, por

$$r \cdot a = \rho(r)a$$

para todo $a \in A$ y todo $r \in R$. ■

**Ejemplo 1.4** Sea $V$ un espacio vectorial sobre un cuerpo $K$ y $T : V \to V$ una aplicación lineal. Sea $K[X]$ el anillo de polinomios en una indeterminada $X$ con coeficientes en $K$. Para $f = f_0 + f_1X + \cdots + f_nX^n \in K[X]$, tomemos el operador $f(T) \in \mathrm{End}(V)$ definido por

$$f(T) = f_0 id_V + f_1T + \cdots + f_nT^n.$$

Una comprobación rutinaria muestra que la aplicación $e_T : K[X] \to \mathrm{End}(V)$ definida por $e_T(f) = f(T)$ para todo $f \in K[X]$ es un homomorfismo de anillos y, así, $V$ viene a ser un $K[X]$–módulo. En resumen, un par $(V,T)$ formado por un $K$–espacio vectorial y una aplicación lineal $T : V \to V$ proporciona una estructura de $K[X]$–módulo sobre $V$.

El proceso recíproco funciona como sigue. Supongamos que $V$ es un $K[X]$–módulo. Dado que $K$ es un subanillo de $K[X]$, mediante restricción de escalares dotamos a $V$ de estructura de $K$–espacio vectorial. Por otra parte, definamos $T : V \to V$ por $T(v) = X \cdot v$ para todo $v \in V$. Comprobemos que $T$ es $K$–lineal. Dados $u, v \in V$ y $k \in K$, tenemos

$$T(u+v) = X \cdot (u+v) = X \cdot u + X \cdot v = T(u) + T(v),$$

y

$$T(k \cdot u) = X \cdot (k \cdot u) = (Xk) \cdot u = (kX) \cdot u = k \cdot (X \cdot u) = k \cdot T(u).$$

Observemos que, en el segundo cálculo, hemos usado que $kX = Xk$.

Que ambos procesos son recíprocos entre sí supone una fácil comprobación.

En definitiva, dar un $K[X]$–módulo es equivalente a dar un $K$–espacio vectorial $V$ junto con una aplicación lineal $T : V \to V$. Esto sugiere que clasificar endomorfismos $K$–lineales es un problema equivalente a clasificar $K[X]$–módulos. ■

**Ejemplo 1.5** Sea $C^\infty(\mathbb{R})$ el epacio vectorial real de todas las funciones de clase infinito definidas en $\mathbb{R}$. Consideremos la estructura de $\mathbb{R}[X]$–módulo sobre $C^\infty(\mathbb{R})$ proporcionada por la aplicación lineal $D : C^\infty(\mathbb{R}) \to C^\infty(\mathbb{R})$ que asocia a cada función $f$ su derivada $D(f) = f'$.

Calculemos

$$(X^2+1) \cdot \sin(t) = (X^2) \cdot \sin(t) + 1 \cdot \sin(t) = X \cdot (X \cdot \sin(t))) + \sin(t) = 0.$$

Así que tenemos que $(X^2+1) \cdot \sin(t) = 0$, y vemos que, en un módulo, es posible que ocurra $a \cdot m = 0$ con $a \neq 0$ y $m \neq 0$. Esto entraña una profunda diferencia entre la teoría de espacios vectoriales y la de módulos. ■

**Notación por yuxtaposición.** En lo que sigue, salvo que el contexto recomiende romper alguna ambigüedad, usaremos la notación $am$ para referirnos al elemento $a \cdot m$, para $m \in M$, un $A$–módulo.

## 1.2 Álgebras asociativas unitales

Vamos a introducir la noción de álgebra asociativa unital. Necesitamos un resultado previo.

**Lema 1.2.1** Dado un anillo $A$, el subconjunto

$$Z(A) = \{c \in A \mid ca = ac \text{ para todo } a \in A\}$$

es un subanillo conmutativo de $A$ llamado *centro* de $A$.

*Demostración.* Como $1 \in Z(A)$, tenemos que $Z(A)$ es no vacío. Veamos que es un subgrupo aditivo de $A$. Si $c, c' \in Z(A)$, entonces, para todo $a \in A$, tenemos

$$(c - c')a = ca - c'a = ac - ac' = a(c - c').$$

Luego $c - c' \in Z(A)$. Por último, comprobemos que si $c, c' \in Z(A)$, entonces $cc' \in Z(A)$. En efecto, para $a \in A$,

$$(cc')a = c(c'a) = c(ac') = (ca)c' = (ac)c' = a(cc').$$

Así, $cc' \in Z(A)$. ■

■ **Ejercicio 1.2** Sea $K$ un cuerpo y $M_n(K)$ el anillo de matrices cuadradas de orden $n$ con entradas en $K$. Demostrar que $Z(M_n(K)) = \{kI_n \mid k \in K\}$, donde $I_n$ es la matriz identidad de orden $n$.

**Proposición 1.2.2** Sea $A$ un anillo y $K$ un cuerpo. Existe una biyección entre

1. Homomorfismos de anillos $\rho : K \to Z(A)$.
2. Estructuras de $K$–espacio vectorial sobre $A$ tales que la multiplicación de $A$ es una aplicación $K$–bilineal.

*Demostración.* A lo largo de esta prueba, denotaremos por $a * b$ el producto en $A$ de $a, b \in A$. Tengamos presente que esta multiplicación verifica las dos propiedades distributivas con respecto de la suma.

Supongamos que $\rho : K \to Z(A)$ es un homomorfismo de anillos. Como $Z(A)$ es un subanillo de $A$, podemos considerar $\rho : K \to A$. Así, $A$ viene a ser un $K$–espacio vectorial, por restricción de escalares. Comprobemos que la multiplicación de $A$ es $K$–bilineal. Dados $k \in K$, $a, b \in A$, tenemos

$$k(a * b) = \rho(k) * (a * b) = (\rho(k) * a) * b = (ka) * b,$$

y

$$k(a * b) = (\rho(k) * a) * b = (a * \rho(k)) * b = a * (\rho(k) * b) = a * (kb).$$

Recíprocamente, supongamos que $A$ es un $K$–espacio vectorial tal que la multiplicación de $A$ es $K$–bilineal, con lo que

$$k(a * b) = (ka) * b = a * (kb) \tag{1.1}$$

para todo $k \in K$ y todo $a, b \in A$. Definamos $\rho : K \to A$ por $\rho(k) = k1_A$, donde $1_A$ denota el "uno" de $A$, y la yuxtaposición la acción de $K$ sobre los elementos de $A$. Bien, los siguientes cálculos muestran que $\rho$ es un homomorfismo de anillos. Tomamos $k, k' \in K$ y $1_K$ el uno de $K$.

$$\rho(k + k') = (k + k')1_A = k1_A + k'1_A = \rho(k) + \rho(k'),$$

$$\rho(kk') = (kk')1_A = k(k'1_A) = k(k'(1_A * 1_A)) \overset{(1.1)}{=} k(1_A * (k'1_A)) \overset{(1.1)}{=} (k1_A) * (k'1_A) = \rho(k) * \rho(k'),$$

$$\rho(1_K) = 1_K 1_A = 1_A.$$

Comprobemos que $Im(\rho) \subseteq Z(A)$. Así, dados $k \in K$ y $a \in A$, tenemos

$$\rho(k) * a = (k1_A) * a \overset{(1.1)}{=} k(1_A * a) = ka = k(a * 1_A) \overset{(1.1)}{=} a * (k1_A) = a * \rho(k).$$

Así que podemos considerar que $\rho : K \to Z(A)$.

Que ambos procesos son mutuamente recíprocos se deja como comprobación al estudiante. ■

En lo que sigue, $K$ seguirá denotando un cuerpo.

**Definición 1.2.1** Una estructura de *$K$–álgebra* (asociativa y unital[a]) sobre un anillo $A$, donde $K$ es un cuerpo, es un homomorfismo de anillos $\rho : K \to A$ tal que $Im(\rho) \subseteq Z(A)$. En vista de la Proposición 1.2.2, esto es equivalente a requerir una estructura de $K$–espacio vectorial en $A$ de manera que la multiplicación de $A$ sea $K$–bilineal. En lo que sigue, usaremos el término $K$–álgebra, o incluso álgebra, para indicar que tenemos una estructura de $K$–álgebra sobre un anillo $A$.

[a] Existen nociones de álgebra asociativa no unital, así como de álgebra no asociativa

**Ejemplo 1.6** El anillo de matrices $M_n(K)$, para $K$ un cuerpo, es una $K$–álgebra. El homomorfismo que lo dota de dicha estructura es $\rho : K \to M_n(K)$ dado por $\rho(k) = kI_n$ para todo $k \in K$. ■

**Ejemplo 1.7** El anillo de polinomios $K[X]$ es obviamente un álgebra sobre el cuerpo $K$. ■

**Ejemplo 1.8** Sea $V$ un espacio vectorial sobre un cuerpo $K$. El conjunto

$$\mathrm{End}_K(V) = \{f : V \to V \mid f \text{ es } K\text{-lineal }\}$$

es un subanillo de $\mathrm{End}(V)$. Consideremos la aplicación $h : K \to \mathrm{End}_K(V)$ que asigna a cada $k \in K$ la homotecia $h(k) : V \to V$, definido por $h(k)(v) = kv$ para todo $v \in K$. Es fácil comprobar que $h$ está bien definida y que es un homomorfismo de anillos. Además, si $T : V \to V$ es $K$–lineal y $k \in K$, tenemos que $T \circ h(k) = h(k) \circ T$, luego $Im(h) \subseteq Z(\mathrm{End}_K(V))$. Así, $\mathrm{End}_K(V)$ es una $K$–álgebra. ■

■ **Ejercicio 1.3** Comprobar todas las afirmaciones hechas en el Ejemplo 1.8.

Discutamos ahora la noción de módulo sobre un álgebra. Previamente, declaremos cuáles son los homomorfismos adecuados entre álgebras.

**Definición 1.2.2** Sean $A$ y $B$ álgebras sobre un cuerpo $K$. Una aplicación $\phi : A \to B$ se dirá un *homomorfismo de álgebras* si es tanto homomorfismo de anillos como de $K$–espacios vectoriales. Un subanillo de $B$ que también es $K$–subespacio vectorial se dirá ser una *subálgebra* de $B$. La aplicación inclusión de la subálgebra en el álgebra es un homomorfismo de álgebras.

■ **Ejercicio 1.4** Supongamos que $A$ y $B$ son $K$–álgebras con morfismos de estructura $\rho_A : K \to A$ y $\rho_B : K \to B$. Sea $\phi : A \to B$ un homomorfismo de anillos. Demostrar que $\phi$ es homomorfismo de $K$–álgebras si, y sólo si, $\phi \circ \rho_A = \rho_B$.

Veamos seguidamente que los módulos sobre un álgebra han de ser espacios vectoriales.

**Proposición 1.2.3** Sea $A$ una $K$–álgebra y $M$ un $A$–módulo. Existe una única estructura de $K$–espacio vectorial sobre $M$ tal que el homomorfismo de estructura $\varphi : A \to \mathrm{End}(M)$ verifica que $Im(\varphi) \subseteq \mathrm{End}_K(M)$ y su co-restricción $\varphi : A \to \mathrm{End}_K(M)$ es un homomorfismo de $K$–álgebras.

*Demostración.* Sea $\rho : K \to A$ el homomorfismo de anillos que dota a $A$ de estructura de $K$–álgebra. Entonces $M$ es un $K$–espacio vectorial con homomorfismo de estructura $\varphi \circ \rho : K \to \mathrm{End}(M)$. Queremos ver que $\varphi(a)$ es $K$–lineal para cada $a \in A$. Tomemos $k \in K$ y $m \in M$ y calculemos

$$\begin{aligned}\varphi(a)(km) &= \varphi(a)(\varphi(\rho(k))(m)) = (\varphi(a) \circ \varphi(\rho(k)))(m) = \varphi(a\rho(k))(m) \\ &= \varphi(\rho(k)a)(m) = (\varphi(\rho(k)) \circ \varphi(a))(m) = \varphi(\rho(k))(\varphi(a)(m)) = k\varphi(a)(m).\end{aligned}$$

Por tanto, $Im(\varphi) \subseteq \mathrm{End}_K(M)$.

Ahora, $\mathrm{End}_K(M)$ es una $K$–álgebra con homomorfismo $h : K \to \mathrm{End}_K(M)$ descrito en el Ejemplo 1.8. Pero, dados $k \in K$ y $m \in M$, tenemos que

$$h(k)(m) = km = (\varphi \circ \rho)(k)(m),$$

luego $h = \varphi \circ \rho$. En virtud del Ejercicio 1.4, $\varphi$ es un homomorfismo de $K$–álgebras.

Para demostrar la unicidad, supongamos que $M$ tiene otra estructura de $K$–espacio vectorial, cuya acción denotaremos por $\cdot$, tal que $\varphi : A \to \mathrm{End}_K(M)$ es un homomorfismo de $K$–álgebras. Si $h' : K \to \mathrm{End}_K(M)$ denota ahora la estructura de $K$–álgebra con esa "nueva" estructura de $K$–espacio vectorial, entonces, para $k \in K$, $m \in M$,

$$k \cdot m = h'(k)(m) = (\varphi \circ \rho)(k)(m) = km,$$

donde hemos usado el Ejemplo 1.8 y el Ejercicio 1.4. ■

**Convenciones finales.** Si $A$ es una $K$–álgebra no trivial, entonces el homomorfismo de anillos $\rho : K \to Z(A)$ que le da estructura es necesariamente inyectivo, ya que su núcleo ha de ser un ideal de $K$ que no es el total ($\rho(1_K) = 1_A \neq 0$). Por tanto, $K$ es isomorfo como anillo a $Im(\rho)$, que es un subanillo de $Z(A)$. Es usual identificar $K$ con su imagen en $Z(A)$ y considerar que $K$ es un subanillo de $Z(A)$. Esta identificación es lícita siempre que se sea consciente de ella. El Ejemplo 1.9 sugiere las limitaciones de esta identificación.

**Ejemplo 1.9** Si $K$ es un cuerpo, entonces $id_K : K \to K$ proporciona obviamente una estructura de $K$–álgebra sobre $K$. Pero cualquier otro automorfismo de cuerpos $\sigma : K \to K$ da una estructura de $K$–álgebra distinta sobre $K$. Por ejemplo, la conjugación $\overline{(\,)} : \mathbb{C} \to \mathbb{C}$ da una estructura de $\mathbb{C}$–álgebra "rara" sobre $\mathbb{C}$. También la estructura de $\mathbb{C}$–espacio vectorial correspondiente sobre $\mathbb{C}$ es inusual. ■

■ **Ejercicio 1.5** Sea $A$ un espacio vectorial sobre un cuerpo $K$, y fijemos esta estructura. La acción de un escalar de $K$ sobre un vector de $A$ se denotará por yuxtaposición. Demostrar que dar una estructura de $K$–álgebra asociativa unital sobre $A$ es equivalente a dar una multiplicación asociativa $* : A \times A \to A$ y $K$–bilineal junto con una aplicación $K$–lineal $\eta : K \to A$ tal que $\eta(k) * a = ka = a * \eta(k)$ para todo $k \in K, a \in A$.

## 1.3 La representación regular. Unidades y divisores de cero.

Sea $A$ un álgebra sobre un cuerpo $K$. La tradición, avalada matemáticamente por la Proposición 1.2.3, llama a un $A$–módulo $M$ *representación de $A$ con espacio de representación $M$*. Un caso especial es la representación dada por el módulo regular, llamada *representación regular de $A$*. Hagámosla explícita en la siguiente proposición.

**Proposición 1.3.1** Sea $A$ cualquier $K$–álgebra. La aplicación $\lambda : A \to \mathrm{End}_K(A)$ que asigna a cada $a \in A$ la aplicación $\lambda(a) : A \to A$ definida por $\lambda(a)(b) = ab$ para todo $b \in A$ es un homomorfismo inyectivo de $K$–álgebras. Como consecuencia, $A$ es isomorfa a una $K$–subálgebra de $\mathrm{End}_K(A)$.

*Demostración.* Aplicamos la Proposición 1.2.3 al $A$–módulo regular $A$. Así, estamos considerando la estructura de $K$–espacio vectorial sobre $A$ dada por $ka = (\lambda \circ \rho)(k)(a) = \rho(k)a$ para todo $k \in K$, $a \in A$, donde $\rho : K \to A$ es el homomorfismo que da estructura de $K$–álgebra a $A$. Observemos que ésta es también la estructura de $K$–espacio vectorial de $A$ por restricción de escalares. Que $\lambda$ es inyectivo es consecuencia de que si $a \in \ker(\lambda)$, entonces $0 = \lambda(a)(1) = a$, por lo que $\ker(\lambda) = \{0\}$. ■

**Endomorfismos y matrices.** Si $V$ es un $K$-espacio vectorial de dimensión finita $n$, y $\mathscr{B}$ es una base de $V$, entonces sabemos[2] que la aplicación

$$M_{\mathscr{B}} : \mathrm{End}_K(V) \to M_n(K)$$

que asigna a cada aplicación lineal $f : V \to V$ su matriz $M_{\mathscr{B}}(f)$ con respecto de la base $\mathscr{B}$ es un isomorfismo de $K$–álgebras. Subrayemos que, si $\mathbf{x}$ es el vector columna de coordenadas de $v \in V$ con respecto de $\mathscr{B}$, e $\mathbf{y}$ es el de $f(v)$, entonces $\mathbf{y} = M_{\mathscr{B}}(f)\mathbf{x}$.

En vista de 1.3, la Proposición 1.3.1 tiene la siguiente consecuencia.

**Corolario 1.3.2** Toda $K$–álgebra de dimensión finita como $K$–espacio vectorial es isomorfa a una subálgebra de un álgebra de matrices con coeficientes en $K$.

**Ejemplo 1.10** Consideremos el cuerpo $\mathbb{C}$ de los números complejos como $\mathbb{R}$–álgebra. Si tomamos la base $\mathscr{B} = \{1, i\}$ de $\mathbb{C}$ como espacio vectorial real, entonces el homomorfismo inyectivo de $\mathbb{R}$–álgebras $m = M_{\mathscr{B}} \circ \lambda : \mathbb{C} \to M_2(\mathbb{R})$ obtenido a patir del $\mathbb{C}$—módulo regular $\lambda : \mathbb{C} \to \mathrm{End}_{\mathbb{R}}(\mathbb{C})$ está definido por $m(a+bi) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$, para $a + bi \in \mathbb{C}$. Así, $\mathbb{C}$ es isomorfo a la $\mathbb{R}$–subálgebra

$$\{\begin{pmatrix} a & -b \\ b & a \end{pmatrix} : a, b \in \mathbb{R}\} \subseteq M_2(\mathbb{R})$$

■

**Ejemplo 1.11** Sea $K$ un cuerpo. El anillo de polinomios $K[X]$ es una $K$–álgebra. Si ahora tomamos un ideal no nulo $I$ de $K[X]$, tenemos la $K$–álgebra cociente $A = K[X]/I$. Sabemos[a] que existe un único polinomio mónico $p(X) \in K[X]$ que genera el ideal $I$,

[2] Se trata de interpretar algunos hechos básicos del Álgebra Lineal.

escribimos $I = \langle p(X) \rangle$. Llamamos $n$ al grado de $f(X)$, y suponemos que $n > 0$ (esto es, $p(x) \neq 1$). Entonces[b] $\mathscr{B} = \{1+I, x+I, \ldots, x^{n-1}+I\}$ es una base de $A$ como $K$–espacio vectorial y, por tanto, $\dim_K A = n$. Escribamos

$$p(X) = p_0 + p_1 X + \cdots + p_{n-1}X^{n-1} + X^n.$$

Bien, la matriz de $M_n(K)$ que representa al endomorfismo $\lambda(x+I)$ con respecto de la base $\mathscr{B}$ es

$$\tilde{N}(p(X)) = \begin{pmatrix} 0 & \cdots & 0 & -p_0 \\ 1 & \cdots & 0 & -p_1 \\ \vdots & & \vdots & \vdots \\ 0 & \cdots & 1 & -p_{n-1} \end{pmatrix},$$

que se llama *matriz compañera* del polinomio $p(X)$. Escribámosla abreviadamente como $\tilde{N}(p)$. Entonces el álgebra $A$ es isomorfa a la subálgebra

$$\{a_0 I + a_1 \tilde{N}(p) + \cdots + a_{n-1}\tilde{N}(p)^{n-1} : a_0, a_1, \ldots, a_{n-1} \in K\} \subseteq M_n(K)$$

■

[a] De hecho, es el mónico de grado mínimo en $I$.
[b] Esto viene de la división con resto de polinomios.

■ **Ejercicio 1.6** * Comprobar todas las afirmaciones hechas en el Ejemplo 1.11.

■ **Ejercicio 1.7** ** Sea $K$ un cuerpo. Dar la lista, salvo isomorfismos, de todas las $K$–álgebras asociativas unitales de dimensión 2.

■ **Ejercicio 1.8** Expresar el cuerpo $\mathbb{Q}(\sqrt{2})$ como una $\mathbb{Q}$–subálgebra de un álgebra de matrices sobre $\mathbb{Q}$.

**Definición 1.3.1** Sea $A$ un álgebra sobre $K$. El álgebra *opuesta* de $A$ es la propia $A$, en tanto que $K$–espacio vectorial, pero con la multplicación dada por $a \cdot b := ba$ para todo $a, b \in A$. Se denota por $A^{op}$.

**Definición 1.3.2** Sea $a$ un elemento no nulo de una $K$–álgebra $A$. Diremos que $a$ es una *unidad* si existe $a^{-1} \in A$ tal que $aa^{-1} = 1 = a^{-1}a$. Es fácil ver que, si existe, el elemento $a^{-1}$ está determinado de manera única por $a$, y se llama *inverso* de $a$. El conjunto de todas las unidades de $A$ es un grupo con la operación multiplicación y se denota por $U(A)$. Es claro que $U(A) = U(A^{op})$, como conjuntos. Como grupos, son isomorfos. ¿Ves el isomorfismo?

**Lema 1.3.3** Sea $A$ una $K$–álgebra de dimensión finita y $\lambda : A \to \mathrm{End}_K(A)$ la representación regular de $A$. Para $a \in A$, las siguientes afirmaciones son equivalentes.

1. $\lambda(a)$ es inyectiva,
2. existe $b \in A$ tal que $ab = 1$,
3. $a \in U(A)$.

*Demostración.* (1) $\Rightarrow$ (2). Si $\lambda(a) : A \to A$ es inyectiva, puesto que $A$ es un $K$–espacio vectorial de dimensión finita, entonces $\lambda(a)$ es biyectiva. Así, existe $b \in A$ tal que $\lambda(a)(b) = 1$, esto es, $ab = 1$.

(2) $\Rightarrow$ (3). Veamos que $\lambda(b)$ es inyectiva. En efecto, si $c \in A$ es tal que $\lambda(b)(c) = 0$, entonces $bc = 0$, por lo que $c = abc = 0$. Como antes, $\lambda(b)$ ha de ser biyectiva, por lo que existe $a' \in A$ tal que $\lambda(b)(a') = 1$. Esto es, $ba' = 1$. Ahora, $a' = aba' = a$, lo que muestra que $ba = 1$. Por tanto, $a \in U(A)$.

(3) $\Rightarrow$ (1). Si $a \in U(A)$, entonces $\lambda(a)$ es biyectiva, puesto que $\lambda(a^{-1})$ es claramente su inversa para la composición. ■

**Proposición 1.3.4** Sea $a \in A$ un elemento no nulo de un álgebra $A$ de dimensión finita sobre $K$.

1. Las siguientes afirmaciones son equivalentes:
   *a*) $a \in U(A)$;
   *b*) existe $b \in A$ tal que $ab = 1$;
   *c*) existe $b \in A$ tal que $ba = 1$.
2. Las siguientes afirmaciones son equivalentes:
   *a*) $a \notin U(A)$;
   *b*) existe $b \in A$ no nulo tal que $ab = 0$;
   *c*) existe $c \in A$ no nulo tal que $ca = 0$.

*Demostración.* 1. La equivalencia entre 1*a* y 1*b* la da el Lema 1.3.3. Este mismo lema, aplicado a $A^{op}$, da cuenta de la equivalencia entre 1*a* y 1*c*.

2. Observemos que 2*b* es equivalente a afirmar que $\lambda(a)$ no es inyectiva. Por tanto, el Lema 1.3.3 implica la equivalencia entre 2*a* y 2*b*. Aplicando el Lema 1.3.3 para $A^{op}$ obtenemos también la equivalencia entre 2*c* y 2*a*. ■

**Definición 1.3.3** Un elemento no nulo $a$ de un álgebra $A$ se dice ser un *divisor de cero* si satisface alguna de las condiciones 2*b* o 2*c* de la Proposición 1.3.4. Según dicha proposición, si $A$ es finito-dimensional, entonces un divisor de cero verifica ambas condiciones. Además, todo elemento no nulo de $A$ es o bien una unidad, o bien un divisor de cero.

R Si un álgebra $A$ es de dimensión finita, y tomamos su representación regular $\lambda : A \to \mathrm{End}_K(A)$, entonces podemos usar el determinante para decidir si un elemento $a \in A$ es una unidad. De hecho, $a \in U(A)$ si y sólo si $\lambda(a)$ es un endomorfismo biyectivo, si y sólo si $\det \lambda(a) \neq 0$ (hemos usado la demostración de la Proposición 1.3.4).

■ **Ejercicio 1.9** Sea

$$\mathbb{H} = \{ \begin{pmatrix} \alpha & -\overline{\beta} \\ \beta & \overline{\alpha} \end{pmatrix} : \alpha, \beta \in \mathbb{C} \}$$

1. Demostrar que $\mathbb{H}$ es una subálgebra real de $M_2(\mathbb{C})$ y que $Z(\mathbb{H}) = \mathbb{R}$.
2. Demostrar que todo elemento no nulo de $\mathbb{H}$ es una unidad.
3. Demostrar que las matrices

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \mathbf{i} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \mathbf{j} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

forman una base de $\mathbb{H}$ como espacio vectorial real.

4. Comprobar las identidades

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1,\ \mathbf{ij} = \mathbf{k},\ \mathbf{jk} = \mathbf{i},\ \mathbf{ki} = \mathbf{j}$$

El álgebra real $\mathbb{H}$ construida en el Ejercicio 1.9 se llama álgebra de los *cuaterniones de Hamilton.* Es un álgebra de división, de acuerdo con la siguiente definición.

**Definición 1.3.4** Un álgebra $A$ se dice ser un *álgebra de división* si $U(A) = A \setminus \{0\}$. Las álgebras de división conmutativas son los cuerpos.

## 1.4 Módulos: construcciones básicas.

En lo que sigue, $A$ denotará un anillo. El hecho de que $M$ es un $A$–módulo se indicará a veces por la notación ${}_AM$.

■ **Ejercicio 1.10** Dado un $A$–módulo $V$ no nulo, demostrar que

$$Ann_A(V) = \{a \in A : av = 0\ \forall v \in V\}$$

es un ideal de $A$. Dotar a $V$ de estructura de $A/Ann_A(V)$–módulo fiel (es decir, la representación correspondiente es fiel).

**Ejemplo 1.12** A modo de complemento del Ejemplo 1.4, supongamos que $V$ es de dimensión finita como $K$–espacio vectorial. Observemos que

$$Ann_{K[X]}(V) = \operatorname{Ker} e_T.$$

Por el Teorema de Isomorfía para anillos, $K[X]/\operatorname{Ker} e_T$ es isomorfa a un subálgebra del álgebra $\operatorname{End}_K(V)$. Por tanto, $K[X]/\operatorname{Ker} e_T$ es un álgebra de dimensión finita, con lo que $\operatorname{Ker} e_T$ resulta ser un ideal no nulo de $K[X]$, luego ha de estar generado por un polinomio mónico $m(X)$ de grado igual al de la dimensión de $K[X]/\operatorname{Ker} e_T$. Este polinomio $m(X)$ se llama *polinomio mínimo* de $T$, en el sentido de que es el de grado más pequeño contenido en $\operatorname{Ker} e_T$. Obviamente, $m(T) = 0$. Además, $m(X)$ ha de ser un divisor de cualquier otro polinomio $a(X)$ que verifique que $a(T) = 0$. ■

Vamos ahora a exponer algunas construcciones y nociones básicas relacionadas con los módulos. Dada una colección de $A$–módulos $M_1, \ldots, M_n$, podemos considerar el producto cartesiano $M_1 \times \cdots \times M_n$ como $A$–módulo con las operaciones siguientes para $(m_1, \ldots, m_n), (m_1', \ldots, m_n') \in M_1 \times \cdots \times M_n$ y $a \in A$:

$$(m_1, \ldots, m_n) + (m_1', \ldots, m_n') = (m_1 + m_1', \ldots, m_n + m_n'),$$

$$a(m_1, \ldots, m_n) = (am_1, \ldots, am_n)$$

Este módulo se llama *suma directa externa* de los módulos $M_1, \ldots, M_n$, y se suele denotar por $M_1 \oplus \cdots \oplus M_n$. Cuando $M_1 = \cdots = M_n = M$, se usa la notación $M^n$.

Para cada natural $n \geq 1$, consideremos el anillo $M_n(A)$ de matrices cuadradas de orden $n$ con coeficientes en $A$, que es una $K$–álgebra si $A$ lo es. El $A$–módulo $M^n = M \overset{(n)}{\oplus \cdots}$

$\oplus M$ resulta ser un $M_n(A)$–módulo. En efecto, si $C=(c_{ij})\in M_n(A)$ y $(m_1,\dots,m_n)\in M^n$, definimos

$$C\begin{pmatrix} m_1\\ m_2\\ \vdots\\ m_n\end{pmatrix}=\begin{pmatrix} \sum_{j=1}^n c_{1j}m_j\\ \sum_{j=1}^n c_{2j}m_j\\ \vdots\\ \sum_{j=1}^n c_{nj}m_j\end{pmatrix},$$

lo que, como puede comprobarse sin dificultad, dota a $M^n$ de estructura de $M_n(A)$–módulo.

**Teorema 1.4.1 — Teorema de Cayley-Hamilton.** Todo endomorfismo de un espacio vectorial de dimensión finita satisface su ecuación característica.

*Demostración.* Sea $V$ un $K$–espacio vectorial de dimensión finita $n$ y $T:V\to V$ una aplicación lineal. Consideramos $V$ como un $K[X]$–módulo via $T$. Escojamos una base $\{v_1,\dots,v_n\}$ de $V$. Tenemos que

$$T(v_i)=\sum_{j=1}^n a_{ij}v_j$$

para ciertos $a_{ij}\in K$. Consideremos la matriz $C=(a_{ij})$ con coeficientes en $K$, y la matriz

$$\Delta=XI_n-C=\begin{pmatrix} X-a_{11} & -a_{12} & \cdots & -a_{1n}\\ -a_{21} & X-a_{22} & \cdots & -a_{2n}\\ \vdots & \vdots & & \vdots\\ -a_{n1} & -a_{n2} & \cdots & X-a_{nn}\end{pmatrix}\in M_n(K[X]).$$

Si llamamos $\widetilde{\Delta}$ a su matriz adjunta, entonces tenemos

$$\widetilde{\Delta}\Delta=det(\Delta)I_n=\begin{pmatrix} det(\Delta) & 0 & \cdots & 0\\ 0 & det(\Delta) & \cdots & 0\\ \vdots & \vdots & & \vdots\\ 0 & 0 & \cdots & det(\Delta)\end{pmatrix}\tag{1.2}$$

Por otra parte, usando la estructura de $M_n(K[X])$–módulo de $V^n$, tenemos

$$\Delta\begin{pmatrix} v_1\\ v_2\\ \vdots\\ v_n\end{pmatrix}=\begin{pmatrix} T(v_1)-\sum_{j=1}^n a_{1j}v_j\\ T(v_2)-\sum_{j=1}^n a_{2j}v_j\\ \vdots\\ T(v_n)-\sum_{j=1}^n a_{nj}v_j\end{pmatrix}=\begin{pmatrix} 0\\ 0\\ \vdots\\ 0\end{pmatrix}\tag{1.3}$$

De aquí deducimos, multiplicando en (1.3) por $\widetilde{\Delta}$, y usando (1.2), que

$$\begin{pmatrix} det(\Delta)v_1\\ det(\Delta)v_2\\ \vdots\\ det(\Delta)v_n\end{pmatrix}=\begin{pmatrix} 0\\ 0\\ \vdots\\ 0\end{pmatrix},$$

de donde $det(\Delta)v_i = 0$ para $i = 1,\dots,n$. Como $v_1,\dots,v_n$ es una base de $V$, deducimos que $det(\Delta)v = 0$ para todo $v \in T$. Ahora bien, $det(\Delta)$ es un polinomio[3] mónico de grado $n$ en $K[X]$, y como la acción de $X$ sobre los elementos de $V$ es aplicar $T$, obtenemos que $T$ satisface la ecuación polinómica

$$det(\Delta)(T) = 0,$$

llamada *ecuación característica* de $T$. ■

Por otra parte, dado un $A$–módulo $M$, diremos que un subconjunto $N$ de $M$ es un *submódulo* de $M$ si es un subgrupo aditivo y $am \in N$ para todo $m \in N$ y todo $a \in A$. Observemos que, si $A$ es una $K$–álgebra, cada submódulo de $M$ es un $K$–subespacio vectorial de $M$. Los submódulos de $A$ se llaman *ideales a izquierda* de $A$.

Si denotamos por $\mathscr{L}(M)$ a la familia de todos los submódulos de $M$, es fácil ver que la intersección de cualquier familia en $\mathscr{L}(M)$ vuelve a ser un submódulo de $M$. Esto permite deducir que, dado cualquier subconjunto $S \subseteq M$, existe el menor submódulo de $M$ que contiene a $S$, denotado por $AS$, y llamado *submódulo* de $M$ generado por $S$.

**Definición 1.4.1** Diremos que un $A$–módulo $M$ es *finitamente generado* si existe $X \subseteq M$ finito tal que $M = AX$. Si $X = \{m_1,\dots,m_n\}$, esto significa que, para cada $m \in M$, existen $a_1,\dots,a_n \in A$ tales que $m = a_1m_1 + \cdots + a_nm_n$. Diremos que $M$ es *cíclico* si admite un conjunto generador de cardinal 1. Esto es, si $M = A\{m\}$ para algún $m \in M$. Se usa la notación abreviada $M = Am$.

**Definición 1.4.2** Dados submódulos $N_1,\dots,N_m$ de un módulo $M$, su *suma*, denotada por $N_1 + \cdots + N_m$, es el menor submódulo de $M$ que contiene a $N_1 \cup \cdots \cup N_m$.

**Lema 1.4.2** Sea $M$ un $A$–módulo.

1. Dados submódulos $N_1,\dots,N_m$ de $M$, tenemos que
$$N_1 + \cdots + N_m = \{n_1 + \cdots + n_m : n_i \in N_i\}$$
2. Dado $X = \{m_1,\dots,m_n\} \subseteq M$, tenemos que $AX = Am_1 + \cdots + Am_n$.

*Demostración.* Se propone como ejercicio. ■

▪ **Ejercicio 1.11** Dar una demostración del Lema 1.4.2.

**Definición 1.4.3** Sean $M,N$ módulos sobre un anillo $A$. Diremos que un homomorfismo de grupos aditivos $f : M \to N$ es un *homomorfismo de $A$–módulos* si $f(am) = af(m)$ para todo $a \in A$, y todo $m \in M$. Diremos, a veces, que $f$ es $A$–lineal.

**Lema 1.4.3** Sea $L$ un submódulo de un $A$–módulo $M$. Entonces el grupo aditivo cociente $M/L$ tiene una estructura de $A$–módulo dada por $a(m+L) = am+L$ para $a \in A$, $m+L \in M/L$. Recordemos que la suma de $M/L$ viene dada por la regla $(m+L)+(m'+L) = m+m'+L$.

*Demostración.* La construcción del grupo cociente $M/L$ se supone conocida de cursos anteriores (ver [1, Proposición 2.40]). Demostrar que la acción propuesta para convertirlo en $A$–módulo funciona correctamente es una rutina fácil. ■

[3] Sí, es el polinomio característico

**Proposición 1.4.4 — Primer Teorema de Isomorfía para módulos.** Sea $f : M \to N$ un homomorfismo de módulos. Entonces $\operatorname{Ker} f$ es un submódulo de $M$ e $\operatorname{Im} f$ es un submódulo de $N$. Además, la aplicación canónica

$$\widetilde{f} : M/\operatorname{Ker} f \to \operatorname{Im} f$$

dada por $\widetilde{f}(m + \operatorname{Ker} f) = f(m)$ para todo $m + \operatorname{Ker} f \in M/\operatorname{Ker} f$ es un isomorfismo de módulos.

*Demostración.* Suponiendo que esta construcción es conocida previamente en el ámbito de grupos aditivos (ver [1, Teorema 2.58]), sólo habría que comprobar que la acción de $A$ sobre $M/L$ está bien definida, y que $\widetilde{f}$ es $A$–lineal. Ambas tareas son fáciles. ■

**Ejemplo 1.13** Supongamos que $M$ es un $A$–módulo y $m \in M$. Consideremos la aplicación $f : A \to M$ definida por $f(a) = am$, para todo $a \in A$. Es fácil ver que $f$ es un homomorfismo de $A$–módulos. Si aplicamos la Proposición 1.4.4 a $f$, tenemos que $\operatorname{Im} f = Am$. Por otra parte,

$$\operatorname{Ker} f = \{a \in A : am = 0\} =: \operatorname{ann}_A(m),$$

ideal a izquierda de $A$ llamado *anulador* de $m$. Tenemos, pues, un isomorfismo de $A$–módulos

$$Am \cong A/\operatorname{ann}_A(m).$$

▪

**Ejemplo 1.14** Consideremos el $A$–módulo $A^n$ y denotemos, para cada $i = 1, \ldots, n$, por $\mathbf{e}_i$ la $i$–tupla de $A^n$ que tiene un 1 en la componente $i$–ésima, y 0 en las demás. El conjunto $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ es un sistema de generadores de $A^n$.

Observemos que, además, si $\mathbf{a} \in A^n$, entonces los coeficientes $a_1, \ldots, a_n \in A$ que permiten escribir $\mathbf{a} = \sum_{i=1}^n a_i \mathbf{e}_i$ son obviamente únicos. Esto permite que, dado un $A$–módulo $M$ y $m_1, \ldots, m_n \in M$, la aplicación $f : A^n \to M$ dada por $f(\sum_{i=1}^n a_i \mathbf{e}_i) = \sum_{i=1}^n a_i m_i$ esté bien definida. Es un interesante ejercicio comprobar que esta aplicación $f$ es, de hecho, un homomorfismo de $A$–módulos. Observemos que $f$ está determinada completamente por las condiciones $f(\mathbf{e}_i) = m_i$ para $i = 1, \ldots, n$. ▪

**Definición 1.4.4** Un conjunto de generadores $\{m_1, \ldots, m_n\}$ de un $A$–módulo se dice ser una *base* de $M$ si cada elemento $m \in M$ se escribe de manera única como $m = \sum_{i=1}^n a_i m_i$ con $a_1, \ldots, a_n \in A$. Si $M$ admite una base, diremos que se *libre*. Un ejemplo de módulo libre es $A^n$.

▪ **Ejercicio 1.12** Demostrar que un conjunto de generadores $\{m_i : i \in I\}$ de un módulo ${}_AM$ es una base si, y sólo si, la igualdad $\sum_{i \in I} r_i m_i = 0$ para $r_i \in A$ implica $r_i = 0$ para todo $i \in I$. Dar un ejemplo de un módulo no nulo finitamente generado que no sea libre.

**Proposición 1.4.5** Sea $M$ un módulo y $B \subseteq M$ un subconjunto no vacío finito. Entonces $B$ es una base de $M$ si, y sólo si, para cualquier módulo $N$ y cualquier aplicación $f : B \to N$ existe un único homomorfismo de $A$–módulos $\overline{f} : M \to N$ tal que $\overline{f}_{|B} = f$.

*Demostración.* Cada elemento $m \in M$ determina de manera única coeficientes $a_i \in A$ tales que $m = \sum_{i\in B} a_i m_i$. Esto permite definir una aplicación $\overline{f}(m) = \sum_{i\in B} a_i f(m_i)$. Para demostrar que $\overline{f}$ preserva sumas, observemos que si $m = \sum_{i\in B} a_i m_i, n = \sum_{i\in B} b_i m_i$, entonces

$$\overline{f}(m+n) = \overline{f}(\sum_{i\in B}(a_i+b_i)m_i) = \sum_{i\in B}(a_i+b_i)f(m_i) =$$
$$\sum_{i\in B} a_i f(m_i) + \sum_{i\in B} b_i f(m_i) = \overline{f}(m) + \overline{f}(n)$$

Análogamente, $\overline{f}(am) = a\overline{f}(m)$ para todo $a \in A$, con lo que tenemos que $\overline{f}$ es un homomorfismo de $A$–módulos. La unicidad es clara. ■

**Corolario 1.4.6** Sea $M$ un $A$–módulo.
1. Si $M$ admite un conjunto de generadores $\{m_1,\dots,m_n\}$, entonces $M \cong A^n/L$ para cierto submódulo $L$ de $A^n$.
2. Si $M$ es libre con base $\{m_1,\dots,m_n\}$, entonces $M$ es isomorfo a $A^n$.

*Demostración.* Dados generadores $m_1,\dots,m_n$ de $M$, tomamos el único homomorfismo de $A$–módulos $f : A^n \to M$ tal que $f(\mathbf{e}_i) = m_i$ para $i = 1,\dots,n$. Obviamente, $f$ es sobreyectiva por lo que, si ponemos $L = \operatorname{Ker} f$, obtenemos $M \cong A^n/L$, por la Proposición 1.4.4. Si $m_1,\dots,m_n$ es una base de $M$, entonces $L = 0$ por el Ejercicio 1.12. ■

▪ **Ejercicio 1.13** Para cada $A$–módulo $M$, demostrar que el conjunto $\operatorname{End}_A(M)$ cuyos elementos son los endomorfismos[4] de $A$–módulos de $M$, es un subanillo de $\operatorname{End}(M)$. Demostrar que si, además, $M$ es libre con base $\{m_1,\dots,m_n\}$, entonces $\operatorname{End}_A(M)^{op}$ es isomorfo, como anillo, a $M_n(A)$. Discutir qué ocurre cuando $A$ es un álgebra sobre un cuerpo $K$.

▪ **Ejercicio 1.14** Sea $M$ un módulo sobre un álgebra finito-dimensional $A$. Demostrar que si $M$ admite bases, como $A$–módulo, $\{m_1,\dots,m_r\}$ y $\{n_1,\dots,n_t\}$, entonces $r = t$. (Nota: Se dice entonces que el módulo $M$ es *libre de rango* $r$).

Vamos ahora a deducir algunas consecuencias más del primer Teorema de isomorfía, que son conocidos como segundo y tercer teoremas de isomorfía.

**Proposición 1.4.7 — Segundo Teorema de Isomorfía.** Sea $M$ un módulo y $L,N \in \mathscr{L}(M)$. Entonces existe un isomorfismo de módulos

$$\frac{L+N}{L} \cong \frac{N}{L\cap N}$$

*Demostración.* Consideremos el homomorfismo de módulos

$$f : N \to \frac{L+N}{L}, \qquad n \mapsto f(n) = n+L.$$

Observemos que si $l+n \in L+N$, con $l \in L$, $n \in N$, entonces $(l+n)+L = n+L$, por lo que $f$ es sobreyectiva. Además, si $n \in \operatorname{Ker} f$, entonces $0+L = f(n) = n+L$, con lo que $n \in L$. Esto es, $\operatorname{Ker} f = N \cap L$. Para terminar, aplicamos el primer Teorema de Isomorfía. ■

[4] Un endomorfismo de $M$ es un homomorfismo $M \to M$.

**Proposición 1.4.8 — Tercer Teorema de Isomorfía.** Sea $M$ un módulo, y $L \subseteq N \in \mathscr{L}(M)$. Entonces $N/L$ es un submódulo de $M/L$ y existe un ismorfismo de módulos

$$\frac{M/L}{N/L} \cong \frac{M}{N}.$$

Además, el conjunto $[L,M]$ de los submódulos de $M$ que contienen a $L$ es isomorfo, como conjunto ordenado por la inclusión, a $\mathscr{L}(M/L)$.

*Demostración.* Consideremos la aplicación

$$f : M/L \to M/N, \qquad m+L \mapsto m+N,$$

que está bien definida ya que $L \subseteq N$. Además, $f$ es obviamente sobreyectiva. Por otra parte, $0+N = f(m+L)$ si, y sólo si, $m \in N$, esto es, $\operatorname{Ker} f = N/L$. Ahora aplicamos el Primer Teorema de Isomorfía.

Para la segunda afirmación, consideramos la aplicación $\varphi : [L,M] \to \mathscr{L}(M/L)$ dada por $N \mapsto N/L$ y demostramos que es biyectiva. Veamos que es inyectiva: supongamos que $X,Y \in [L,M]$ son tales que $X/L = Y/L$. Si $x \in X$, entonces $x+L \in Y/L$. luego $x+L = y+L$ para cierto $y \in Y$. Por tanto, $x-y \in L$, de donde $x \in y+L \subseteq Y$. Esto prueba que $X \subseteq Y$. La inclusión recíproca se deduce igual. Para ver que la aplicación es sobreyectiva, tomemos $Z \in \mathscr{L}(M/L)$ y definamos $X = \{m \in M : m+L \in Z\}$. Es fácil comprobar que $X \in [L,M]$ y que $X/L = Z$. ■

## 1.5 Módulos simples. Teorema de Jordan-Hölder

Los módulos cuya estructura, en tanto que tales, es más sencilla son los módulos simples, de acuerdo con la siguiente definición.

**Definición 1.5.1** Un módulo $M$ se dice *simple* si $\mathscr{L}(M)$ tiene, exactamente, dos elementos. Esto es, $M \neq \{0\}$ y los submódulos de $M$ son, exactamente, $\{0\}$ y $M$.

R Si $M$ es un módulo no nulo y $N \subseteq M$ es un submódulo, entonces se deduce de la Proposición 1.4.8 que $M/N$ es simple si, y sólo si, $N$ es maximal en el conjunto ordenado por inclusión de todos los submódulos estrictamente contenidos en $M$. Un tal submódulo se dice, simplemente, *maximal*.

▪ **Ejercicio 1.15** Sea $\theta \in \mathbb{R}$ y $T_\theta : \mathbb{R}^2 \to \mathbb{R}^2$ el endomorfismo que gira los vectores un ángulo $\theta$ en sentido contrario de las agujas del reloj. Consideremos la correspondiente estructura de $\mathbb{R}[X]$–módulo definida por $T_\theta$ sobre $\mathbb{R}^2$. Llamamos a este módulo $V_\theta$. Discutir para qué valores de $\theta$ es $V_\theta$ simple.

▪ **Ejercicio 1.16** Siguiendo la notación del Ejercicio 1.15, ¿Para qué valores $\theta, \theta'$ son los $\mathbb{R}[X]$–módulos $V_\theta$ y $V_{\theta'}$ isomorfos?

▪ **Ejercicio 1.17** Sea $M$ un $A$–módulo. Demostrar que $M$ es simple si, y sólo si, $M = Am$ para todo $0 \neq m \in M$.

▪ **Ejercicio 1.18** Sea $A$ un anillo. Demostrar que $A$ es un anillo de división si, y sólo si, $A$ es un $A$–módulo simple.

■ **Ejercicio 1.19** Demostrar que un $A$–módulo es simple si, y sólo si, es isomorfo a $A/I$, donde $I$ es un submódulo maximal de $A$ (también llamados ideales a izquierda maximales). Deducir cuáles son las dimensiones posibles, como $K$–espacios vectoriales, de los $K[X]$–módulos simples, para $K = \mathbb{R}$ y $\mathbb{C}$. ¿Qué pasa con $K = \mathbb{Q}$?

**Definición 1.5.2** Sea $M$ un módulo. Diremos que una cadena de submódulos $0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$ es una *serie de composición* de $M$ si cada $M_{i-1}$ es maximal en $M_i$, con $i = 1, \ldots, n$.

**Teorema 1.5.1 — de Jordan-Hölder.** Sea $A$ una $K$–álgebra y $M$ un $A$–módulo no nulo de dimensión finita como $K$–espacio vectorial. Entonces $M$ admite, al menos, una serie de composición. Además, dadas dos series de composición

$$\{0\} = M_0 \subset M_1 \subset \cdots \subset M_n = M$$

y

$$\{0\} = N_0 \subset N_1 \subset \cdots \subset N_m = M$$

de $M$, se tiene que $n = m$ y existe una permutación $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$ tal que $M_i/M_{i-1} \cong N_{\sigma(i)}/N_{\sigma(i)-1}$ para todo $i = 1, \ldots, n$.

*Demostración.* Para la existencia, podemos argumentar por inducción sobre la dimensión como $K$–espacio vectorial de $M$. Tengamos en cuenta que cada submódulo es un subespacio vectorial.

Si $dim_K(M) = 1$, entonces $M$ es simple, y $\{0\} \subset M$ es una serie de composición. Si $dim_K(M) > 1$, aún puede ocurrir que $M$ sea simple, y tenemos, como antes, una serie de composición. Si $M$ no es simple, entonces existe un submódulo maximal $N$ de $M$. Por ejemplo, $N$ podría tomarse de dimensión máxima entre los submódulos de $M$ estrictamente contenidos en $M$. Como $dim_K(N) < dim_K(M)$, por hipótesis de inducción, $N$ admite una serie de composición, con lo que, claramente, $M$ admite una serie de composición cuyo último "eslabón" es la inclusión $N \subset M$.

Para la afirmación que compara las dos series de composición, argumentamos por inducción sobre $n$. Si $n = 1$, entonces $M = M_1$ es simple y, por tanto, $m = 1$, y $N_1 = M = M_1$. Supongamos que $n > 1$. Entonces $M$ no es simple y, por tanto, $m > 1$. Distinguimos dos casos.

**Caso 1.** Si $M_{n-1} = N_{m-1}$, tenemos la situación descrita por el diagrama de la izquierda en la Figura 1.1. Por hipótesis de inducción, tenemos que $n - 1 = m - 1$ y existe una permutación $\sigma : \{1, \ldots, n-1\} \to \{1, \ldots, n-1\}$ tal que $M_i/M_{i-1} \cong N_{\sigma(i)}/N_{\sigma(i)-1}$ para $i = 1, \ldots, n-1$. Tenemos, pues, que $n = m$ y $\sigma$ se extiende por $\sigma(n) = n$.

**Caso 2.** Si $M_{n-1} \neq N_{m-1}$ entonces $M_{n-1} + N_{m-1} = M$, puesto que $M_{n-1}$ y $N_{m-1}$ son submódulos maximales de $M$.

El submódulo $N_{m-1} \cap M_{n-1}$ de $M$ admite, por ser de dimensión finita, una serie de composición

$$\{0\} = L_0 \subset L_1 \subset \cdots \subset L_k = N_{m-1} \cap M_{n-1}.$$

El diagrama que describe esta situación es el de la Figura 1.1 (derecha). El segundo teorema

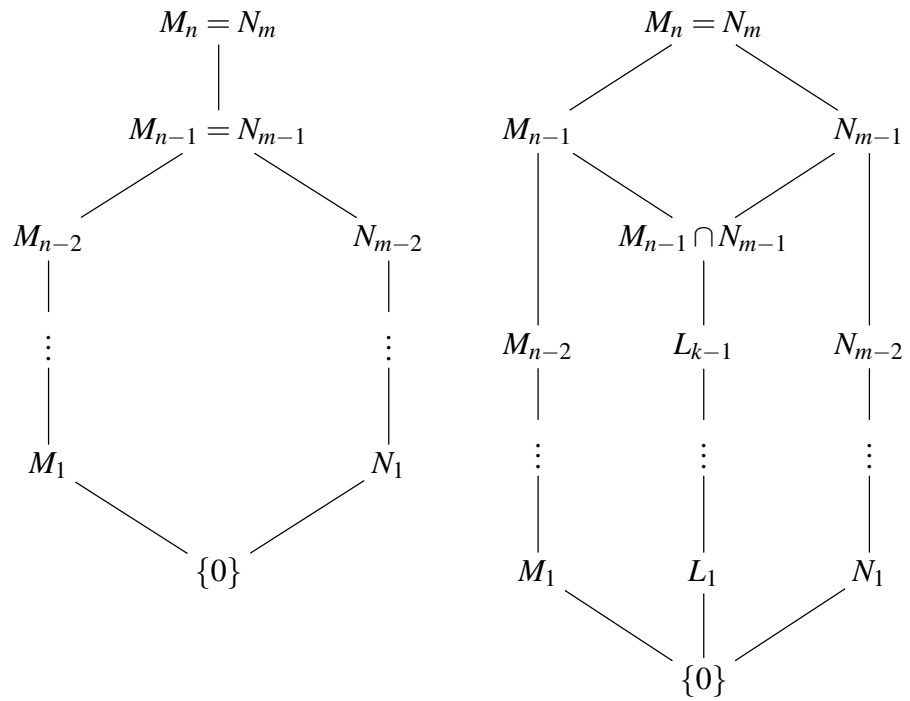


Figura 1.1: Diagramas de Hasse que describen el Caso 1 (izquierda) y el Caso 2 (derecha).

de isomorfía nos da que

$$\frac{M}{N_{m-1}} = \frac{M_{n-1}+N_{m-1}}{N_{m-1}} \cong \frac{M_{n-1}}{N_{m-1}\cap M_{n-1}}$$

y, puesto que $M/N_{m-1}$ es simple, obtenemos una serie de composición

$$\{0\} = L_0 \subset L_1 \subset \cdots \subset L_k \subset M_{n-1}$$

de $M_{n-1}$. Por hipótesis de inducción, $k+1 = n-1$, y existe una permutación $\tau : \{1,\ldots,n-1\} \to \{1,\ldots,n-1\}$ tal que $L_i/L_{i-1} \cong M_{\tau(i)}/M_{\tau(i)-1}$ para $i = 1,\ldots,n-2$ y $M_{n-1}/L_{n-2} \cong M_{\tau(n-1)}/M_{\tau(n-1)-1}$. Ahora bien,

$$\{0\} = L_0 \subset L_1 \subset \cdots \subset L_{n-2} \subset N_{m-1}$$

resulta ser una serie de composición de longitud $n-1$ de $N_{m-1}$, ya que

$$\frac{M}{M_{n-1}} = \frac{N_{m-1}+M_{n-1}}{M_{n-1}} = \frac{N_{m-1}}{N_{m-1}\cap M_{n-1}},$$

por lo que podemos aplicar de nuevo la hipótesis de inducción para obtener que $n-1 = m-1$ y la existencia de una permutación $\rho : \{1,\ldots,n-1\} \to \{1,\ldots,n-1\}$ tal que $L_i/L_{i-1} \cong N_{\rho(i)}/N_{\rho(i)-1}$ para $i = 1,\ldots,n-2$ y $N_{n-1}/L_{n-2} \cong N_{\rho(n-1)}/N_{\rho(n-1)-1}$. Reuniendo toda la información, obtenemos que $n = m$, y que la permutación $\sigma : \{1,\ldots,n\} \to \{1,\ldots,n\}$ definida por

$$\sigma(i) = \begin{cases} \rho\tau^{-1}(i) & \text{si } i \in \{1,\ldots,n-1\} \text{ y } \tau^{-1}(i) \in \{1,\ldots,n-2\} \\ n & \text{si } i \in \{1,\ldots,n-1\} \text{ y } \tau^{-1}(i) = n-1 \\ \rho(n-1) & \text{si } i = n \end{cases}$$

es tal que existen isomorfismos de módulos $M_i/M_{i-1} \cong N_{\sigma(i)}/N_{\sigma(i)-1}$ para $i = 1,\dots,n$. ■

**Definición 1.5.3** Los módulos $M_i/M_{i-1}$, $i = 1,\dots,n$ que aparecen en una serie de composición de $M$ se llaman *factores de composición* de $M$ y están determinados, salvo isomorfismo y reordenación, por el propio $M$. El número $n$ se llama *longitud* de $M$ como $A$–módulo, y se denotará por $\ell(M)$. Al módulo cero le asignamos longitud cero.

**Proposición 1.5.2** Sea $M$ un módulo de dimensión finita, y $N \in \mathscr{L}(M)$. Entonces $\ell(M) = \ell(N) + \ell(M/N)$.

*Demostración.* Sea

$$\{0\} = N_0 \subset N_1 \subset \cdots \subset N_{\ell(N)} = N$$

una serie de composición de $N$, y

$$\frac{N}{N} = \frac{M_0}{N} \subset \frac{M_1}{N} \subset \cdots \subset \frac{M_{\ell(M/N)}}{N} = \frac{M}{N},$$

una serie de composición de $M/N$. Por el tercer teorema de isomorfía,

$$M_j/M_{j-1} \cong \frac{M_j/N}{M_{j-1}/N},$$

que es simple, para $j = 1,\dots,\ell(M/N)$. Por tanto,

$$\{0\} = N_0 \subset N_1 \subset \cdots \subset N_{\ell(N)} = N = M_0 \subset M_1 \subset \cdots \subset M_{\ell(M/N)} = M$$

es una serie de composición de $M$. Como consecuencia, $\ell(M) = \ell(N) + \ell(M/N)$. ■

**Corolario 1.5.3** Sea $M$ un módulo de dimensión finita y $N, L \in \mathscr{L}(M)$. Entonces

$$\ell(N+L) + \ell(N \cap L) = \ell(N) + \ell(L).$$

*Demostración.* Por el segundo teorema de isomorfía, $(L+N)/L \cong N/(L \cap N)$. Obviamente, módulos isomorfos tienen la misma longitud, así que, de la Proposición 1.5.2, deducimos que

$$\ell(L+N) - \ell(L) = \ell(N) - \ell(L \cap N),$$

de donde obtenemos inmediatamente la fórmula del enunciado. ■

▪ **Ejercicio 1.20** * Consideramos $T : \mathbb{R}^3 \to \mathbb{R}^3$ una aplicación lineal, y la estructura de $\mathbb{R}[X]$–módulo correspondiente sobre $\mathbb{R}^3$. Discutir los posibles valores de la longitud de $\mathbb{R}^3$ como $\mathbb{R}[X]$–módulo, dependiendo de cómo sea $T$. Poner un ejemplo de $T$ para el que se alcance cada longitud.

▪ **Ejercicio 1.21** Sea $\mathbb{P}_n$ el espacio vectorial real de las funciones polinómicas en una variable de grado menor o igual que $n$. Sea $T : \mathbb{P}_n \to \mathbb{P}_n$ la aplicación lineal que asigna a cada polinomio su derivada. Calcular una serie de composición de $\mathbb{P}_n$ visto como $\mathbb{R}[X]$–módulo via $T$.

▪ **Ejercicio 1.22** ** En la condiciones del Ejercicio 1.21, calcular todos los $\mathbb{R}[X]$–submódulos de $\mathbb{P}_n$.

■ **Ejercicio 1.23** * Clasificar, salvo isomorfismos, todos los $\mathbb{C}[X]$–módulos simples.

■ **Ejercicio 1.24** * Sea $K$ un cuerpo y

$$R = \begin{pmatrix} K & K \\ 0 & K \end{pmatrix} = \{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a,b,c \in K \}.$$

Comprobar que $R$ es una subálgebra de $M_2(K)$ y calcular la longitud, en tanto que $R$–módulo, de $R$.

## 1.6 Independencia lineal y sumas directas internas

En esta sección tratamos la independencia lineal de familias de submódulos de un módulo dado (siempre sobre un anillo $A$). Aunque vamos a tratar el caso finito, en realidad los argumentos que siguen son válidos para cualquier familia de submódulos, finita o no (ver sección 1.7). Con todo, supongamos $I$ un conjunto finito no vacío. Si $\{N_i \mid i \in I\}$ es un conjunto de submódulos de un módulo $M$, denotaremos su suma por $\sum_{i\in I} N_i$.

Usaremos la siguiente terminología: dado un homomorfismo de módulos $f : N \to M$, diremos que $f$ es un *monomorfismo* (resp. *epimorfismo*) si $f$ es inyectivo (resp. *sobreyectivo*).

**Definición 1.6.1** Una familia $\{N_i \mid i \in I\}$ de submódulos no nulos de un módulo $M$ se dirá *independiente* si para todo $j \in I$ se verifica que $N_j \cap \sum_{j\neq i\in I} N_i = \{0\}$. En tal caso, diremos que el submódulo $\sum_{i\in I} N_i$ es *suma directa interna* de los submódulos $\{N_i \mid i \in I\}$.

Recordemos que siempre podemos formar la suma directa externa $\oplus_{i\in I} N_i$. Para cada índice $i \in I$, denotemos por $\imath_i : N_i \to \bigoplus_{i\in I} N_i$ el monomorfismo canónico que lleva $m \in N_i$ en la $I$—tupla todas cuyas componentes son 0 salvo la $i$–ésima, que es $m$.

**Lema 1.6.1** Existe un único homomorfismo de módulos $\theta : \bigoplus_{i\in I} N_i \to \sum_{i\in I} N_i$ tal que $\theta\, \imath_i(m) = m$ para todo $i \in I$ y todo $m \in N_i$.

*Demostración.* El homomorfismo $\theta$ se define como $\theta((m_i)_{i\in I}) = \sum_{i\in I} m_i$. El resto es una comprobación rutinaria. ■

**Proposición 1.6.2** Las siguientes condiciones son equivalentes

1. La familia $\{N_i \mid i \in I\}$ es independiente.
2. Para todo subconjunto no vacío $F \subseteq I$, la familia $\{N_i \mid i \in F\}$ es independiente.
3. La expresión de cada elemento $m \in \sum_{i\in I} N_i$ como $m = \sum_{i\in I} m_i$, con $m_i \in N_i$ es única.
4. Si $0 = \sum_{i\in I} m_i$ con $m_i \in N_i$, entonces $m_i = 0$ para todo $i \in I$.
5. El homomorfismo canónico $\theta : \bigoplus_{i\in I} N_i \to \sum_{i\in I} N_i$ es inyectivo (y, así, un isomorfismo).
6. Para cada par de subconjuntos no vacíos $J_1, J_2 \subseteq I$ con $J_1 \cap J_2 = \emptyset$, se tiene $\sum_{i\in J_1} N_i \cap \sum_{i\in J_2} N_i = \{0\}$.

*Demostración.* (i) $\Rightarrow$ (ii). Esto es obvio.
(ii) $\Rightarrow$ (iii)[5]. Supongamos dos expresiones de $m$ como suma de elementos de los módulos

[5]Como $I$ es finito, en realidad esta implicación es obvia tomando $I = F$. No obstante, cuando $I$ es infinito, como se discute en la próxima sección, la demostración aquí presentada tiene todo el sentido.

de la familia.

$$m = \sum_{i\in I} m_i = \sum_{i\in I} m'_i. \tag{1.4}$$

Tomemos $F \subseteq I$ tal que $m_i = m'_i = 0$ para todo $i \notin F$. Para todo $j \in F$ deducimos de (1.4) que

$$m_j - m'_j = \sum_{j\neq i\in F} m'_i - m_i$$

lo que implica, por independencia, que $m_j - m'_j = 0$.
(iii) $\Rightarrow$ (iv). Evidente.
(iv) $\Rightarrow$ (v). Supongamos una $I$–tupla $(m_i)_{i\in I} \in \ker\theta$. Entonces $\sum_{i\in I} m_i = 0$, luego, por hipótesis, la $i$–tupla tiene todas sus componentes nulas. Esto muestra que $\theta$ es inyectivo.
(v) $\Rightarrow$ (vi). Un elemento no nulo $m \in \sum_{i\in J_1} N_i \cap \sum_{i\in J_2} N_i$ es imagen de dos $I$–tuplas en $\bigoplus_I M_i$ con 'soporte' distinto. Pero esto es imposible, ya que $\theta$ se supone inyectivo.
(vi) $\Rightarrow$ (i). Evidente. ■

Cuando la suma $\sum_{i\in I} N_i$ es directa, usaremos la notación $\bigoplus \sum_{i\in I} N_i$ si queremos insistir en el hecho de que no se trata de la suma directa externa. No obstante, en ausencia de riesgo de confusión, usualmente escribiremos $\bigoplus \sum_{i\in I} N_i = \bigoplus_{i\in I} N_i$.

**Corolario 1.6.3** Si $\{N_i \mid i \in I\}$ es una familia independiente de submódulos de $M$ de y $N$ es un submódulo no nulo de $M$ tal que $N \cap \bigoplus_{i\in I} N_i = \{0\}$, entonces $\{N_i \mid i \in I\} \cup \{N\}$ es independiente.

*Demostración.* Supongamos $0 = n + \sum_{i\in I} n_i \in N + \bigoplus_{i\in I} N_i$. Entonces

$$n = -\sum_{i\in I} n_i \in N \cap \bigoplus_{i\in I} N_i = \{0\},$$

de donde $n = \sum_{i\in I} n_i = 0$. Como la familia $\{N_i \mid i \in I\}$ es independiente, se sigue que $n_i = 0$ para todo $i \in I$. La Proposición 1.6.2 implica que $\{N_i \mid i \in I\} \cup \{N\}$ es independiente. ■

Un resultado fundamental del Álgebra Lineal es que todo espacio vectorial finitamente generado tiene una base. Vamos a demostrar una versión más general de este hecho.

**Teorema 1.6.4** Sea $\{M_i : i \in I\}$ una familia no vacía de submódulos simples de un módulo $M$. Sea $M' = \sum_{i\in I} M_i$ y $N \subseteq M'$ submódulo propio (es decir, $N \neq M'$). Existe $J \subseteq I$ tal que $\{M_i : i \in J\}$ es independiente, $N \cap (\bigoplus_{i\in J} M_i) = \{0\}$, y $M' = N + \bigoplus_{i\in J} M_i$.

*Demostración.* Sea $\Gamma$ el conjunto de los subconjuntos $S \subseteq I$ tales que la familia $\{M_j \mid j \in S\}$ es independiente y $\left(\oplus_{j\in S} M_j\right) \cap N = \{0\}$. Ordenamos $S$ por la relación inclusión.

Razonemos primero que $\Gamma$ es no vacío, demostrando que existe $i \in I$ tal que $\{i\} \in \Gamma$.

Si $N = \{0\}$, entonces basta con tomar $i \in I$ cualquiera para obtener que $\{i\} \in \Gamma$. Si $N \neq \{0\}$, pero $M_i \cap N = \{0\}$ para algún $i \in I$, entonces volvemos a tener que $\{i\} \in \Gamma$. Por último, si $N \cap M_i \neq \{0\}$ para todo $i \in I$, entonces, por ser cada $M_i$ simple, obtenemos que $N \cap M_i = M_i$ para todo $i \in I$, o sea, $M_i \subseteq N$ para todo $i \in I$. Esto claramente implica que $M' = N$, en contra de nuestra hipótesis sobre $N$.

Como $\Gamma$ es un conjunto finito, ha de tener un elemento maximal $J$. Afirmamos que, para todo índice $i \notin J$, ocurre que

$$M_i \cap (N + \bigoplus_{j\in J} M_j) \neq \{0\}. \tag{1.5}$$

En efecto, como $J \cup \{i\} \notin \Gamma$, tenemos que, o bien $\{M_j : j \in J\} \cup \{M_i\}$ no es independiente, o bien $N \cap (\oplus_{j\in J} M_j \oplus M_i) \neq \{0\}$.

En el primer caso, en virtud del Corolario 1.6.3, tenemos que $M_i \cap (\oplus_{j\in J} M_j) \neq \{0\}$. En el segundo, tomemos $0 \neq x \in N \cap (\oplus_{j\in J} M_j \oplus M_i)$. Así,

$$x = \sum_{j\in J} m_j + m_i,$$

para $m_j \in M_j$, con $j \in J$, y $m_i \in M_i$. Además, $m_i \neq 0$ ya que, de lo contrario, $x \in N \cap (\oplus_{j\in J} M_j)$, lo que no es posible porque $J \in \Gamma$. Por tanto,

$$0 \neq m_i = x - \sum_{j\in J} m_j \in N + \oplus_{j\in J} M_j.$$

Así que $\{0\} \neq M_i \cap (N + \oplus_{j\in J} M_j)$.

Finalicemos. Como $M_i$ es simple, (1.5) implica que $M_i \subseteq N + \bigoplus_{j\in J} M_j$, lo que concluye la prueba, puesto que hemos visto que $N + \bigoplus_{j\in J} M_j$ contiene a $M_i$ para todo índice $i \in I$. ■

Los módulos sobre un anillo de división $D$ se suelen llamar *D–espacios vectoriales*[6].

**Corolario 1.6.5** Sea ${}_DV$ un espacio vectorial sobre un anillo de división $D$. Para todo conjunto de generadores no nulos $\{v_i \mid i \in I\}$ de $V$ existe un subconjunto $J \subseteq I$ tal que $V = \oplus_{j\in J} Dv_j$. Como consecuencia, todo espacio vectorial finitamente generado sobre $D$ tiene una base.

*Demostración.* Observemos que $D = \sum_{i\in I} Dv_i$. Para cada $i \in I$, tenemos un homomorfismo sobreyectivo de $D$–módulos $f_i : D \to Dv_i$ definido por $f(a) = av_i$ para todo $a \in D$. Como ${}_DD$ es simple en virtud del Ejercicio 1.18, se sigue $\operatorname{Ker} f_i = \{0\}$, con lo que $f_i$ es un isomorfismo y, así, $Dv_i$ es simple. Ahora aplicamos la Proposición para obtener $J$ tal que $V = \oplus_{j\in J} Dv_j$. De aquí, dado que $D \cong Dv_j$ para todo $j \in J$, es fácil deducir que ${}_DV$ es libre con base $\{v_j \mid j \in J\}$. ■

Por supuesto, ${}_DV \cong D^{(J)}$, lo que se puede considerar una clasificación, salvo isomorfismos, de todos los $D$–espacios vectoriales finitamente generados.

■ **Ejercicio 1.25** ** Supongamos $T : V \to V$ un endomorfismo $K$–lineal, donde $V$ es un espacio vectorial de dimensión finita que consideramos, como de costumbre, como un $K[X]$–módulo. Supongamos que el polinomio mínimo $m(X)$ de $T$ es irreducible en $K[X]$ (ver Ejemplo 1.12 para el concepto de polinomio mínimo). Demostrar que existen $K[X]$–submódulos simples $V_1, \ldots, V_t$ de $V$ tales que $V = V_1 \oplus \cdots \oplus V_t$ como $K[X]$–módulo.

■ **Ejercicio 1.26** ** En las condiciones del Ejercicio 1.25, demostrar que el polinomio característico de $T$ es $m(X)^t$.

[6] Se suelen llamar $D$–espacios vectoriales a izquierda, dándose el nombre de $D$–espacios vectoriales a derecha a los $D^{op}$–espacios vectoriales

## 1.7 Los mismos resultados, sin condiciones de finitud

Los resultados de la sección anterior son válidos, con mínimas adaptaciones de las demostraciones, sin condiciones de finitud. Así, el conjunto de índices $I$ puede ser arbitrario, finito o no. Las modificaciones necesarias son las siguientes:

- La suma directa externa $\bigoplus_{i\in I} N_i$ se define ahora como el subconjunto del producto cartesiano $\Pi_{i\in I} N_i$ formado por aquellas $I$–tuplas $(m_i)_{i\in I}$ tales que $m_i = 0$ salvo para un número finito de índices $i$.
- En la Proposición 1.6.2 hay que modificar la condición 2, estableciendo "Para todo subconjunto *finito* $F \subseteq I$..."
- En la demostración del Teorema 1.6.4, la existencia del elemento maximal $J$ de $\Gamma$ se obtiene invocando el Lema de Zorn. El razonamiento es el siguiente. Queremos aplicar el Lema de Zorn a $\Gamma$, ordenado por inclusión, así que tomemos una cadena $\chi$ en $\Gamma$, y sea $S = \bigcup_{C\in\chi} C$. Para demostrar que el conjunto $\{M_i \mid i \in S\}$ es independiente podemos, en virtud de la Proposición 1.6.2 modificada según el apartado anterior, considerar cualquier subconjunto finito $F \subseteq S$. Pero entonces $F \subseteq C$ para algún $C \in \chi$, y la familia $\{M_i : i \in F\}$ es independiente por serlo el conjunto $\{M_i : i \in C\}$. Por otra parte, si $m \in N \cap (\oplus_{i\in S} M_i)$, entonces $m \in N \cap (\oplus_{i\in C} M_i)$ para algún $C \in \chi$, luego $m = 0$. Así que $S \in \Gamma$ es una cota superior para $\chi$. Por el Lema de Zorn, $\Gamma$ ha de tener un elemento maximal $J$.

Si miramos ahora el Corolario 1.6.5 con $I$ cualquiera, podemos tomar como $I$ un conjunto de generadores de un $D$–espacio vectorial cualquiera $V$ y obtenemos.

**Corolario 1.7.1** Todo espacio vectorial no nulo sobre un anillo de división $D$ tiene una base (finita o no). Si el espacio vectorial es finitamente generado, entonces tiene una base finita.

## 1.8 Clasificación de las álgebras de división reales de dimensión finita.

Recordemos que un álgebra sobre un cuerpo se llama de división si cada elemento no nulo es invertible con respecto de la multiplicación del álgebra. Vamos a demostrar seguidamente un famoso teorema de Frobenius que afirma que, salvo isomorfismos, sólo hay tres álgebras reales finito-dimensionales de división, a saber, los cuerpos de los números reales y complejos, y el álgebra de división de los cuaterniones de Hamilton.

Comenzaremos demostrando un lema previo, para cuya comprensión debemos recordar que un álgebra de dimensión finita siempre se puede ver como una subálgebra de un álgebra de endomorfismos lineales (o de matrices). Concretamente, si $D$ es un álgebra de división real de dimensión $n$, consideraremos la representación regular $\lambda : D \to \mathrm{End}_{\mathbb{R}}(D)$. Con ello, si $a \in D$, entonces entendemos que el determinante de $a$, su traza, su polinomio característico y su polinomio mínimo son los del endomorfismo lineal $\lambda(a) : D \to D$.

**Lema 1.8.1** Sea $D$ un álgebra de división real de dimensión finita mayor o igual que 2. Entonces

$$\{a \in D : a^2 \leq 0\} = \{a \in D : tr(a) = 0\}$$

Por tanto, $V = \{a \in D : a^2 \leq 0\}$ es un subespacio vectorial real de $D$ y $D = \mathbb{R} \oplus V$. Además, la dimensión real de $D$ es par.

*Demostración.* Denotemos por $n$ la dimensión de $D$ como $\mathbb{R}$–espacio vectorial. Sabemos[7] que podemos considerar $\mathbb{R} \subseteq D$ como subálgebra real. Dado un elemento $a \in D$, podemos considerar su polinomio característico $p(X) \in \mathbb{R}[X]$. Por el Teorema Fundamental del Álgebra,

$$p(X) = (X - r_1) \cdots (X - r_k) q_1(X) \cdots q_m(X),$$

donde $r_1, \ldots, r_k \in \mathbb{R}$, y $q_1(X), \ldots, q_m(X) \in \mathbb{R}[X]$ son polinomios cuadráticos irreducibles y mónicos. Por el Teorema de Cayley-Hamilton, tenemos que $p(a) = 0$ lo que implica, dado que $D$ es un anillo de división, que $a - r_i = 0$ para algún $i \in \{1, \ldots, k\}$, o bien $q_j(a) = 0$ para algún $j \in \{1, \ldots, m\}$. En el primer caso, $a \in \mathbb{R}$ y, por tanto, si $a^2 \leq 0$, tenemos que $a = 0$. Por otra parte, si $a \in \mathbb{R}$, entonces $tr(a) = na$, luego $tr(a) = 0$ implica también $a = 0$. Esto también implica que $V \cap \mathbb{R} = \{0\}$.

Tomemos, por tanto, $a \in D$ pero $a \notin \mathbb{R}$. Entonces $q_j(a) = 0$ para algún $j$ y deducimos que $q_j(X)$ es el polinomio mínimo de $a$, puesto que es irreducible. Llamemos $q(X) = q_j(X)$. Por el Ejercicio 1.26[8], $p(X) = q(X)^t$ para algún $t$. De hecho, $2t = n$. Ahora, por ser irreducible, tenemos que $q(X) = (X - z)(X - \overline{z})$ para algún número complejo $z$ no real. De modo que

$$q(X) = X^2 - (2Rez)X + |z|^2, \tag{1.6}$$

donde $Rez$ denota la parte real de $z$ y $|z|$ el módulo de $z$. De (1.6) deducimos que

$$p(X) = X^{2t} - (2tRez)X^{2t-1} + \cdots \tag{1.7}$$

Por otra parte,

$$p(X) = X^{2t} - tr(a)X^{2t-1} + \cdots \tag{1.8}$$

De (1.8) y (1.7) deducimos que $2tRez = tr(a)$. Teniendo en cuenta que $q(a) = 0$ y sustituyendo en (1.6), obtenemos

$$a^2 - \frac{tr(a)}{t}a + |z|^2 = 0 \tag{1.9}$$

Por tanto, para $a \in D$ no real, deducimos[9] de (1.9) que $a^2 < 0$ si, y sólo si, $tr(a) = 0$.

Que $D = \mathbb{R} \oplus V$ es consecuencia de que $tr : D \to \mathbb{R}$ es una forma lineal no nula cuyo núcleo es $V$. ■

**Teorema 1.8.2** [Frobenius] Sea $D$ un álgebra de división real de dimensión finita. Entonces $D$ es isomorfa bien a $\mathbb{R}$, o bien a $\mathbb{C}$ o bien a $\mathbb{H}$.

*Demostración.* Supongamos que $D$ no es isomorfa a $\mathbb{R}$. Entonces, según el Lema 1.8.1, la dimensión de $D$ es par, digamos $2t$. Sea $V = \{a \in D : a^2 \leq 0\}$ que, según el mismo lema, es un subespacio vectorial real de $D$ tal que $D = \mathbb{R} \oplus V$. Consideremos la aplicación

$$B : V \times V \to \mathbb{R}, \qquad B(a,b) = \frac{ab + ba}{2}$$

Veamos que, realmente, $B(a,b) \in \mathbb{R}$ para todo $a, b \in D$:

$$ab + ba = (a+b)^2 - a^2 - b^2,$$

[7] Ver el final de la Sección 1.2

[8] Aquellos alumnos que hayan seguido un curso de Álgeba Lineal que incluya formas canónicas de matrices, no necesitan este ejercicio, claro

[9] Tengamos en cuenta que la condición $a^2 < 0$ entraña que $a^2 \in \mathbb{R}$.

que es un elemento de $\mathbb{R}$ puesto que $a, b, a+b \in V$. Es fácil comprobar que $B$ es una forma bilineal real y simétrica. Además, $B(a,a) = a^2 \leq 0$ para todo $a \in V$ y $B(a,a) = 0$ si y sólo si $a = 0$. Por tanto, $B$ es definida negativa. Esto significa que existe una base $\{e_1, \ldots, e_{2t-1}\}$ de $V$ tal que $B(e_i, e_j) = 0$ si $i \neq j$ y $B(e_i, e_i) = -1$ para todo $i = 1, \ldots, 2t-1$. En vista de la definición de $B$, lo que tenemos es

$$e_i e_j = -e_j e_i, \quad (i \neq j); \qquad e_i^2 = -1$$

Si $t = 1$, entonces es claro que $D = \mathbb{R} \oplus V$ es isomorfa a $\mathbb{C}$, con $e_1$ la unidad imaginaria.

Supongamos ahora $t > 1$. Entonces, para $j \geq 3$, tenemos el siguiente cálculo para $u = e_1 e_2 e_j$:

$$u^2 = e_1 e_2 e_j e_1 e_2 e_j = -e_1 e_2 e_1 e_j e_2 e_j = e_1 e_2 e_1 e_2 e_j^2 = -e_1 e_2 e_1 e_2 = 1$$

Así que $0 = (u-1)(u+1)$, de donde, al ser $D$ un anillo de división, $u = \pm 1$. Esto es, $e_j = \pm e_1 e_2$ para todo $j \geq 3$. Por tanto, $t = 2$ y $V$ tiene como base $e_1, e_2, e_3$. Deducimos que $\{1, e_1, e_2, e_1 e_2\}$ es una base de $D$ como $\mathbb{R}$–espacio vectorial.

Tenemos, pues, un isomorfismo de espacios vectoriales reales $\varphi : \mathbb{H} \to D$ determinado por $\varphi(\mathbf{1}) = 1, \varphi(\mathbf{i}) = e_1, \varphi(\mathbf{j}) = e_2, \varphi(\mathbf{k}) = e_1 e_2$. Una comprobación rutinaria muestra que $\varphi$ respeta las identidades del apartado 4 del Ejercicio 1.9. De aquí es fácil deducir que $\varphi$ es multiplicativa. Por tanto, es un isomorfismo de $\mathbb{R}$–álgebras, lo que concluye esta demostración. ■

**Corolario 1.8.3** Toda álgebra de división compleja de dimensión finita es isomorfa a $\mathbb{C}$.

*Demostración.* Sea $D$ un álgebra de división compleja de dimensión finita. Obviamente, al ser $\mathbb{R}$ un subcuerpo de $\mathbb{C}$, resulta que $D$ es un álgebra de división real de dimensión finita. Luego la dimensión compleja de $D$ ha de ser 1 o 2. Pero, en el segundo caso, $D$ sería isomorfa a $\mathbb{H}$, cuyo centro es $\mathbb{R}$, luego no es un álgebra sobre $\mathbb{C}$. ■

## 1.9 Idempotentes y anillos de matrices.

En esta sección, denotaremos por $R$ un anillo, que, en ocasiones, se supondrá un álgebra sobre un cuerpo $K$.

**Definición 1.9.1** Un elemento $e \in R$ se llama *idempotente* si $e = e^2$. Es claro que 1 y 0 son siempre elementos idempotentes. Diremos que un idempotente $e$ es no trivial si $e \neq 1, 0$.

▪ **Ejercicio 1.27** Encontrar todos los idempotentes en $\mathbb{Z}[\sqrt{3}]/\langle 3 \rangle$.

▪ **Ejercicio 1.28** ** Sea $R$ un álgebra sobre un cuerpo de característica distinta de 2, y $a, b, e \in R$ idempotentes. Demostrar que si $e = a + b$, entonces $ab = ba = 0$. Si la característica es 2, encontrar un contraejemplo con $b \neq a$.

**Definición 1.9.2** Un conjunto $\{e_1, \ldots, e_n\}$ de idempotentes no nulos de $R$ se dirá un *conjunto completo de idempotentes ortogonales* (abreviatura CCIO), si $1 = e_1 + \cdots + e_n$ y $e_i e_j = 0$ para todo $i \neq j$.

▪ **Ejercicio 1.29** Dar un CCIO con $n$ elementos para $R = M_n(K)$.

Los CCIOs están íntimamente relacionados con las descomposiciones del módulo regular como suma directa de submódulos (ideales a izquierda), como muestran los siguientes resultados.

**Lema 1.9.1** Sea $\{e_1, \ldots, e_n\}$ un CCIO para $R$. Entonces $R = Re_1 \oplus \cdots \oplus Re_n$.

*Demostración.* Dado $r \in R$, tenemos que

$$r = r1 = r(e_1 + \cdots + e_n) = re_1 + \cdots + re_n,$$

luego $R = Re_1 + \cdots + Re_n$.

Para ver que la suma es directa, hemos de comprobar que $Re_j \cap (\sum_{i \neq j} Re_i) = \{0\}$ para todo $j = 1, \ldots, n$. Supongamos $r_j e_j = \sum_{i \neq j} r_i e_i$, para ciertos $r_i \in R$. Entonces $r_j e_j = r_j e_j^2 = \sum_{i \neq j} r_i e_i e_j = 0$. ■

**Lema 1.9.2** Supongamos $R = I_1 \oplus \cdots \oplus I_n$, con $I_1, \ldots, I_n$ ideales a izquierda no nulos de $R$. Sea $1 = e_1 + \cdots + e_n$, con $e_i \in I_i$ para todo $i = 1, \ldots, n$. Entonces $\{e_1, \ldots, e_n\}$ es un CCIO para $R$ e $I_i = Re_i$ para todo $i = 1, \ldots, n$. Además, si $r \in R$, entonces $r \in I_i$ si, y sólo si, $re_i = r$.

*Demostración.* Sea $x \in I_j$ para algún $j$. Entonces $x = x \sum_i e_i$, de donde $x - xe_j = \sum_{i \neq j} xe_i$. De modo que $x - xe_j \in I_j \cap (\sum_{i \neq j} I_i) = \{0\}$, lo que implica que $x - xe_j = 0$, esto es, $x = xe_j$. Hemos demostrado, pues, que

$$I_j = \{x \in R : xe_j = x\}$$

Una consecuencia inmediata (tomo $x = e_j$) es que $e_j$ es idempotente para todo $j = 1, \ldots, n$. Deducimos fácilmente que $Re_i = I_i$ para todo $i = 1, \ldots, n$.

Por último, para cada $i = 1, \ldots, n$, tenemos que

$$e_i = e_i(\sum_j e_j) = e_i + \sum_{j \neq i} e_i e_j,$$

de donde $\sum_{j \neq i} e_i e_j = 0$. Como $I_1, \ldots, I_n$ son independientes, deducimos de aquí que $e_i e_j = 0$ para todo $i \neq j$. ■

Fijemos ahora un CCIO $\{e_1, \ldots, e_n\}$ para $R$, y definamos para cada $i, j \in \{1, \ldots, n\}$,

$$e_i R e_j = \{e_i r e_j : r \in R\}.$$

Es claro que cada $e_i R e_j$ es un subgrupo aditivo de $R$.

Recordemos que $M_n(R)$ denota el anillo de las matrices de orden $n \times n$ con coeficientes en $R$. Consideremos el subconjunto de $M_n(R)$ siguiente

$$Mat_{1 \leq i,j \leq n}(e_i R e_j) = \{(r_{ij}) \in M_n(R) : r_{ij} \in e_i R e_j, \ \forall i, j = 1, \ldots, n\}.$$

Cuando el conjunto de índices $\{1, \ldots, n\}$ está claro por el contexto, usaremos simplemente la notación $Mat(e_i R e_j)$. Es fácil ver que $Mat(e_i R e_j)$ es un subgrupo aditivo de $M_n(R)$.

Observemos que, si $r_{ik} \in e_i R e_k$ y $s_{kj} \in e_k R e_j$ para $i, j, k \in \{1, \ldots, n\}$, entonces $r_{ik} s_{kj} \in e_i R e_j$. De aquí deducimos fácilmente que $Mat(e_i R e_j)$ es un subconjunto cerrado para la

multiplicación[10] de $M_n(R)$. No obstante, no es un subanillo, ya que la matriz identidad no pertenece a $Mat(e_iRe_j)$. Aún así, la matriz diagonal

$$\begin{pmatrix} e_1 & 0 & \cdots & 0 \\ 0 & e_2 & \cdots & 0 \\ \vdots & & & \vdots \\ 0 & 0 & \cdots & e_n \end{pmatrix}, \tag{1.10}$$

es un elemento neutro multiplicativo para $Mat(e_iRe_j)$. Esto se deduce de que si $r_{ij} \in e_iRe_j$, entonces $e_ir_{ij} = r_{ij} = r_{ij}e_j$, para cualesquiera $i, j$.

En resumen, $Mat(e_iRe_j)$ es un anillo, con las operaciones suma y producto heredadas de $M_n(R)$, pero no es un subanillo, puesto que su uno es distinto.

Es fácil convencerse de que, si $R$ es una $K$–álgebra, entonces así lo es el subespacio vectorial $Mat(e_iRe_j)$ de $M_n(R)$.

**Proposición 1.9.3** La aplicación $\phi : R \to Mat(e_iRe_j)$ definida por

$$\phi(r) = (e_ire_j)_{1\leq i,j\leq n}$$

para $r \in R$ es un isomorfismo de anillos. Si $R$ es una $K$–álgebra, entonces $\phi$ es un isomorfismo de $K$–álgebras.

*Demostración.* Es bastante claro que $\phi$ es una aplicación aditiva (y $K$–lineal, en su caso). Para ver que $\phi$ preserva productos, tomemos $r, s \in R$. La componente $i, j$–ésima de la matriz producto $\phi(r)\phi(s)$ es

$$\sum_k e_ire_ke_kse_j = \sum_k e_ire_kse_j = e_ir(\sum_k e_k)se_j = e_irse_j,$$

que es la componente $i, j$–ésima de $\phi(rs)$. Como $\phi(1)$ es claramente la matriz (1.10), deducimos que $\phi$ es un homomorfismo de anillos (de $K$–álgebras, en su caso).

Observemos que, si $r \in R$, entonces

$$r = (\sum_i e_i)r(\sum_j e_j) = \sum_{i,j} e_ire_j.$$

Por tanto, si $\phi(r) = 0$, entonces $e_ire_j = 0$ para todo $i, j$, por lo que $r = 0$. Esto prueba que $\phi$ es inyectivo.

Por último, veamos que $\phi$ es sobreyectiva. Dada una matriz de la forma $(r_{ij})_{1\leq i,j\leq n}$, con $r_{ij} \in e_iRe_j$, tomamos $r = \sum_{i,j} r_{ij} \in R$. Bien, la componente $i, j$–ésima de $\phi(r)$ es $e_i(\sum_{k,l} r_{kl})e_j = r_{ij}$, ya que $e_ir_{kl}e_j = 0$ si $i \neq k$ o $l \neq j$, mientras que $e_ir_{ij}e_j = r_{ij}$. ■

**Ejemplo 1.15** Supongamos que $M$ es un módulo sobre un anillo $A$, Entonces

$$\mathrm{End}_A(M) = \{f : M \to M \mid f \text{ es homomorfismo de } A-\text{módulos}\}$$

es un subanillo de $\mathrm{End}(M)$, llamado *anillo de endomorfismos del $A$–módulo $M$* (y es una subálgebra de $\mathrm{End}_K(M)$ si $A$ es una $K$–álgebra).

Si $M = M_1 \oplus \cdots \oplus M_n$, denotemos, para cada $i = 1, \ldots, n$, por $\iota_i : M_i \to M$ la inclusión canónica, y por $\pi_i : M \to M_i$ la aplicación que asigna $\pi_i(m) = m_i$ a cada $m = m_1 + \cdots +$

[10] es decir, $A, B \in Mat(e_iRe_j)$ implica que $AB \in Mat(e_iRe_j)$.

$m_n \in M$, con $m_j \in M_j$ para $j = 1, \ldots, n$. Si denotamos por $e_i = \iota_i \pi_i$ para $i = 1, \ldots, n$, no es difícil ver que $\{e_1, \ldots, e_n\}$ es un CCIO para el anillo $\mathrm{End}_A(M)$. ▪

▪ **Ejercicio 1.30** Comprobar las afirmaciones realizadas en el Ejemplo 1.15.

**Proposición 1.9.4** Sea $M$ un $A$–módulo, y pongamos $R = \mathrm{End}_A(M)$. Supongamos que $M = M_1 \oplus \cdots \oplus M_n$ para submódulos $M_i$ tales que existe un $A$–módulo $N$ y un isomorfismo de $A$–módulos $M_i \cong N$ para cada $i = 1, \ldots, n$.

Si $\Delta = \mathrm{End}_A(N)$, entonces existe un isomorfismo de anillos $R \cong M_n(\Delta)$ que, si $A$ es una $K$–álgebra, es de $K$–álgebras.

*Demostración.* Para cada $i = 1, \ldots, n$, tenemos por hipótesis un isomorfismo de $A$–módulos $\varphi_i : M_i \to N$. Seguiremos la notación del Ejemplo 1.15. Sabemos que $R$ es isomorfo con el anillo de matrices $Mat(e_i R e_j)$. Definimos la aplicación $\phi : Mat(e_i R e_j) \to M_n(\Delta)$ por

$$\phi(r_{ij}) = (\varphi_i \pi_i r_{ij} \iota_j \varphi_j^{-1}).$$

Una comprobación rutinaria muestra que $\phi$ es un homomorfismo de anillos (o de $K$–álgebras, en su caso). Además, la aplicación $\psi : M_n(\Delta) \to Mat(e_i R e_j)$ definida por

$$\psi(s_{ij}) = (\iota_i \varphi_i^{-1} s_{ij} \varphi_j \pi_j)$$

es la inversa para la composición de $\phi$. Por tanto, $\phi$ es un isomorfismo de anillos. ■

▪ **Ejercicio 1.31** Cubrir los detalles de la demostración de la Proposición 1.9.4

Hemos visto que una descomposición de un anillo como suma directa de ideales a izquierda da lugar a un conjunto completo de idempotentes ortogonales. Seguidamente, mostraremos que si los sumandos directos son ideales, entonces los idempotentes son centrales.

**Lema 1.9.5** Supongamos que $R = I_1 \oplus \cdots \oplus I_n$ con $I_i$ ideal[11] no nulo de $R$ para todo $i = 1, \ldots, n$, y sea $\{e_1, \ldots, e_n\}$ el CCIO asociado. Entonces $e_i \in Z(R)$ para todo $i = 1, \ldots, n$.

*Demostración.* Sea $i \in \{1, \ldots, n\}$. Dados $x \in I_i, y \in \oplus_{j \neq i} I_j$ tenemos que

$$xy \in I_i \cap \oplus_{j \neq i} I_j = \{0\},$$

esto es, $xy = 0$. Análogamente, $yx = 0$. Ahora, dado $r \in R$, tenemos que $e_i r \in I_i$ y, por tanto, $e_i r e_i = e_i r$. Por otra parte,

$$re_i = (\sum_j e_j) re_i = e_i re_i + \sum_{j \neq i} e_j re_i = e_i re_i,$$

ya que $\sum_{j \neq i} e_j \in \oplus_{j \neq i} I_j$ y $re_i \in I_i$. Tenemos, pues, que $e_i r = e_i re_i = re_i$, luego $e_i \in Z(R)$. ■

▪ **Ejercicio 1.32** Sea $\{e_1, \ldots, e_n\}$ un CCIO para $R$. Demostrar que los idempotentes $e_1, \ldots, e_n$ son centrales si, y sólo si, $e_i R e_j = \{0\}$ para todo $i \neq j$.

[11] A veces, se dice ideal *bilátero* para distinguir, en el caso no conmutativo, de la noción más débil de ideal a izquierda.

Obviamente, si $\{e_1,\dots,e_n\}$ es un CCIO centrales de $R$, entonces cada $Re_i$ es un ideal y $R = Re_1 \oplus \cdots \oplus Re_n$ es una suma directa de ideales biláteros. Pero hay otra forma de ver esta descomposición. Para ello, notemos que si $R_1,\dots,R_n$ son anillos (respectivamente, $K$–álgebras), entonces el producto cartesiano

$$R_1 \times \cdots \times R_n$$

es un anillo (respectivamente, una $K$–álgebra) con las operaciones obvias definidas "componente a componente".

**Proposición 1.9.6** Sea $\{e_1,\dots,e_n\}$ un CCIO centrales de $R$. Entonces $Re_i$ es un anillo (o una $K$–álgebra, si lo es $R$) con unidad $e_i$ para cada $i = 1,\dots,n$ y la aplicación $R \to Re_1 \times \cdots \times Re_n$ que lleva $r \in R$ en $(re_1,\dots,re_n)$ es un isomorfismo de anillos (o de $K$–álgebras, en su caso).

*Demostración.* Puesto que cada $e_i$ es central, es claro que cada $Re_i = e_iRe_i$ es una $K$–álgebra con unidad $e_i$. Como $e_iRe_j = 0$ para $i \neq j$, deducimos de la Proposición 1.9.3 el isomorfismo del enunciado[12]. ■

**Definición 1.9.3** Supongamos $e$ un idempotente central de $R$. Diremos que $e$ es *indescomponible*[a] si $e \neq 0$ y $Re$ no se puede poner como suma directa de dos ideales no nulos de $R$.

[a] Se le suele llamar también idempotente central primitivo. Pero también se adjetiva como primitivo, en otro contexto, a un idempotente no necesariamente central, lo que puede llevar a confusiones lamentables. Por eso, preferimos aquí usar el adjetivo indescomponible.

**Proposición 1.9.7** Si $R$ tiene un CCIO centrales indescomponibles, entonces este conjunto es único. En particular, cada $K$–álgebra de dimensión finita admite un único CCIO centrales indescomponibles.

*Demostración.* Sean $\{e_1,\dots,e_n\}$, $\{f_1,\dots,f_m\}$ dos conjuntos de CCIO centrales indescomponibles. Observemos que $e_if_j$ es un idempotente central para cada par de índices $i,j$. Además, $Re_i = Re_if_j \oplus Re_i(1-f_j)$. De modo que, si $e_if_j \neq 0$, entonces $Re_i(1-f_j) = 0$, es decir, $e_i(1-f_j) = 0$, con lo que $e_i = e_if_j$. Pero, por un argumento simétrico, se demuestra que si $e_if_j \neq 0$, entonces $e_if_j = f_j$. Luego hemos probado que $e_if_j \neq 0$ implica que $e_i = f_j$.

Por otra parte, dado $e_i$, tenemos que

$$0 \neq e_i = e_i(f_1 + \cdots + f_m) = e_if_1 + \cdots + e_if_m,$$

por lo que $e_if_j \neq 0$ para algún $j$, así que $e_i = f_j$. Por tanto $\{e_1,\dots,e_n\} \subseteq \{f_1,\dots,f_m\}$. La otra inclusión se deduce igual cambiando los papeles de los dos CCIO centrales indescomponibles. ■

▪ **Ejercicio 1.33** Demostrar que, si $M$ un $R$–módulo y $e \in R$ un idempotente central, entonces $eM = \{em : m \in M\}$ es un submódulo de $M$. Si ahora $\{e_1,\dots,e_n\}$ es un CCIO centrales de $R$, demostrar que $M = e_1M \oplus \cdots \oplus e_nM$.

▪ **Ejercicio 1.34** Con la notación del Ejercicio 1.33, demostrar que $M$ es cíclico si, y sólo si, $e_iM$ es cíclico para todo $i = 1,\dots,n$.

[12] Una demostración alternativa es usar el Teorema Chino de los Restos, ver [1, página 2.68]

■ **Ejercicio 1.35** * Consideremos un polinomio no constante $f \in K[X]$, con $K$ un cuerpo. Describir un CCIO (centrales) indescomponibles para $A = K[X]/\langle f \rangle$.

■ **Ejercicio 1.36** ** Sea $V$ un $K$–espacio vectorial de dimensión finita $n$ y $T : V \to V$ una aplicación lineal. Diremos que un vector $v \in V$ es cíclico para $T$ si $\{v, T(v), \ldots, T^{n-1}(v)\}$ es una base de $V$ como $K$–espacio vectorial. Demostrar que $V$ admite un vector cíclico si, y sólo si, el polinomio mínimo de $T$ tiene grado $n$. ¿Cuál es entonces la longitud de $V$ en tanto que $K[X]$–módulo?

## 1.10 El álgebra de endomorfismos de un módulo semisimple.

Cualquier subespacio vectorial de un espacio vectorial tiene un complementario. Esto no ocurre en en general para los módulos sobre un álgebra. Seguidamente, estudiaremos aquellos módulos que sí disfrutan de esta propiedad. En esta sección, $A$ denotará un álgebra sobre un cuerpo $K$, y los módulos serán sobre este álgebra.

**Definición 1.10.1** Sea $M$ un módulo, y $N$ un submódulo de $M$. Un *complemento* de $N$ en $M$ es un submódulo $X$ de $M$ tal que $M = N \oplus X$. Por comodidad, vamos a admitir la notación $M = M \oplus \{0\}$, bien entendido que $M$ y $\{0\}$ no son submódulos independientes de $M$.

En caso de que exista dicho complemento, diremos que $N$ es un *sumando directo* de $M$.

■ **Ejercicio 1.37** Sea $A = K[X]/\langle X^2 \rangle$, donde $K$ es un cuerpo, y $K[X]$ es el anillo de polinomios. Demostrar que, visto como $A$–módulo, $A$ no tiene sumandos directos no triviales.

**Proposición 1.10.1** Sea $M$ un módulo no nulo de dimensión finita como $K$–espacio vectorial. Las siguientes condiciones son equivalentes.

1. Todo submódulo de $M$ es un sumando directo;
2. $M$ se descompone como suma directa finita de submódulos simples;
3. $M$ es suma de un conjunto finito de submódulos simples.

*Demostración.* (1) $\Rightarrow$ (2). Sea $\{M_1, \ldots, M_n\}$ una familia independiente de submódulos simples de $M$ tal que $dim_K(M_1 \oplus \cdots \oplus M_n)$ es máxima entre todas las familias de este tipo. Notemos que, dado que $dim_K(M)$ es finita, existe al menos un submódulo simple de $M$, luego hay, al menos, una tal familia.

Pongo $N = M_1 \oplus \cdots \oplus M_n$. Por hipótesis, existe un submódulo $X$ de $M$ tal que $M = N \oplus X$. Si $X \neq \{0\}$, entonces $X$ contiene un submódulo simple $M_{n+1}$. Pero entonces $\{M_1, \ldots, M_n, M_{n+1}\}$ es una familia independiente, ya que $M_{n+1} \cap N = \{0\}$. Esto va en contra de la elección de la familia $\{M_1, \ldots, M_n\}$, luego $X = \{0\}$.
(2) $\Rightarrow$ (3). Esto es obvio.
(3) $\Rightarrow$ (1). Es consecuencia directa del Teorema 1.6.4. ■

**Definición 1.10.2** Un módulo de dimensión finita se dice *semisimple* si todo submódulo es un sumando directo. Según la Proposición 1.10.1, los módulos semisimples no nulos de dimensión finita son, precisamente, las sumas (directas) finitas de módulos simples (de dimensión finita, claro).

Queremos describir la estructura del álgebra de endomorfismos de un módulo semisimple de dimensión finita. Comencemos por un resultado clásico.

**Lema 1.10.2 — Lema de Schur.** Si $M$ y $M'$ son dos módulos simples y $f : M \to M'$ es un homomorfismo de módulos, entonces, si $f \neq 0$, entonces $f$ es un isomorfismo. Como consecuencia, el anillo de endomorfismos de un módulo simple es un anillo de división.

*Demostración.* Si $f \neq 0$, entonces $\operatorname{Ker} f$ es un submódulo propio de $M$, luego, al ser $M$ simple, $\operatorname{Ker} f = \{0\}$. Por tanto, $\operatorname{Im} f$ es un sumbódulo no nulo de $M'$, por lo que, al ser $M'$ simple, $\operatorname{Im} f = M'$. Luego $f$ es un isomorfismo. ■

▪ **Ejercicio 1.38** Sean $M$ y $N$ módulos semisimples con descomposiciones como suma directa de submódulos simples $M = S_1 \oplus \cdots \oplus S_t$ y $N = T_1 \oplus \cdots \oplus T_s$. Supongamos que $S_i$ no es isomorfo a $T_j$ para todo $i = 1, \ldots, t$, $j = 1, \ldots, s$. Demostrar que todo homomorfismo de módulos de $M$ a $N$ es cero.

**Proposición 1.10.3** Si $M$ es un módulo semisimple de dimensión finita, entonces todo submódulo de $M$ y todo cociente de $M$ es semisimple.

*Demostración.* Supongamos que $M$ es no nulo, y que $f : M \to N$ es un epimorfismo de módulos. Pongamos $M = \sum_{i \in I} M_i$, con $M_i$ simple para todo $i \in I$. Entonces $N = \sum_{i \in I} f(M_i)$. Como consecuencia del Lema de Schur (bueno, de su demostración), $f(M_i)$ es o nulo o isomorfo a $M_i$ para cada $i \in I$. Por tanto, $N$ es suma de módulos simples, con lo que es semisimple, según la Proposición 1.10.1.

Supongamos ahora que $N$ es un submódulo de $M$. Como $M$ es semisimple, existe un submódulo $X$ de $M$ tal que $M = N \oplus X$. Por el Tercer Teorema de Isomorfía, tenemos que

$$\frac{M}{X} = \frac{N \oplus X}{X} \cong \frac{N}{N \cap X} \cong N,$$

ya que $N \cap X = \{0\}$. Por tanto, $N$ es la imagen de $M$ por un epimorfismo, luego es semisimple, según la primera parte de esta demostración. ■

**Proposición 1.10.4** Sea $M$ un módulo semisimple de dimensión finita, y $M = M_1 \oplus \cdots \oplus M_n = N_1 \oplus \cdots \oplus N_m$ dos descomposiciones de $M$ como suma directa de submódulos simples. Entonces $n = m$ y, tras eventual reindexación, $M_i \cong N_i$ para todo $i = 1, \ldots, n$.

*Demostración.* Vamos a aplicar el Teorema de Jordan-Hölder. Para ello, observemos que

$$\{0\} = M_0 \subset M_1 \subset M_1 \oplus M_2 \subset \cdots \subset M_1 \oplus \cdots \oplus M_n = M$$

es una serie de composición de $M$. Esto es consecuencia de que, por el Segundo Teorema de Isomorfía

$$\frac{M_j \oplus \cdots \oplus M_0}{M_{j-1} \oplus \cdots \oplus M_0} \cong \frac{M_j}{(M_{j-1} \oplus \cdots \oplus M_0) \cap M_j} \cong M_j$$

ya que $(M_{j-1} \oplus \cdots \oplus M_0) \cap M_j = \{0\}$, para todo $j = 1, \ldots, n$. Por tanto, los módulos $M_1, \ldots, M_n$ son factores de composición de $M$. Por supuesto, también lo son $N_1, \ldots, N_m$. Así que la proposición se sigue del Teorema de Jordan-Hölder. ■

**Definición 1.10.3** Dado un módulo semisimple no nulo de dimensión finita $M$, tomemos $M = M_1 \oplus \cdots \oplus M_n$ con $M_1, \ldots, M_n$ submódulos simples. Reunamos estos sumandos directos en subconjuntos de módulos isomorfos entre sí. Esto significa que podemos escoger módulos simples $\Sigma_1, \ldots, \Sigma_t$ y una partición

$$\{1, \ldots, n\} = \Lambda_1 \cup \cdots \cup \Lambda_t$$

tal que $M_i \cong \Sigma_j$ si y sólo si $i \in \Lambda_j$. Si ponemos $M_{\Lambda_j} = \oplus_{i \in \Lambda_j} M_i$ para cada $j = 1, \ldots, t$, entonces, obviamente, $M = M_{\Lambda_1} \oplus \cdots \oplus M_{\Lambda_t}$. Los submódulos $M_{\Lambda_j}$ se llaman *componentes isotípicas* u *homogéneas* de la descomposición de $M$.

Pongamos $n_j$ el cardinal de $\Lambda_j$ para cada $j = 1, \ldots, n$. Entonces $n_j$ se llama *multiplicidad* de $\Sigma_j$ en $M$. Es consecuencia de la Proposición 1.10.4 que las multiplicidades $n_1, \ldots, n_t$ no dependen de la descomposición escogida. Los módulos simples $\Sigma_j$ están también determinados por $M$ salvo isomorfismos. A la lista de $(\Sigma_1, n_1), \ldots, (\Sigma_t, n_t)$ la llamaremos *estructura de* $M$. Se tiene, obviamente, que

$$dim_K(M) = n_1 dim_K(\Sigma_1) + \cdots + n_t dim_K(\Sigma_t).$$

■ **Ejercicio 1.39** Sea $M$ un módulo semisimple de dimensión finita con estructura $(\Sigma_1, n_1), \cdots, (\Sigma_t, n_t)$. Si $N$ es un submódulo de $M$, demostrar que su estructura es $(\Sigma_1, m_1), \ldots, (\Sigma_t, m_t)$ para ciertos $m_j \leq n_j$ (admitimos que $m_j = 0$ significa que $\Sigma_j$ no aparece en la estructura de $N$).

■ **Ejercicio 1.40** Establecer un enunciado análogo al del Ejercicio 1.39 para cada cociente de $M$.

**Teorema 1.10.5** Sea $M$ un $A$–módulo semisimple no nulo con estructura

$$(\Sigma_1, n_1), \ldots, (\Sigma_t, n_t).$$

Entonces $\Delta_j := \mathrm{End}_A(\Sigma_j)$ es una $K$–álgebra de división de dimensión finita para todo $j = 1, \ldots, t$, y existe un isomorfismo de $K$–álgebras

$$\mathrm{End}_A(M) \cong M_{n_1}(\Delta_1) \times \cdots \times M_{n_t}(\Delta_t)$$

*Demostración.* Que $\Delta_j$ es una $K$–álgebra de división lo da el Lema de Schur. Es de dimensión finita porque $\Delta_j$ es una subálgebra de $\mathrm{End}_K(\Sigma_j)$.

Cojamos una descomposición de $M$ en componentes isotípicas

$$M = M_{\Lambda_1} \oplus \cdots \oplus M_{\Lambda_t},$$

y sea $\{e_1, \ldots, e_t\}$ el CCIO de $R := \mathrm{End}_A(M)$ correspondiente (ver Ejemplo 1.15). Queremos demostrar que se trata de idempotentes centrales.

Según el Ejercicio 1.32, hemos de ver que $e_i r e_j = 0$ para todo $r \in R$ siempre que $i \neq j$. Tenemos que $\pi_i r \iota_j : M_{\Lambda_j} \to M_{\Lambda_i}$ es un homomorfismo de $A$–módulos. Puesto que $e_i r e_j = \iota_i \pi_i r \iota_j \pi_j$, bastará con que demostremos que si $f : M_{\Lambda_j} \to M_{\Lambda_i}$ es un homomorfismo de $A$–módulos con $i \neq j$, entonces $f = 0$. Pero esto es consecuencia del Ejercicio 1.38.

Deducimos de la Proposición 1.9.6 el isomorfismo de $K$–álgebras

$$R \cong Re_1 \times \cdots \times Re_t.$$

Fijemos $i \in \{1,\dots,t\}$. Puesto que $Re_i = e_iRe_i$, tenemos que la aplicación

$$\varphi : e_iRe_i \to \mathrm{End}_A(M_{\Lambda_i})$$

definida por $\varphi(r) = \pi_i r \iota_i$ tiene por inversa para la composición a la aplicación

$$\rho : \mathrm{End}_A(M_{\Lambda_i}) \to e_iRe_i$$

dada por $\rho(f) = \iota_i f \pi_i$. Es fácil comprobar que $\rho$ es un homomorfismo de $K$–álgebras, así que tenemos que $Re_i \cong \mathrm{End}_A(M_{\Lambda_i})$. Por último, $\mathrm{End}_A(M_{\Lambda_i}) \cong M_{n_i}(\Delta_i)$ por la Proposición 1.9.4. ■

## 1.11 Álgebras semisimples de dimensión finita.

En esta sección, salvo mención en contra, $A$ denotará una $K$–álgebra de dimensión finita como $K$–espacio vectorial[13].

**Definición 1.11.1** Un álgebra $A$ de dimensión finita se dice *semisimple* si todo $A$–módulo de dimensión finita es semisimple.

**Proposición 1.11.1** Un álgebra de dimensión finita $A$ es semisimple si, y sólo si, $A$ es semisimple como $A$–módulo.

*Demostración.* Si $A$ es un álgebra semisimple, entonces, $A$, vista como módulo, es semisimple, por definición. Recíprocamente, sea $M$ un $A$–módulo semisimple finito-dimensional. Entonces $M$ es cociente de un $A$–módulo libre $A^n$. Como $A^n$ es semisimple, se sigue de la Proposición 1.10.3 que $M$ es semisimple. ■

**Corolario 1.11.2** Si $A$ es un álgebra semisimple y su estructura como $A$–módulo es $(\Sigma_1,n_1),\dots,(\Sigma_t,n_t)$, entonces todo $A$–módulo finito-dimensional tiene como estructura $(\Sigma_1,m_1),\cdots,(\Sigma_t,m_t)$, para ciertos enteros no negativos $m_1,\dots,m_t$ (donde entendemos que $m_j = 0$ significa que $\Sigma_j$ no aparece en la estructura del módulo). En particular, todo $A$–módulo simple es isomorfo a uno de los módulos $\Sigma_j$.

*Demostración.* Si $M$ es un módulo de dimensión finita, hemos visto que es isomorfo a un cociente de $A^n$ para algún $n$. Como la estructura del $A$–módulo $A^n$ es $(\Sigma_1,nn_1),\cdots,(\Sigma_t,nn_t)$, el corolario se sigue del Ejercicio 1.40. ■

R Recordemos que nuestros $A$–módulos son siempre $A$–módulos de los llamados **a izquierda**. Veremos más tarde que el álgebra $A$ es semisimple si, y sólo si, el álgebra opuesta $A^{op}$ es semisimple. Esto nos dará que los módulos **a derecha** (es decir, los $A^{op}$–módulos), son semisimples.

[13] la teoría desarrollada aquí puede extenderse a anillos, los anillos llamados semisimples, que no tienen por qué ser álgebras de dimensión finita sobre un cuerpo. Dicha teoría requiere del desarrollo de las nociones de módulo noetheriano y módulo artiniano, que no son objeto de este curso

**Ejemplo 1.16** Sea $D$ una $K$–álgebra de división de dimensión finita, y $A = M_n(D)$ el álgebra de matrices de orden $n$ con coeficientes en $D$. Queremos ver que $A$ es semisimple. Para ello, adoptamos la siguiente notación. Para $i, j \in \{1, \dots, n\}$, sea $E_{ij} \in M_n(D)$ la matriz cuya entrada $(i, j)$–ésima es 1, y toda otra entrada es cero. Es evidente que $\{E_{ij} : 1 \leq i, j \leq n\}$ es una base de $A$ como $D$–espacio vectorial. Además, la multiplicación en $M_n(D)$ está determinada por las reglas

$$aE_{ij}bE_{kl} = \begin{cases} 0 \text{ si } j \neq k \\ abE_{il} \text{ si } j = k \end{cases}, \qquad \text{para todo } a, b \in D$$

Es claro que $\{E_{11}, \dots, E_{nn}\}$ es un CCIO para $A$ (pero ninguno de estos idempotentes es central).

Dado $j \in \{1, \dots, n\}$, sea $A_j$ el $D$–subespacio vectorial de $A$ con base $\{E_{1j}, \dots, E_{nj}\}$. Es fácil comprobar que $A_j$ es un ideal a izquierda de $A$. De hecho, $A_j = AE_{jj}$. Veamos que es simple, comprobando que está generado por cualquiera de sus elementos no nulos (ver Ejercicio 1.17). Sea $0 \neq \mathbf{a} = a_1E_{1j} + \cdots + a_nE_{nj} \in A_j$, entonces $a_i \neq 0$ para algún $i$. Por tanto, $E_{jj} = a_i^{-1}E_{ji}a_iE_{ij} \in A\mathbf{a}$, luego $A\mathbf{a} = AE_{jj} = A_j$.

Por último, es fácil ver que $A = A_1 \oplus \cdots \oplus A_n$, luego $A$ es semisimple. ∎

■ **Ejercicio 1.41** Dada una $K$–álgebra $A$, demostrar que la aplicación $\rho : A \to \mathrm{End}_A(A)^{op}$ definida por $\rho(a)(a') = a'a$ es un isomorfismo de $K$–álgebras.

Profundicemos ahora en la estructura de las álgebras de matrices con coeficientes en álgebras de división son semisimples.

**Proposición 1.11.3** Sea $D$ un álgebra de división finito-dimensional. Entonces $A = M_n(D)$ es un álgebra semisimple tal que todos los $A$–módulos simples son isomorfos entre sí. De hecho, la estructura de $A$ como $A$–módulo semisimple es $(\Sigma, n)$ con $\Sigma$ tal que $D \cong \mathrm{End}_A(\Sigma)^{op}$. Además, el álgebra opuesta $A^{op}$ es isomorfa a $M_n(D^{op})$, por lo que es también semisimple con un único tipo de módulo simple.

*Demostración.* Hemos visto que $A$ es semisimple en el Ejemplo 1.16. Veamos que la estructura de $A$, como $A$–módulo, es $(A_1, n)$. Para ello, basta con que mostremos un isomorfismo de $A$–módulos $f : A_1 \to A_j$ para cada $j = 2, \dots, n$. Definamos

$$f(a_1E_{11} + \cdots + a_nE_{n1}) = a_1E_{1j} + \cdots + a_nE_{nj},$$

donde $a_1, \dots, a_n \in D$. Se trata, obviamente, de un isomorfismo de $D$–espacios vectoriales. El siguiente cálculo muestra que $f$ es un homomorfismo de $A$–módulos:

$$f((\sum_{i,k} a_{ik}E_{ik})\sum_u a_uE_{u1}) = f(\sum_{i,k} a_{ik}a_kE_{i1}) = \sum_{i,k} a_{ik}a_kE_{ij} = (\sum_{i,k} a_{ik}E_{ik})\sum_u a_uE_{uj} = (\sum_{i,k} a_{ik}E_{ik})f(\sum_u a_uE_{u1}).$$

De modo que la estructura de $A$ es $(A_1, n)$.

En vista del Corolario 1.11.2, todo $A$–módulo simple es isomorfo a $A_1$.

Para demostrar la siguiente afirmación, podemos tomar $\Sigma = A_1$. Consideramos la aplicación $\rho : D \to \mathrm{End}_A(A_1)^{op}$ que asigna a cada $d \in D$ la aplicación $D$–lineal $\rho(d)$

determinada[14] por $\rho(d)(E_{i1}) = dE_{i1}$, para $i = 1,\dots,n$. Es fácil ver que $\rho$ es un homomorfismo inyectivo de $K$–álgebras. Para ver que es sobreyectivo, observemos que, de acuerdo con el Ejercicio 1.41, $A$ es isomorfa como $K$–álgebra a $\mathrm{End}_A(A)^{op}$. Por otra parte, sabemos por la Proposición 1.9.4 que $\mathrm{End}_A(A) \cong M_n(\mathrm{End}_A(\Sigma))$. De modo que $\dim_K(A) = n^2 \dim_K(\mathrm{End}_A(\Sigma))$. Como, por otra parte. $\dim_K M_n(D) = n^2 \dim_K(D)$, deducimos que $\dim_K(D) = \dim_K(\mathrm{End}_A(\Sigma))$, con lo que $\rho$ ha de ser sobreyectivo.

La última afirmación se deja como ejercicio (ver Ejercicio 1.42). ■

▪ **Ejercicio 1.42** * Sea $B$ un álgebra. Demostrar que la aplicación que asigna a cada matriz su traspuesta da un isomorfismo de álgebras $M_n(B)^{op} \cong M_n(B^{op})$.

Nos dirigimos ahora a desentrañar la estructura de las álgebras semisimples con un sólo tipo de simple. Necesitamos varios resultados que vamos desarrollando paulatinamente.

**Lema 1.11.4** Si $D$ es una $K$–álgebra de división, entonces $Z(D)$ es un cuerpo. Además, $Z(M_n(D))$ es isomorfo a $Z(D)$. Como consecuencia, el único idempotente central no nulo de $M_n(D)$ es 1.

*Demostración.* Si $0 \neq c \in Z(D)$, entonces, para todo $d \in D$, tenemos que $d = dcc^{-1} = cdc^{-1}$. Por tanto, $c^{-1}d = dc^{-1}$, lo que implica que $c^{-1} \in Z(D)$. ■

▪ **Ejercicio 1.43** Sea $\varphi : R \to S$ un isomorfismo de $K$–álgebras, e $I, J$ ideales a izquierda de $R$. Demostrar que $\varphi(I), \varphi(J)$ son ideales a izquierda de $S$ y que dado cualquier homomorfismo de $R$–módulos $f : I \to J$, la aplicación $\widehat{f} : \varphi(I) \to \varphi(J)$ definida por $\widehat{f}(y) = \varphi f \varphi^{-1}(y)$ para $y \in \varphi(I)$ es un homomorfismo de $S$–módulos.

**Teorema 1.11.5** Un álgebra $A$ es semisimple con un sólo tipo de simple si, y sólo si, $A \cong M_n(D)$ para $D$ una $K$–álgebra de división de dimensión finita. Además, $n$ es único y $D$ es única salvo isomorfismo.

*Demostración.* Si $A \cong M_n(D)$, entonces es semisimple con un sólo tipo de simple por la Proposición 1.11.3.

Recíprocamente, observemos que, por el Ejercicio 1.41, la aplicación $\rho : A \to \mathrm{End}_A(A)^{op}$ definida por $\rho(a)(a') = a'a$ para todo $a, a' \in A$ es un isomorfismo de $K$–álgebras. Si $(\Sigma, n)$ es la estructura de $A$ como $A$–módulo semisimple, entonces, por la Teorema 1.10.5, $\mathrm{End}_A(A) \cong M_n(\Delta)$, donde $\Delta = \mathrm{End}_A(\Sigma)$. Tomando $D = \Delta^{op}$, obtenemos es isomorfismo de álgebras $A \cong M_n(D)$ (ver el Ejercicio 1.42).

Vayamos con la unicidad: supongamos que $B = M_m(D')$ es una $K$–álgebra de matrices isomorfa a $A$, y sea $\varphi : A \to B$ un isomorfismo. Sabemos que

$$A = Re_1 \oplus \cdots \oplus Re_n,$$

para $\{e_1,\dots,e_n\}$ un CCIO tal que todos los $Ae_i$ son simples y $Ae_i \cong Ae_j$ para todos los índices $i, j$. Claramente, $\{\varphi(e_1),\dots,\varphi(e_n)\}$ es un CCIO para $B$.

Por otra parte, si $f : Ae_i \to Ae_j$ es un isomorfismo de $A$–módulos, entonces tenemos un isomorfismo de $B$–módulos $\widehat{f} : B\varphi(e_i) \to B\varphi(e_j)$ por el Ejercicio 1.43. Es también fácil ver que cada $B\varphi(e_i)$ es un $B$–módulo simple. Así que la estructura de $B$ es

[14] esto es, $\rho(d)(\sum_{i=1}^n d_i E_{i1}) = \sum_{i=1}^n d_i dE_{i1}$.

$(B\varphi(e_1),n)$. Por la Proposición 1.11.3, $m=n$ y $D' \cong \mathrm{End}_B(B\varphi(e_1))^{op}$. Pero la aplicación $\mathrm{End}_A(Ae_1) \to \mathrm{End}_B(B\varphi(e_1))$ que lleva $f: Ae_1 \to Ae_1$ en $\widehat{f}: B\varphi(e_1) \to B\varphi(e_1)$ (otra vez usamos el Ejercicio 1.43) es un isomorfismo de $K$–álgebras. Así que $D' \cong \mathrm{End}_B(B\varphi(e_1))^{op} \cong \mathrm{End}_A(Ae_1)^{op} \cong D$, lo que concluye la demostración. ■

**Definición 1.11.2** Una $K$–álgebra de dimensión finita semisimple con un sólo tipo de simple se llamará *simple*.

Junto con el Teorema de Frobenius, la anterior proposición nos permite deducir:

**Corolario 1.11.6** Las álgebras reales simples de dimensión finita son, salvo isomorfismos, $M_n(\mathbb{R}), M_n(\mathbb{C}), M_n(\mathbb{H})$ con $n \geq 1$.

**Corolario 1.11.7** Las álgebras complejas simples de dimensión finita son, salvo isomorfismos, $M_n(\mathbb{C})$ con $n \geq 1$.

Nos disponemos ahora a clasificar las álgebras semisimples. Comenzamos por un ejercicio que usaremos seguidamente.

▪ **Ejercicio 1.44** Sean $R_1,\ldots,R_n$ $K$–álgebras y $R = R_1 \times \cdots \times R_n$. Los ideales por la izquierda de $R$ son de la forma $I_1 \times \cdots \times I_n$, con $I_i$ ideal a izquierda de $R_i$ para $i = 1,\ldots,n$. Análoga descripción tienen los ideales de $R$.

**Teorema 1.11.8 — Wedderburn.** Una $K$–álgebra de dimensión finita $A$ es semisimple si, y sólo si, es isomorfa a un álgebra de la forma

$$M_{n_1}(D_1) \times \cdots \times M_{n_t}(D_t),$$

para $D_1,\ldots,D_t$ álgebras de división de dimensión finita sobre $K$.

Además, los parámetros $(D_1,n_1),\ldots,(D_t,n_t)$ están determinados de manera única, en el sentido de que si se tiene otro isomorfismo de $K$–álgebras

$$A \cong M_{m_1}(D_1') \times \cdots \times M_{m_s}(D_s'),$$

con $D_1',\ldots,D_s'$ álgebras de división, entonces $s=t$ y, tras eventual reordenación, $n_i = m_i$ y $D_i \cong D_i'$ para todo $i = 1,\ldots,t$.

*Demostración.* Veamos primero que $R = M_{n_1}(D_1) \times \cdots \times M_{n_t}(D_t)$ es un álgebra semisimple de dimensión finita, siempre que $D_1,\ldots,D_t$ sean álgebras de división finito-dimensionales. Para ello, tomemos un ideal a izquierda $I$ de $R$, y demostremos que es un sumando directo. Según el Ejercicio 1.44, $I = I_1 \times \cdots \times I_t$, para $I_j$ ideal izquierda de $M_{n_j}(D_j)$ para $j = 1,\ldots,t$. Como cada una de estas álgebras es simple, $I_j \oplus J_j = M_{n_j}(D_j)$ para ciertos ideales izquierda $J_j \leq M_{n_j}(D_j)$ con $j = 1,\ldots t$. Si tomo $J = J_1 \times \cdots \times J_t$, es fácil ver que $R = I \oplus J$. Ahora, si $A \cong R$, entonces se sigue fácilmente que cada ideal izquierda de $A$ es un sumando directo, luego $A$ es semisimple.

Recíprocamente, supongamos que $A$ es un álgebra semisimple y que su estructura como $A$–módulo semisimple es $(\Sigma_1,n_1),\ldots,(\Sigma_t,n_t)$. Sabemos por el Teorema 1.10.5 que $\mathrm{End}_A(A)$ es isomorfa a $R := M_{n_1}(\Delta_1) \times \cdots \times M_{n_t}(\Delta_t)$ para $\Delta_i = \mathrm{End}_A(\Sigma_i)$, $i = 1,\ldots,t$. Por tanto, $A \cong \mathrm{End}_A(A)^{op} \cong M_{n_1}(D_1) \times \cdots \times M_{n_t}(D_t)$, con $D_i = \Delta_i^{op}$ para $i = 1,\ldots,t$.

Para la unicidad, supongamos

$$R = M_{n_1}(D_1) \times \cdots \times M_{n_t}(D_t),$$

y

$$S = M_{m_1}(D'_1) \times \cdots \times M_{m_s}(D'_t),$$

y que hay un isomorfismo de álgebras $\varphi : R \to S$. Sea, para cada $j = 1, \ldots, t$, $e_j \in R$ la $t$–tupla que tiene 0 en todas sus componentes, salvo la $j$–ésima, que vale $1 \in M_{n_j}(D_j)$. Es fácil ver que $\{e_1, \ldots, e_t\}$ es un CCIO centrales de $R$. Además, $Re_j \cong M_{n_j}(D_j)$, isomorfismo de álgebras, para cada $j = 1, \ldots, t$. Como, de acuerdo con el el Lema 1.11.4, $Z(M_{n_j}(D_j)) \cong Z(D_j)$ es un cuerpo, deducimos que $e_j$ es indescomponible. Por tanto, $\{\varphi(e_1), \ldots, \varphi(e_t)\}$ es el CCIO centrales indescomponibles de $S$. Así, $t = s$ y, tras eventual reordenación,

$$M_{n_j}(D_j) \cong Re_j \cong S\varphi(e_j) \cong M_{m_j}(D'_j)$$

para cada $j = 1, \ldots, t$. Por el Teorema 1.11.5, $n_j = m_j$ y $D_j \cong D'_j$, para $j = 1, \ldots, t$. ■

De la demostración del Teorema de Wedderburn, extraemos la siguiente información sobre el centro de un álgebra semisimple.

**Corolario 1.11.9** Si $A$ es una álgebra semisimple de dimensión finita, entonces $Z(A)$ es un producto finito de cuerpos que son extensiones finitas de $K$. El número de factores que aparecen es igual que el número de $A$–módulos simples no isomorfos que aparecen en la estructura de $A$, o también el número de bloques matriciales que aparecen en la estructura de $A$ como producto de álgebras de matrices.

*Demostración.* Seguir atentamente la demostración del Teorema 1.11.8, junto con el hecho de que el centro de un producto de álgebras es isomorfo al producto de los centros de los factores. ■

**Corolario 1.11.10** Si $A$ es un álgebra semisimple de dimensión finita, entonces $A^{op}$ es un álgebra semisimple.

*Demostración.* Por el Teorema de Wedderburn, $A$ es un producto de álgebras de matrices con coeficientes en álgebras de división, lo que implica que $A^{op}$ tiene una estructura similar, cambiando las álgebras de división por sus opuestas. El Teorema de Wedderburn nos da ahora que $A^{op}$ es semisimple. ■

**Corolario 1.11.11 — Molien.** Un álgebra compleja $A$ de dimensión finita es semisimple si, y sólo si, es isomorfa a $M_{n_1}(\mathbb{C}) \times \cdots \times M_{n_t}(\mathbb{C})$. Los números $t$ y $n_1, \ldots, n_t$ son únicos y satisfacen la ecuación

$$\dim_{\mathbb{C}}(A) = n_1^2 + \cdots + n_t^2$$

■ **Ejercicio 1.45** * Sea $A$ un álgebra simple finito-dimensional. Demostrar que $R = M_n(A)$ es un álgebra simple de dimensión finita. Demostrar asimismo que si $\Sigma$ es un $A$–módulo simple y $M$ es un $R$–módulo simple, entonces $\mathrm{End}_A(\Sigma)$ y $\mathrm{End}_R(M)$ son álgebras de división isomorfas.

■ **Ejercicio 1.46** Sea $R$ un anillo y $\{e_1, \ldots, e_m\}$ un CCIO centrales de $R$. Sea $S$ un $R$–módulo simple. Demostrar que existe un único $j \in \{1, \ldots, m\}$ tal que $e_j S \neq \{0\}$. Deducir que, para $s \in S$, se tiene que $e_j s = s$ y $e_i s = 0$ para $i \neq j$.

# 2. Representaciones de Grupos Finitos

En esta segunda parte, vamos a aplicar la teoría desarrollada en la primera para dar una introducción a la teoría de caracteres de un grupo finito. Supondremos conocidas propiedades básicas de los grupos finitos, como las estudiadas en *Álgebra II*.

## 2.1 Representaciones lineales de grupos finitos y módulos

Sea $G$ un grupo finito, $K$ un cuerpo y $V$ un $K$–espacio vectorial de dimensión finita $n$. Sea $GL(V)$ el conjunto de las aplicaciones lineales de $V$ en $V$ que son invertibles. Se trata de un grupo con la operación composición de aplicaciones, de hecho, $GL(V)$ es el grupo de unidades de la $K$–álgebra $\mathrm{End}_K(V)$. A pesar de que $GL(V)$ no suele ser un grupo finito, ha resultado históricamente fructífero representar los elementos de $G$ mediante elementos de $GL(V)$, ya que, para éste, las herramientas del Álgebra Lineal están disponibles.

**Definición 2.1.1** Una *representación $K$–lineal* de $G$ es un homomorfismo de grupos $\Pi : G \to GL(V)$. Llamaremos a $V$ *espacio de representación* y a $n$ *dimensión (o grado) de la representación*. Es útil denotar usar la notación $(V,\Pi)$ para designar a la representación.

R Es obvio que en la definición de representación no parece esencial que $V$ sea de dimensión finita. No obstante, nosotros sólo consideraremos representaciones con espacio de representación finito-dimensional.

**Ejemplo 2.1** Sea $C_n = \{0,1,\ldots,n-1\}$ con su estructura usual de grupo cíclico (o sea, sumo y me quedo con el resto de dividir entre $n$). Consideremos la aplicación $\chi_n : C_n \to \mathbb{C}^\times$ definida por

$$\chi_n(k) = e^{2k\pi i/n} = \cos 2k\pi/n + i \sin 2k\pi/n, \qquad k \in C_n$$

que es un homomorfismo de grupos. Bajo la identificación $\mathbb{C}^\times \cong GL(\mathbb{C})$, $\chi_n$ da una representación compleja de $C_n$ de dimensión 1. Geométricamente, estamos viendo $C_n$ como el grupo de los giros de un polígono regular de $n$ vértices, inserto en el plano complejo, que es el espacio de representación. ■

**Ejemplo 2.2** Para cada $q \in \mathbb{H}$ tal que $||q||^2 = qq^* = 1$, consideremos la aplicación $T_q : V \to V$ dada por $T_q(v) = qvq^*$, donde $V$ es el subespacio vectorial real de $\mathbb{H}$ con base $\{\mathbf{i},\mathbf{j},\mathbf{k}\}$. Que $T_q(v) \in V$ para todo $v \in V$ es consecuencia de que, según vimos en la demostración del Teorema 1.8.2, $V = \{a \in \mathbb{H} : a^2 \leq 0\}$.

Por otra parte, resulta fácil demostrar que $T_q$ es $\mathbb{R}$–lineal y que preserva la norma de $V$, por lo que $T_q \in O(V)$. De hecho, $T_q \in SO(V)$ (es decir, es un giro), lo que no es tan inmediato, pero no es demasiado difícil de ver. En cualquier caso, $T_q \in GL(V)$. Además $T_{pq} = T_p \circ T_q$, para todo $p,q \in \mathbb{H}$ de norma 1.

Consideremos ahora $Q = \{\pm 1, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}$ que es un subgrupo multiplicativo de $\mathbb{H}^\times$ con 8 elementos, llamado *grupo cuaterniónico*. Por todo lo discutido, $T : Q \to GL(V)$, definida por $T(q) = T_q$ para $q \in Q$, proporciona una representación real de $Q$ de grado (o dimensión) 3. ■

■ **Ejercicio 2.1** * Demostrar que $T_q \in SO(V)$ para todo cuaternio $q$ de norma 1.

■ **Ejercicio 2.2** * Calcular explícitamente una representación real no trivial de grado 2 del grupo de permutaciones $S_3$.

Es hora de conectar las representaciones de grupos con los módulos estudiados en la primera parte. El artilugio que lo consigue es el álgebra de grupo, descrita en la siguiente definición.

**Definición 2.1.2** Dado un grupo finito $G$ y un cuerpo $K$, definimos el *álgebra de grupo* $KG$ como sigue. Como $K$–espacio vectorial, $KG$ tiene como base $G$, esto es, los elementos de $KG$ son combinaciones lineales formales de los elementos de $G$. Explícitamente,

$$KG = \{\sum_{g\in G} \lambda_g g : \lambda_g \in K\}$$

La suma de vectores y la acción de los escalares sobre ellos vienen dadas, pues, por

$$(\sum_{g\in G} \lambda_g g) + (\sum_{g\in G} \mu_g g) = \sum_{g\in G} (\lambda_g + \mu_g) g, \quad \alpha(\sum_{g\in G} \lambda_g g) = \sum_{g\in G} (\alpha\lambda_g) g,$$

para $\alpha, \lambda_g, \mu_g \in K$.

Normalmente, los paréntesis no imprescindibles no se escriben. La multiplicación de $KG$ es la aplicación $K$–bilineal que, sobre los vectores de la base, esto es, sobre los elementos de $G$, coincide con la multiplicación de $G$. Explícitamente,

$$(\sum_{g\in G} \lambda_g g)(\sum_{h\in G} \mu_h h) = \sum_{h,g\in G} \lambda_g \mu_h gh$$

■ **Ejercicio 2.3** Comprobar que la multiplicación definida sobre $KG$ es asociativa. Su elemento neutro es $1e$, donde $e$ es el elemento neutro de $G$.

R Normalmente, escribimos $g$ en lugar de $1g$ para cada $g \in G$. En particular, $e$ es el uno de $KG$. Pero también se usa la notación 1 para el uno de $KG$. Así, el uso de las identidades $1 = 1e = e$ es muy extendido, ya que está justificado por el modo de operar en $KG$ como $K$–álgebra que es[1].

**Proposición 2.1.1** Sea $V$ un $K$–espacio vectorial y $G$ un grupo finito. La aplicación que asigna a cada homomorfismo de $K$–álgebras $\Pi : KG \to \mathrm{End}_K(V)$ su restricción $\Pi : G \to GL(V)$ es una biyección sobre el conjunto de las representaciones $K$–lineales de $G$ con espacio de representación $V$. Así, las representaciones $K$–lineales de $G$ con espacio de representación $V$, y las estructuras de $KG$–módulo sobre $V$ están en correspondencia biyectiva.

*Demostración.* Sabemos que las aplicaciones $K$–lineales de $KG$ en $\mathrm{End}_K(V)$ están en correspondencia biyectiva con las aplicaciones de $G$ en $\mathrm{End}_K(V)$, ya que $G$ es una base de $KG$. Puesto que cada elemento de $G$ es una unidad en $KG$, $\Pi(g)$ es una unidad de $\mathrm{End}_K(V)$, esto es, un elemento de $GL(V)$. Como $\Pi$ es multiplicativa, es claro que su restricción a $G$ da un homomorfismo de grupos. Por útimo, es fácil ver que cada homomorfismo de grupos de $G$ en $GL(V)$ determina una aplicación lineal $KG \to \mathrm{End}_K(V)$ que es multiplicativa, por la forma en que hemos definido el producto de $G$. ■

La Proposición 2.1.1 permite trasladar nociones clásicas en el ámbito de las representaciones al formalismo de módulos. La primera es la de subespacio invariante.

**Definición 2.1.3** Sea $(V,\Pi)$ una representación $K$–lineal de un grupo finito $G$. Un subespacio vectorial $W \leq V$ se dice $\Pi$–*invariante* si $\Pi(g)(W) \leq W$ para todo $g \in G$. Equivalentemente, $W$ es un $KG$–submódulo de $V$.

▪ **Ejercicio 2.4** Calcular todos los subespacios invariantes para la representación de $Q$ del Ejemplo 2.2.

▪ **Ejercicio 2.5** Calcular todos los subespacios invariantes para la representación de $S_3$ del Ejercicio 2.2.

**Definición 2.1.4** Una representación $K$–lineal de un grupo finito $G$ se dice *irreducible* si su espacio de representación es no nulo y sus únicos subespacios invariantes son $\{0\}$ y el total. Equivalentemente, el $KG$–módulo correspondiente es simple.

**Ejemplo 2.3** La representación compleja de $C_n$ dada en el Ejemplo 2.1 es irreducible, obviamente. ▪

## 2.2 Representaciones completamente reducibles. Teorema de Maschke.

Vamos a demostrar que, si el cuerpo $K$ es adecuado, entonces cualquier espacio de representación de un grupo finito $G$ se descompone como suma directa de subespacios invariantes irreducibles. Por $|G|$ denotaremos el orden de $G$, es decir, su cardinal como conjunto.

[1] Concretamente, el homomorfismo de anillos $K \to KG$ que lleva $\alpha \in K$ en $\alpha e$ es el que dota a $KG$ de estructura de $K$–álgebra

**Definición 2.2.1** Una representación $K$–lineal $(V,\Pi)$ de un grupo finito $G$ se dice *completamente reducible* si, o bien $V=\{0\}$, o $V$ es suma directa de subespacios invariantes irreducibles. Equivalentemente, el $KG$–módulo correspondiente es semisimple.

**Teorema 2.2.1 — Maschke.** Sea $G$ un grupo finito y $K$ un cuerpo cuya característica no divide al orden de $G$. Entonces toda representación $K$–lineal de $G$ es completamente reducible. En otras palabras, $KG$ es un álgebra semisimple.

*Demostración.* Vamos a demostrar primero que, si $M,N$ son $KG$–módulos, y $f:M\to N$ es una aplicación $K$–lineal, entonces la aplicación $\tilde{f}:M\to N$ definida por

$$\tilde{f}(v)=\frac{1}{|G|}\sum_{g\in G} gf(g^{-1}v), \qquad (v\in M)$$

es un homomorfismo de $KG$–módulos. Observemos que $|G|\neq 0$ en $K$, ya que la característica de $K$ no divide a $|G|$. Es fácil comprobar que $\tilde{f}$ es $K$–lineal. De aquí, será $KG$–lineal en cuanto demostremos que $\tilde{f}(hv)=h\tilde{f}(v)$ para todo $h\in G$ y todo $v\in M$. Esto se comprueba en el siguiente cálculo:

$$\tilde{f}(hv)=\frac{1}{|G|}\sum_{g\in G} gf(g^{-1}hv)=\frac{1}{|G|}\sum_{g\in G} hh^{-1}gf(g^{-1}hv)=$$
$$h\frac{1}{|G|}\sum_{g\in G} h^{-1}gf(g^{-1}hv)=h\frac{1}{|G|}\sum_{k\in G} kf(k^{-1}v)=h\tilde{f}(v),$$

donde, en la penúltima igualdad, hemos usado que la aplicación de $G$ en $G$ dada por $g\mapsto k=h^{-1}g$ es una biyección.

Supongamos ahora un $KG$–módulo $V$ y $W\leq V$ un $KG$–submódulo. Hemos de demostrar que $W$ es un sumando directo de $V$ como $KG$–submódulo. Para ello, consideremos la proyección canónica $\pi:V\to V/W$, y tomemos $\varphi:V/W\to V$ una aplicación $K$–lineal tal que $\pi\circ\varphi=id_{V/W}$ (esto se hace con ayuda de un complemento de $W$ en $V$ como $K$–espacio vectorial). Sea $\tilde{\varphi}:V/W\to V$ la aplicación $KG$–lineal construida según hemos visto a partir de $\varphi$. Dado $x\in V/W$, realizamos en siguiente cálculo:

$$\pi(\tilde{\varphi}(x))=\pi(\frac{1}{|G|}\sum_{g\in G} g\varphi(g^{-1}x))=\frac{1}{|G|}\sum_{g\in G} g\pi(\varphi(g^{-1}x))=\frac{1}{|G|}\sum_{g\in G} gg^{-1}x=x$$

Así que $\pi\circ\tilde{\varphi}=id_{V/W}$.

Pongamos $U=\mathrm{Im}\tilde{\varphi}$, que es un $KG$–submódulo de $V$ isomorfo a $V/W$ (ya que $\tilde{\varphi}$ es obviamente inyectiva). Si $v\in W\cap U$, entonces $v=\tilde{\varphi}(x)$ para algún $x\in V/W$. Pero, con esto, $0=\pi(v)=\pi(\tilde{\varphi}(x))=x$, lo que implica que $v=\tilde{\varphi}(x)=0$. Luego $W\cap U=\{0\}$. Como $\dim_K U=\dim_K V/W=\dim_K V-\dim_K W$, concluimos que $V=W\oplus U$.

Hemos demostrado, pues, que todo $KG$–submódulo de $V$ es un sumando directo, como queríamos. ■

La siguiente es una terminología clásica para representaciones lineales de grupos.

**Definición 2.2.2** Dos representaciones $K$–lineales de un grupo $G$ se llaman *equivalentes* si los $KG$–módulos correspondientes son isomorfos.

Supongamos que la característica de $K$ no divide al orden de $G$. Según el Teorema de Maschke, $KG$ es un álgebra semisimple. Traduzcamos al lenguaje de representaciones lo que conocemos sobre $KG$–módulos.

Bien, la propia álgebra $KG$ da una representación llamada *representación regular* $K$–lineal de $G$, y la denotamos por $\rho_{reg}$. Por el Corolario 1.11.2, hay, salvo equivalencias, un número finito de representaciones $K$–lineales irreducibles de $G$, digamos $(V_1,\rho_1),\dots,(V_t,\rho_t)$. La representación regular $\rho_{reg}$ es equivalente, por el Corolario 1.11.2, a una suma directa de estas representaciones irreducibles (entendemos suma directa de representaciones a la representación dada por la suma directa de los módulos correspondientes). Brevemente, diremos que $\rho_{reg}$ es equivalente a $\rho_1^{n_1}\oplus\cdots\oplus\rho_t^{n_t}$, donde cada $n_i$ denota en número de copias del módulo simple correspondiente a $(V_i,\rho_i)$ en la descomposición de $KG$ como suma directa de simples. Aplicando estas ideas a cualquier representación $(V,\rho)$, obtenemos que

$$\rho \sim \rho_1^{m_1}\oplus\cdots\oplus\rho_t^{m_t} \tag{2.1}$$

para ciertos $m_i \geq 0$. A $m_i$ se le llama *multiplicidad de* $\rho_i$ *en* $\rho$, bien entendido que si $m_i = 0$, entonces $\rho_i$ no aparece en la descomposición (2.1). Estas multiplicidades determinan $\rho$ salvo equivalencias, como consecuencia de la Proposición 1.10.4. Si $m_i \geq 1$, diremos que $\rho_i$ es una *constituyente* de $\rho$.

Por otra parte, el Teorema de Wedderburn nos da que $KG$ es una $K$–álgebra isomorfa a $M_{n_1}(D_1)\times\cdots\times M_{n_t}(D_t)$, donde $D_1,\dots,D_t$ nos álgebras de división de dimensión finita sobre $K$. Pongamos $d_i = \dim_K(D_i)$ para $i = 1,\dots,t$.

**Proposición 2.2.2** Supongamos que la característica de $K$ no divide a $|G|$. Sean

$$(V_1,\rho_1),\dots,(V_t,\rho_t)$$

las representaciones $K$–lineales irreducibles de $G$, y supongamos que $n_i$ es la multiplicidad de $\rho_i$ en la representación regular, para $i = 1,\dots,t$. Entonces $\dim_K V_i = d_i n_i$ para $i = 1,\dots,t$. Además, $|G| = d_1 n_1^2 + \cdots + d_t n_t^2$.

*Demostración.* En la descomposición de Wedderburn de $KG$ como producto de álgebras de matrices, el módulo correspondiente a $(V_i,\rho_i)$ aparece como el ideal a izquierda de $M_{n_i}(D_i)$ dado por las “matrices primera columna". En tanto que $K$–espacio vectorial tenemos, pues, que $V_i$ es isomorfo a la suma directa de $n_i$ copias de $D_i$, de donde $\dim_K(V_i) = n_i d_i$. La segunda igualdad se deduce inmediatamente del Teorema de Wedderburn. ■

**Corolario 2.2.3** Sean $(V_1,\rho_1),\dots,(V_t,\rho_t)$ las representaciones irreducibles complejas de $G$, con multiplicidades $(n_1,\dots,n_t)$ en la representación regular. Entonces $\dim_{\mathbb{C}} V_i = n_i$ para $i = 1,\dots,t$ y $|G| = n_1^2 + \cdots + n_t^2$.

■ **Ejercicio 2.6** Deducir del Corolario 2.2.3 cuántas representaciones irreducibles complejas no equivalentes tiene $S_3$, y cuáles son sus dimensiones. Calcularlas explícitamente.

■ **Ejercicio 2.7** Deducir del Corolario 2.2.3 cuántas representaciones irreducibles complejas no equivalentes tiene $Q$, y cuáles son sus dimensiones. Calcularlas explítamente.

Continuemos extrayendo información sobre las representaciones irreducibles de un grupo a partir del álgebra de grupo. Concretamente, vamos a ver que existe una estrecha relación entre las clases de conjugación del grupo finito y sus representaciones irreducibles.

**Proposición 2.2.4** Sean $\mathscr{C}_1,\dots,\mathscr{C}_r$ las clases de conjugación de $G$. Entonces

$$\dim_K Z(KG) = r.$$

*Demostración.* Fijemos, para cada $i = 1,\dots,r$, $g_i \in \mathscr{C}_i$ un representante de la clase de conjugación. Si $c = \sum_{g\in G}\lambda_g g \in Z(KG)$, entonces, para cada $h \in G$, tenemos que $h\sum_{g\in G}\lambda_g g = (\sum_{g\in G}\lambda_g g)h$ o, equivalentemente,

$$\sum_{g\in G}\lambda_g hgh^{-1} = \sum_{g\in G}\lambda_g g.$$

Observemos que la aplicación $g \mapsto hgh^{-1}$ es una biyección, por lo que podemos reescribir la anterior igualdad como

$$\sum_{g\in G}\lambda_{h^{-1}gh} g = \sum_{g\in G}\lambda_g g.$$

Igualando coeficientes, $\lambda_{h^{-1}gh} = \lambda_g$ para todo $h \in G$. Por tanto, los coeficientes $\lambda_g$ son constantes sobre las clases de conjugación. Así, si ponemos $c_i = \sum_{g\in\mathscr{C}_i} g$ para cada $i = 1,\dots,r$, tenemos que $c = \sum_{i=1}^{r}\lambda_{g_i}c_i$, y que $c_1,\dots,c_r$ son, evidentemente, $K$–linealmente independientes. Es claro, por otra parte, que $c_i \in Z(KG)$ para todo $i = 1,\dots,r$. Por tanto, $\{c_1,\dots,c_r\}$ es una $K$–base de $Z(KG)$, lo que concluye la prueba. ■

**Corolario 2.2.5** El número de clases de conjugación de $G$ coincide con el número de representaciones irreducibles complejas de $G$.

*Demostración.* Por la Proposición 2.2.4, si $r$ es el número de clases de conjugación de $G$, entonces $r = \dim_{\mathbb{C}} Z(\mathbb{C}G)$. Por otra parte, por el Corolario 1.11.11, tenemos $Z(\mathbb{C}G) \cong \mathbb{C}^t$, donde $t$ es el número de módulos simples no isomorfos sobre $\mathbb{C}G$. Así que $r = t$, que es lo afirmado en el enunciado. ■

**Ejemplo 2.4** Recordemos[a] que cada elemento del grupo simétrico $S_n$ se descompone de manera única, salvo orden de los factores, como producto de ciclos disjuntos. Por otra parte, dos permutaciones en $S_n$ son conjugadas si, y sólo si, sus descomposiciones como producto de ciclos disjuntos tienen la misma estructura. Así, el número de clases de conjugación de $S_n$ coincide con el número de particiones de $n$, esto es, las formas de descomponer $n$ como suma de naturales (no nulos).

Por ejemplo, para $S_3$ tenemos que $3 = 1+1+1$, que corresponde claramente a la clase de conjugación $Cl((1)) = \{(1)\}$, $3 = 2+1$, que corresponde a la clase de conjugación $Cl((1,2)) = \{(12),(13),(2,3)\}$, y $3 = 3$, para la clase de conjugación $Cl((123)) = \{(123),(132)\}$.

Para $S_4$, tenemos las clases cinco clases de conjugación

$$Cl((1)), Cl((12)), Cl((123)), Cl((1234)), Cl((12)(34)).$$

Por tanto, $S_4$ tiene 5 representaciones irreducibles complejas. ■

[a] De Álgebra II

■ **Ejercicio 2.8** Sea $H$ un subgrupo normal de $G$ y $\pi : G \to G/H$ la proyección canónica. Demostrar que $(V,\rho)$ es una representación irreducible de $G/H$ si, y sólo si, $(V,\rho\pi)$ es una representación irreducible de $G$.

## 2.3 Caracteres

Aunque parte de la teoría de caracteres (definiciones más abajo) puede desarrollarse sobre un cuerpo general, los resultados clásicos se obtienen para caracteres complejos. A partir de este momento, trabajaremos con representaciones complejas. Seguimos denotando por $G$ a un grupo finito.

**Definición 2.3.1** Sea $(V,\rho)$ una representación compleja de $G$. La aplicación $\chi_\rho : G \to \mathbb{C}$ definida por $\chi_\rho(g) = tr(\rho(g))$ para $g \in G$ se llama *carácter complejo proporcionado por* $\rho$. Cuando $\rho$ es irreducible, diremos que el carácter $\chi_\rho$ es irreducible. El grado del carácter $\chi_\rho$ es el grado de $\rho$, esto es, la dimensión de $V$ como espacio vectorial complejo. Se denotará por $\deg \chi_\rho$.

**Lema 2.3.1** Dos representaciones complejas equivalentes de $G$ proporcionan el mismo carácter.

*Demostración.* Sean $(V,\rho)$, $(W,\pi)$ representaciones complejas de $G$, y $T : V \to W$ un isomorfismo de $\mathbb{C}G$–módulos. Entonces, para cada $g \in G$, tenemos que $T\rho(g) = \pi(g)T$, para todo $g \in G$. Esto es, $\rho(g) = T^{-1}\pi(g)T$, lo que implica que

$$tr\rho(g) = trT^{-1}\pi(g)T = tr\pi(g),$$

para todo $g \in G$. ■

Uno de los objetivos que perseguimos es demostrar que dos representaciones complejas que proporcionan el mismo carácter han de ser equivalentes.

**Proposición 2.3.2** Sea $G$ un grupo finito, $g \in G$ y $m \geq 1$ tal que $g^m = 1$. Consideremos una representación compleja $(V,\rho)$ de grado $n$ de $G$. Entonces existen raíces $m$–ésimas de la unidad $\omega_1,\ldots,\omega_n \in \mathbb{C}$ (pueden repetirse) tales que $\rho(g)$ diagonaliza completamente con valores propios $\omega_1,\ldots,\omega_n$. Como consecuencia,

$$\chi_\rho(g) = \omega_1 + \cdots + \omega_n,$$

y

$$\chi_\rho(g^{-1}) = \overline{\chi_\rho(g)}.$$

*Demostración.* El endomorfismo $\mathbb{C}$–lineal $\rho(g) : V \to V$ verifica que $\rho(g)^m = \rho(g^m) = \rho(1) = id_V$, así que su polinomio mínimo $p(X)$ en $\mathbb{C}[X]$ es un divisor de $X^m - 1$. Por tanto, todas las raíces complejas de $p(X)$ son simples, y $p(X)$ factoriza en $\mathbb{C}[X]$ como un producto de factores lineales distintos[2]. Eso significa, por el Teorema Chino del Resto,

[2] El resto del argumento persigue demostrar que $\rho(g)$ es diagonalizable, con valores propios dados por raíces de $p(X)$. Esto es inmediato para los alumnos que hayan estudiado Álgebra Lineal a nivel de un grado estándar en Matemáticas, como se hace en muchas universidades. Aquí damos un argumento alternativo para los alumnos cuya formación en este campo resulte insuficiente.

que el anillo $B := \mathbb{C}[X]/\langle p(X)\rangle$ es isomorfo a un producto directo finito de copias de $\mathbb{C}$. En otras palabras, $B$ es un álgebra compleja conmutativa semisimple, y cada $B$–módulo simple ha de tener dimensión 1 como $\mathbb{C}$–espacio vectorial. Por tanto, el $B$–módulo $V$ proporcionado por la acción de $\rho(g)$ es semisimple y, así, $V = V_1 \oplus \cdots \oplus V_n$, donde $V_i$ es un $B$–submódulo de dimensión 1 sobre $\mathbb{C}$.

Si $v_i \in V_i$ es no nulo, entonces $\rho(g)(v_i) = Xv_i = \omega_i v_i$, para cierto $\omega_i \in \mathbb{C}$. Además, $v_i = \rho(g)^m(v_i) = \omega_i^m v_i$, de donde cada $\omega_i$ es una raíz $m$–ésima de la unidad. Esto significa que el endomorfismo $\rho(g)$ es diagonalizable y sus valores propios son $\omega_1, \ldots, \omega_n$.

Por último, $\rho(g^{-1}) = \rho(g)^{-1}$, por lo que $\rho(g^{-1})$ es diagonalizable con valores propios $\overline{\omega}_1, \ldots, \overline{\omega}_n$. Por tanto, $\chi_\rho(g^{-1}) = \overline{\chi_\rho(g)}$. ■

**Proposición 2.3.3** Sea $G$ un grupo finito y $(V, \rho)$ una representación compleja de $G$. Dado $g \in G$, y $m \geq 1$ tal que $g^m = 1$, se tiene que

$$|\chi_\rho(g)| \leq \deg \chi_\rho.$$

Además, $|\chi_\rho(g)| = \deg \chi_\rho$ si, y sólo si, $\rho(g) = \omega\, id_V$, para $\omega$ una raíz $m$–ésima de la unidad. En particular, $\chi_\rho(g) = \deg \chi_\rho$ si, y sólo si, $\rho(g) = id_V$.

*Demostración.* Según la Proposición 2.3.2, $\chi_\rho(g) = \sum_{i=1}^n \omega_i$, para $n = \deg \chi_\rho$ y $\omega_1, \ldots, \omega_n \in \mathbb{C}$ raíces $m$–ésimas de la unidad. La desigualdad triangular da entonces

$$|\chi_\rho(g)| = |\sum_{i=1}^n \omega_i| \leq \sum_{i=1}^n |\omega_i| = n \tag{2.2}$$

Además, se da la igualdad en (2.2) si, y sólo si, $\omega_1, \ldots, \omega_n$ son múltiplos positivos reales unos de otros. Estando todos sobre la circunferencia de radio 1, esto sólo es posible si son iguales. Según la Proposición 2.3.2, esto es equivalente a tener $\rho(g) = \omega\, id_V$ para $\omega$ el valor común de todos los $\omega_i$. ■

**Definición 2.3.2** Dado un carácter complejo $\chi$ de $G$, definimos

$$Ker\chi = \{g \in G : \chi(g) = \chi(1)\}.$$

**Corolario 2.3.4** Si $\chi$ es un carácter complejo de $G$, entonces $Ker\chi$ es un subgrupo normal de $G$.

*Demostración.* Tenemos que $\chi = \chi_\rho$ para una representación $\rho$ de $G$. Además, $\deg \chi = \chi(1)$. Por la Proposición 2.3.3, $Ker\chi_\rho = Ker\rho$, que es un subgrupo normal de $G$, ya que $\rho$ es un homomorfismo de grupos. ■

En lo que sigue, usaremos la siguiente notación. Dada una representación $(V, \rho)$ de $G$, por $\widetilde{\rho} : \mathbb{C}G \to \mathrm{End}_{\mathbb{C}}(V)$ denotaremos su estructura de $\mathbb{C}G$–módulo correspondiente. Por otra parte, si $\chi_\rho$ es el carácter complejo proporcionado por $\rho$, entonces denotaremos por $\widetilde{\chi_\rho} : \mathbb{C}G \to \mathbb{C}$ a la forma lineal determinada por $\chi_\rho : G \to \mathbb{C}$.

▪ **Ejercicio 2.9** Demostrar que, para todo $a \in \mathbb{C}G$, se tiene que $\widetilde{\chi_\rho}(a) = tr\widetilde{\rho}(a)$.

Recordemos que, por el Teorema de Maschke, $A = \mathbb{C}G$ es un álgebra semisimple compleja y que, si $\{e_1, \ldots, e_t\}$ es un CCIO centrales indescomponibles, entonces $A = Ae_1 \oplus \cdots \oplus Ae_t$, donde cada $Ae_i$ es, como álgebra, isomorfa a un álgebra de matrices $M_{n_i}(\mathbb{C})$. La segunda afirmación viene garantizada por el Teorema de Wedderburn-Molien, que viene siendo onmipresente.

Además, en tanto que $A$–módulo, $Ae_i$ es suma de $n_i$ submódulos simples isomorfos entre sí, cada uno de ellos de dimensión exactamente $n_i$. Estos $A$–módulos simples dan (salvo equivalencias) el conjunto de representaciones complejas $(V_1, \rho_1), \ldots, (V_t, \rho_t)$. Observemos que, dado $j$, si $v_j \in V_j$, tenemos que $e_j v_j = v_j$ y $e_i v_j = 0$ si $i \neq j$ (ver Ejercicio 1.46).

Los caracteres de las representaciones

$$(V_1, \rho_1), \ldots, (V_t, \rho_t),$$

que denotaremos por

$$\chi_1, \ldots, \chi_t,$$

son llamados *caracteres irreducibles complejos* de $G$, y jugarán un papel prominente. Recordemos, por último, que $t$ coincide con el número de clases de conjugación de $G$, ver Corolario 2.2.5. Observemos que $n_i = \dim_{\mathbb{C}} V_i = \chi_i(1)$ para $i = 1, \ldots, t$.

**Lema 2.3.5** Supongamos que $(W, \pi)$ es una representación de $G$, y que $W = W_1 \oplus \cdots \oplus W_m$ como $\mathbb{C}G$–módulos. Denotemos por $\pi_i$ la representación dada por el $\mathbb{C}G$–módulo $W_i$. Entonces

$$\chi_\pi = \chi_{\pi_1} + \cdots + \chi_{\pi_m}.$$

*Demostración.* Si tomamos una base $B_i$ de cada $W_i$, entonces $B = B_1 \cup \cdots \cup B_m$ es una base de $W$. Dado $g \in G$, la matriz de $\pi(g)$ con respecto de $B$ es una matriz diagonal por bloques, siendo éstos las matrices de $\pi_i(g)$ con respecto de $B_i$. De donde se sigue el resultado. ■

El $\mathbb{C}G$–módulo regular da una representación de $G$, llamada representación regular, cuyo carácter, que denotaremos por $\chi_{reg}$, se llama *carácter regular*.

**Lema 2.3.6**

1. $\chi_{reg}(g) = \begin{cases} |G|, \text{ si } g = 1 \\ 0, \text{ si } g \neq 1 \end{cases}$
2. $\chi_{reg} = \chi_1(1)\chi_1 + \cdots + \chi_t(1)\chi_t$

*Demostración.* 1. Basta con que pensemos que la representación regular $\rho_{reg}$ transforma cada $g \in G$ en el endomorfismo $\rho_{reg}(g) : \mathbb{C}G \to \mathbb{C}G$ que multiplica cada elemento de la base $G$ por $g$. De modo que, salvo si $g = 1$, $\rho_{reg}(g)$ permuta todos los elementos de $G$ sin dejar uno invariante. La matriz de $\rho_{reg}(g)$ tendrá, pues, sólo ceros en su diagonal principal. Para $g = 1$, $\rho_{reg}(1) = id_{\mathbb{C}G}$.
2. Se sigue del Teorema de Wedderburn, junto con el Lema 2.3.5. ■

**Proposición 2.3.7** Sea $\{e_1, \ldots, e_t\}$ el CCIO centrales indescomponibles de $\mathbb{C}G$. Entonces, para cada $i = 1, \ldots, t$,

$$e_i = \frac{1}{|G|} \sum_{g \in G} \chi_i(1)\overline{\chi_i(g)}g$$

*Demostración.* Pongamos $e_i = \sum_{g\in G} \alpha_g g$, y tratemos de calcular los coeficientes $\alpha_g \in \mathbb{C}$. Dado $g \in G$, tenemos que $e_i g^{-1} = \sum_{h\in G} \alpha_h h g^{-1}$. De donde

$$\widetilde{\chi_{reg}}(e_i g^{-1}) = \sum_{h\in G} \alpha_h \widetilde{\chi_{reg}}(hg^{-1}) = \alpha_g |G|,$$

donde, en la última igualdad, hemos usado el apartado 1 del Lema 2.3.6. Su apartado segundo da

$$\alpha_g |G| = \chi_1(1)\widetilde{\chi}_1(e_i g^{-1}) + \cdots + \chi_t(1)\widetilde{\chi}_t(e_i g^{-1})$$

Por el Ejercicio 2.9, tenemos que

$$\widetilde{\chi}_j(e_i g^{-1}) = tr(\widetilde{\rho}_j(e_i g^{-1})).$$

Recordemos que $\widetilde{\rho}_j(e_i g^{-1})(v_j) = e_i g^{-1} v_j = g^{-1} e_i v_j$ para todo $v_j \in V_j$. Así, si $j \neq i$, tenemos que $g^{-1} e_i v_j = 0$, en tanto que $g^{-1} e_i v_j = g^{-1} v_j$ si $j = i$. Por tanto,

$$\widetilde{\rho}_j(e_i g^{-1}) = \begin{cases} 0, & \text{si } j \neq i \\ \widetilde{\rho}_i(g^{-1}) & \text{si } j = i. \end{cases}$$

Tomando trazas,

$$\widetilde{\chi}_j(e_i g^{-1}) = \begin{cases} 0, \text{ si } j \neq i \\ \chi_i(g^{-1}), \text{ si } j = i \end{cases}$$

Por tanto,

$$\alpha_g |G| = \chi_i(1)\chi_i(g^{-1}),$$

de donde

$$e_i = \frac{1}{|G|} \sum_{g\in G} \chi_i(1)\overline{\chi_i(g)} g.$$

■

Las identidades demostradas en el siguiente teorema se llaman *relaciones de ortogonalidad.*

**Teorema 2.3.8** Sean $\chi_1, \ldots, \chi_t$ los caracteres irreducibles complejos de un grupo finito $G$. Entonces, para $i = 1, \ldots, t$,

$$\sum_{g\in G} \overline{\chi_i(g)}\chi_j(g) = 0, \text{ si } i \neq j, \tag{2.3}$$

y

$$\sum_{g\in G} |\chi_i(g)|^2 = |G|. \tag{2.4}$$

*Demostración.* Con la notación de la Proposición 2.3.7, tenemos, para $i, j = 1, \ldots, t$,

$$e_i e_j = \frac{1}{|G|^2} \sum_{g,h\in G} \chi_i(1)\overline{\chi_i(g)}\chi_j(1)\overline{\chi_j(h)} gh. \tag{2.5}$$

Pero $e_i e_j = \delta_{ij} e_i$, donde $\delta_{ij}$ es la delta de Kronecker. De nuevo por la Proposición 2.3.7,

$$\delta_{ij} e_i = \frac{\delta_{ij}}{|G|} \sum_{g \in G} \chi_i(1) \overline{\chi_i(g)} g. \tag{2.6}$$

Igualando los coeficientes de $1 \in G$ en (2.5) y (2.6), obtenemos

$$\frac{1}{|G|} \sum_{g \in G} \overline{\chi_i(g)} \chi_j(1) \overline{\chi_j(g^{-1})} = \delta_{ij} \overline{\chi_i(1)},$$

de donde

$$\chi_j(1) \sum_{g \in G} \overline{\chi_i(g)} \chi_j(g) = \delta_{ij} |G| \chi_i(1).$$

Si $i \neq j$, obtenemos (2.3), ya que $\chi_j(1) \neq 0$, en tanto que si $i = j$, deducimos (2.4) simplificando $\chi_i(1)$. ■

▪ **Ejercicio 2.10** Demostrar que todo carácter de un grupo finito $G$ es constante sobre cada clase de conjugación de $G$.

## 2.4 La tabla de caracteres

Sea $G$ un grupo finito, con clases de conjugación $\mathscr{C}_1, \ldots, \mathscr{C}_t$. Sean $\chi_1, \ldots, \chi_t$ los caracteres irreducibles complejos de $G$. Sabemos que dichos caracteres son constantes sobre las clases de conjugación de $G$. Concretamente, si para cada $i = 1, \ldots, t$ llamamos $\chi_{ij}$ al valor de $\chi_i$ sobre $\mathscr{C}_j$, para $j = 1, \ldots, t$, entonces estos valores determinan completamente $\chi_i$. Podemos construir la *matriz de caracteres* $X = (\chi_{ij})$ que describe de manera compacta los caracteres irreducibles complejos de $G$. Esta información se presenta usualmente mediante la *tabla de caracteres*:

| | $h_1$ | $\cdots$ | $h_t$ |
|---|---|---|---|
| $G$ | $\mathscr{C}_1$ | $\cdots$ | $\mathscr{C}_t$ |
| $\chi_1$ | $\chi_{11}$ | $\cdots$ | $\chi_{1t}$ |
| $\vdots$ | $\vdots$ | | $\vdots$ |
| $\chi_t$ | $\chi_{t1}$ | $\cdots$ | $\chi_{tt}$ |

donde $h_i$ es el cardinal de $\mathscr{C}_i$ para $i = 1, \ldots, t$. Es frecuente escribir en la tabla de caracteres un elemento de $\mathscr{C}_i$ como etiqueta de la propia clase de conjugación.

▪ **Ejercicio 2.11** Calcular la tabla de caracteres del grupo cíclico $C_4$.

**Teorema 2.4.1 — Frobenius.** Sean $\mathscr{C}_1, \ldots, \mathscr{C}_t$ las clases de conjugación de un grupo finito $G$, y pongamos $h_i = |\mathscr{C}_i|$, para $i = 1, \ldots, t$. Sean $\chi_1, \ldots, \chi_t$ los caracteres irreducibles de $G$, y sea $\chi_{ij}$ el valor que toma $\chi_i$ sobre la clase de conjugación $\mathscr{C}_j$, para $i, j = 1, \ldots, t$. Entonces

1. $\sum_{k=1}^{t} h_k \overline{\chi_{ik}} \chi_{jk} = \delta_{ij} |G|$, para todo $i, j = 1, \ldots, t$.
2. $\sum_{i=1}^{t} \chi_{ij} \overline{\chi_{ik}} = \frac{|G|}{h_k} \delta_{jk}$, para todo $j, k = 1, \ldots, t$.

*Demostración.* El conjunto de igualdades del primer apartado se deduce fácilmente del Teorema 2.3.8.

Para demostrar el segundo apartado, tomemos las matrices $X = (\chi_{ij})$ y $H = diag(h_1, \ldots, h_t)$. Las igualdades de la afirmación 1 se escriben entonces como

$$\overline{X} H X^T = |G| I_t.$$

De modo que la matriz inversa de $X^T$ es $|G|^{-1}\overline{X}H$. Por tanto, $|G|^{-1} X^T \overline{X} H = I_t$. De donde

$$X^T \overline{X} = |G| H^{-1}.$$

La anterior igualdad de matrices es equivalente a la afirmación 2. ■

**Ejemplo 2.5** Vamos a calcular la tabla de caracteres de $S_3$. Las clases de conjugación de $S_3$ tienen como representantes $(1), (12), (123)$, cuyos cardinales son 1, 3 y 2, respectivamente. Por tanto, $S_3$ tiene tres caracteres complejos irreducibles, llamémosle $\chi_1, \chi_2, \chi_3$. Como es costumbre, $\chi_1$ será el carácter trivial, correspondiente a la representación irreducible trivial, que manda todo elemento de $S_3$ al número complejo 1. Esto completa la primera fila de la tabla de caracteres.

La segunda fila está proporcionada por la representación irreducible que asigna a cada permutación su signatura. Para la última fila, notemos primero que $\chi_3(1)$ ha de ser la dimensión de la representación irreducible restante, y ha de verificarse que $1 + 1 + \chi_{31}^2 = 6$. Por tanto, $\chi_{31} = 2$. Por último, de la relaciones de ortogonalidad entre la fila tercera, y la primera y segunda, respectivamente, obtenemos las ecuaciones

$$\begin{aligned} 2 + 3\chi_{32} + 2\chi_{33} &= 0 \\ 2 - 3\chi_{32} + 2\chi_{33} &= 0, \end{aligned}$$

cuya solución simultánea completa la tercera fila de la tabla de caracteres de $S_3$.

| | 1 | 3 | 2 |
|---|---|---|---|
| $S_3$ | $(1)$ | $(12)$ | $(123)$ |
| $\chi_1$ | 1 | 1 | 1 |
| $\chi_2$ | 1 | -1 | 1 |
| $\chi_3$ | 2 | 0 | -1 |

■

**Ejemplo 2.6** Queremos calcular la tabla de caracteres de $S_4$. De nuevo comenzamos con la descripción de sus clases de conjugación, y sus tamaños, consignados en la tabla de caracteres parcialmente llena más abajo.

La primera fila en la misma corresponde el carácter trivial, en tanto que la segunda se construye a partir del carácter irreducible dado por la representación que asigna a cada permutación su signo.

Para el carácter $\chi_3$ nos vamos a apoyar en el Ejercicio 2.8. Para ello, consideremos el subgrupo $V = \{(1), (12)(34), (13)(24), (14)(23)\}$ de $S_4$. Como $V$ es unión de dos clases de conjugación de $S_4$, deducimos que se trata de un subgrupo normal de $S_4$.

Ahora consideremos el homomorfismo de grupos dado por la composición

$$S_3 \xrightarrow{\iota} S_4 \xrightarrow{\pi} S_4/V,$$

donde $\pi$ es la proyección canónica, e $\iota$ es el encaje de $S_3$ como las permutaciones de $S_4$ que dejan fijo el símbolo 4. El núcleo de $\pi\iota$ es $S_3 \cap V = \{(1)\}$, luego $\pi\iota$ es una aplicación inyectiva. Como tanto $S_3$ como $S_4/V$ tienen 6 elementos, deducimos que $\pi\iota$ es biyectiva y, así, es un isomorfismo de grupos. La representación irreducible de grado 2 de $S_3$, llamémosla $\rho$, proporciona, en virtud del Ejercicio 2.8, una representación irreducible de $S_4$, y, por tanto, el carácter $\chi_3$. Calculemos formalmente $\chi_3((1234))$ con esta idea:

$$\chi_3((1234)) = tr(\rho(\pi\iota)^{-1}\pi(1234)) = \\ tr(\rho(\pi\iota)^{-1})((13)(12)(34)V))) = tr(\rho(\pi\iota)^{-1})((13)V))) = tr(\rho(13)) = 0,$$

donde la última igualdad viene de la tabla de caracteres de $S_3$. Fijémonos que el anterior cálculo consiste, a fin de cuentas, en calcular la preimagen de $(1234)V$ en $S_3$ y aplicarle el carácter correspondiente de $S_3$. Con este procedimiento, completamos los valores de $\chi_3$. En este momento, la tabla de caracteres puede ser escrita como

| | 1 | 6 | 8 | 3 | 6 |
|---|---|---|---|---|---|
| $S_4$ | $(1)$ | $(12)$ | $(123)$ | $(12)(34)$ | $(1234)$ |
| $\chi_1$ | 1 | 1 | 1 | 1 | 1 |
| $\chi_2$ | 1 | $-1$ | 1 | 1 | $-1$ |
| $\chi_3$ | 2 | 0 | $-1$ | 2 | 0 |
| $\chi_4$ | 3 | $x$ | $y$ | $z$ | $t$ |
| $\chi_5$ | 3 | $x'$ | $y'$ | $z'$ | $t'$ |

donde $x,y,z,t$ y $x',y',z',t'$ son valores por determinar. Observemos que si $n,m$ son los grados de $\chi_4$ y $\chi_5$, entonces $24 = 1+1+4+n^2+m^2$, de donde $n = m = 3$, tal como refleja la tabla anterior.

Las relaciones de ortogonalidad por filas (Teorema 2.4.1.1) de $\chi_4$ con respecto de las tres primeras filas proporcionan ecuaciones idénticas a las análogas de $\chi_5$. Esto es, $x,y,z,t$ son soluciones del mismo sistema de ecuaciones que $x',y',z',t'$. Este sistema es

$$\begin{aligned} 3+6x+8y+3z+6t &= 0 \\ 3-6x+8y+3z-6t &= 0 \\ 6-8y+6z &= 0 \end{aligned}$$

Tras resolverlo, vemos que su solución es $y = 0, z = -1, t = -x$.

Por otra parte, deducimos de la Proposición 2.3.2 que, puesto que $(12)^2 = (1)$, $x = \chi_3(12)$ es suma de tres raíces cuadradas de 1. Luego $x \in \{-3,-1,1,3\}$. Por último, en virtud de nuevo de Teorema 2.4.1.1, obtenemos[a]

$$9+6x^2+8y^2+3z^2+6t^2 = 24.$$

Por tanto, $x = 1$ o $x = -1$. La discusión previa implica que dichas soluciones proporcionan los valores restantes de los caracteres $\chi_4$ y $\chi_5$, con lo que completamos la tabla de caracteres de $S_4$:

| | 1 | 6 | 8 | 3 | 6 |
|---|---|---|---|---|---|
| $S_4$ | (1) | (12) | (123) | (12)(34) | (1234) |
| $\chi_1$ | 1 | 1 | 1 | 1 | 1 |
| $\chi_2$ | 1 | $-1$ | 1 | 1 | $-1$ |
| $\chi_3$ | 2 | 0 | $-1$ | 2 | 0 |
| $\chi_4$ | 3 | 1 | 0 | $-1$ | $-1$ |
| $\chi_5$ | 3 | $-1$ | 0 | $-1$ | 1 |

■

[a] sabemos que $\overline{x} = x$

■ **Ejercicio 2.12** * Calcular razonadamente la tabla de caracteres del grupo $Q$ definido en el Ejemplo 2.2.

■ **Ejercicio 2.13** Los caracteres irreducibles de $S_4$ proporcionan, por restricción, algunos caracteres de $A_4$. Describir estos caracteres. ¿Son irreducibles?

■ **Ejercicio 2.14** * Calcular razonadamente la tabla de caracteres del grupo diédrico $D_4$.

■ **Ejercicio 2.15** ** Calcular razonadamente la tabla de caracteres del grupo diédrico $D_n$, para $n \geq 2$.

■ **Ejercicio 2.16** Sea $G$ un grupo abeliano finito, y sea $\widehat{G}$ el conjunto de los caracteres complejos irreducibles de $G$. Demostrar que el producto inducido por el de números complejos dota a $\widehat{G}$ de estructura de grupo.

■ **Ejercicio 2.17** ** Sea $G$ un grupo abeliano finito, y $\widehat{G}$ el grupo definido en el Ejercicio 2.16. Demostrar que existe un isomorfismo de grupos $G \cong \widehat{G}$.

Veamos, como aplicación, que los subgrupos normales de $G$ se pueden describir a partir de la tabla de caracteres de $G$. El resultado que permite esto es el siguiente. Denotamos por $Irr(G) = \{\chi_1, \ldots, \chi_t\}$ el conjunto de los caracteres irreducibles de $G$.

**Proposición 2.4.2** Los subgrupos normales de $G$ son de la forma $\bigcap_{\chi \in \Gamma} Ker\chi$, para $\Gamma \subseteq Irr(G)$.

*Demostración.* Comprobemos primero que $\bigcap_{\chi \in Irr(G)} Ker\chi = \{1\}$. Sabemos que $\chi_{reg} = n_1\chi_1 + \cdots + n_t\chi_t$. Si $\chi_i(g) = \chi_i(1)$ para todo $i = 1, \ldots, t$, entonces

$$\chi_{reg}(g) = n_1\chi_1(g) + \cdots + n_t\chi_t(g) = n_1\chi_1(1) + \cdots + n_t\chi_t(1) = |G|,$$

de donde $g = 1$, por el Lema 2.3.6.

Por el Corolario 2.3.4, cada $Ker\chi$ es un subgrupo normal de $G$, lo que demuestra que si $\Gamma \subseteq Irr(G)$, entonces $\bigcap_{\chi \in \Gamma} Ker\chi$ es un subgrupo normal de $G$. Tenemos que demostrar, pues, que todo subgrupo normal $N$ de $G$ es de esta forma. Cada carácter en $Irr(G/N)$ da lugar a un carácter $\chi$ en $Irr(G)$ tal que $N \subseteq Ker\chi$. Identificamos así $Irr(G/N)$ con un subconjunto $\Gamma$ de $Irr(G)$. Por lo demostrado previamente,

$$N/N = \bigcap_{\varphi \in Irr(G/N)} Ker\varphi,$$

luego

$$N = \bigcap_{\chi \in \Gamma} Ker\chi.$$

■

## 2.5 Funciones de Clase.

Consideremos el espacio vectorial complejo $\mathbb{C}^G$ cuyos elementos son las aplicaciones $\varphi : G \to \mathbb{C}$. En este espacio vectorial de dimensión $|G|$ definimos el producto interno

$$(\varphi, \psi) = \frac{1}{|G|} \sum_{g \in G} \overline{\varphi(g)} \psi(g).$$

Una consecuencia inmediata del Teorema 2.3.8 es que los caracteres irreducibles $\{\chi_1, \ldots, \chi_t\}$ de $G$ forman un conjunto ortonormal de vectores en $\mathbb{C}^G$. Si $G$ es abeliano, entonces tiene tantas clases de conjugación como elementos, es decir, $t = |G|$, y, por tanto, los caracteres irreducibles forman una base ortonormal de $\mathbb{C}^G$. Si $G$ no es abeliano, los caracteres irreducibles sólo generan un subespacio de $\mathbb{C}^G$. A fin de describir dicho subespacio, introducimos la siguiente terminología: una *función de clase* de $G$ es una aplicación $\varphi : G \to \mathbb{C}$ que es constante sobre cada clase de conjugación de $G$. El conjunto de todas las funciones de clase, denotado por $\mathscr{C}(G)$, es un subespacio vectorial complejo de $\mathbb{C}^G$.

**Proposición 2.5.1** Los caracteres irreducibles $Irr(G) = \{\chi_1, \ldots, \chi_t\}$ constituyen una base ortonormal de $\mathscr{C}(G)$.

*Demostración.* De lo expuesto en el párrafo que precede al enunciado, deducimos que basta con demostrar que $\mathscr{C}(G)$ tiene, exactamente, dimensión $t$. Sean $\mathscr{C}_1, \ldots, \mathscr{C}_t$ las clases de conjugación de $G$. Para cada $i = 1, \ldots, t$, definimos la función de clase

$$\varphi_i(g) = \begin{cases} 1 \text{ si } g \in \mathscr{C}_i \\ 0 \text{ si } g \notin \mathscr{C}_i \end{cases}$$

Es claro que el conjunto $\{\varphi_1, \ldots, \varphi_t\}$ es linealmente independiente, y es bastante fácil ver que cualquier función de clase se escribe como combinación lineal de $\varphi_1, \ldots, \varphi_t$. Por tanto, $\{\varphi_1, \ldots, \varphi_t\}$ es una base de $\mathscr{C}(G)$, con lo que la dimensión de este espacio vectorial complejo es $t$. ■

La interpretación proporcionada por la Proposición 2.5.1 de las relaciones de ortogonalidad tiene la siguiente consecuencia relevante.

**Teorema 2.5.2** Dos representaciones complejas de $G$ son equivalentes si, y sólo si, proporcionan el mismo carácter.

*Demostración.* Sabemos, por el Lema 2.3.1, que representaciones equivalentes proporcionan el mismo carácter, así que nos concentramos en demostrar que el carácter proporcionado por una representación dada la determina salvo equivalencias.

Sea, pues, $\rho$, una representación compleja de $G$. Usando la correspondencia entre representaciones de $G$ y $\mathbb{C}G$–módulos, vemos que, salvo equivalencia, $\rho = \rho_1^{m_1} \oplus \cdots \oplus \rho_t^{m_t}$,

donde $\rho_1, \ldots, \rho_t$ son las representaciones irreducibles de $G$ que fijamos en su momento, y $m_1, \ldots, m_t$ son las multiplicidades de $\rho$. De aquí,

$$\chi_\rho = m_1\chi_1 + \cdots + m_t\chi_t.$$

Puesto que $\{\chi_1, \ldots, \chi_t\}$ es una base ortonormal de $\mathscr{C}(G)$, obtenemos que $m_i = (\chi_i, \chi_\rho)$ para todo $i = 1, \ldots, t$. Por tanto, $\chi_\rho$ determina las multiplicidades y éstas determinan $\rho$ salvo equivalencia. ■

R Usando la notación de la demostración del Teorema 2.5.2, tenemos que $(\chi_\rho, \chi_\rho) = m_1^2 + \cdots + m_t^2$. Deducimos que $\chi_\rho$ es irreducible si, y sólo si, tiene longitud 1 como vector de $\mathscr{C}(G)$.

▪ **Ejercicio 2.18** Sea $G$ un grupo finito y $g \in G$. Demostrar que $g$ es conjugado con $g^{-1}$ si, y sólo si, $\chi(g) \in \mathbb{R}$ para todo carácter complejo irreducible $\chi$ de $G$.

**Ejemplo 2.7** Vamos a comenzar el cálculo de la tabla de caracteres del grupo alternado $A_5$. Tenemos, desde luego, el carácter trivial $\chi_1$. Veremos que podemos usar el producto interno en el espacio de las funciones de clase $\mathscr{C}(A_5)$ para calcular un segundo carácter irreducible.

Antes, describamos las clases de conjugación de $A_5$. Vamos a tener en cuenta las siguientes observaciones, para sacar partido de que disponemos de una descripción bastante explícita de las clases de conjugación de $S_5$.

- Como $A_5$ es un subgrupo normal de $S_5$, tenemos que $A_5$ es unión de algunas clases de conjugación de $S_5$.
- Cada clase de conjugación de $S_5$ contenida en $A_5$ se partirá en una o varias clases de conjugación de $A_5$.

De acuerdo con la primera observación, los 60 elementos de $A_5$ se reparten en las clases de conjugación de $S_5$ representadas por $(1)$ (un elemento), $(123)$ (20 elementos), $(12)(34)$ (15 elementos) y $(12345)$ (24 elementos). Vamos a razonar ahora que todas éstas son clases de conjugación de $A_5$, salvo la última, que se divide en dos clases de conjugación distintas.

Para la clase de $(1)$ no hay nada que analizar, así que consideremos la clase de conjugación de $(123)$. Observemos que este elemento genera un subgrupo de orden 3, esto es, un 3–subgrupo de Sylow de $A_5$. Por los teoremas de Sylow, todos estos subgrupos son conjugados entre sí. Ahora, puesto que $(132)$ es conjugado en $A_5$ con $(123)$ mediante el elemento $(23)(45) \in A_5$, deducimos que todos los 3–ciclos están conjugados entre sí en $A_5$.

También podemos usar que el subgrupo generado por $(12345)$ es un 5–subgrupo de Sylow de $A_5$. Pero, esta vez, $(12345)$ no está conjugado en $A_5$ con su cuadrado $(13524)$. Éste sí lo está con el cubo de $(12345)$, mientras que $(12345)$ es conjugado en $A_5$ con su potencia cuarta. En resumen, los 5–ciclos dan dos clases de conjugación del mismo cardinal en $A_5$.

Por último, que todo producto de dos transposiciones disjuntas es conjugado, mediante una permutación par, con $(12)(34)$ es fácil de comprobar, usando que este elemento genera un 2–subgrupo de Sylow de $A_5$.

Bien, ahora consideremos un espacio vectorial complejo $V$ con base

$$\{v_1, v_2, v_3, v_4, v_5\},$$

y la representación $\rho$ de $A_5$ que asigna a cada $\sigma \in A_5$ la transformación lineal de $V$ definida sobre la base como $v_i \mapsto v_{\sigma(i)}$. Calculando trazas, obtenemos el carácter asociado

| | 1 | 20 | 12 | 12 | 15 |
|---|---|---|---|---|---|
| $A_5$ | (1) | (123) | (12345) | (13524) | (12)(34) |
| $\chi_\rho$ | 5 | 2 | 0 | 0 | 1 |

Si $\chi_1$ es la representación trivial de $A_5$, obtenemos $(\chi_\rho, \chi_1) = 1$. Esto significa que $\chi_\rho - \chi_1$ es un carácter de $A_5$. Ahora, un fácil cálculo nos da $(\chi_\rho - \chi_1, \chi_\rho - \chi_1) = 1$. Luego se trata de un carácter irreducible de grado 4. Por otra parte, como $A_5$ es simple, la única representación irreducible de grado 1 es la trivial. Con toda esta información, como la suma de los cuadrados de los grados de las representaciones irreducibles ha de ser 60, obtenemos que estos grados son $1, 3, 3, 4, 5$. Tenemos, poniendo $\chi_4 = \chi_\rho - \chi_1$, que la tabla de caracteres de $A_5$ tiene el siguiente aspecto:

| | 1 | 20 | 12 | 12 | 15 |
|---|---|---|---|---|---|
| $A_5$ | (1) | (123) | (12345) | (13524) | (12)(34) |
| $\chi_1$ | 1 | 1 | 1 | 1 | 1 |
| $\chi_2$ | 3 | | | | |
| $\chi_3$ | 3 | | | | |
| $\chi_4$ | 4 | 1 | $-1$ | $-1$ | 0 |
| $\chi_5$ | 5 | | | | |

■

## 2.6 Reciprocidad.

Supongamos ahora que $H$ es un subgrupo de $G$. Tenemos la aplicación, claramente lineal, $(-)_H : \mathscr{C}(G) \to \mathscr{C}(H)$ que asigna a cada función de clase $\psi : G \to \mathbb{C}$ su restricción $\psi_H : H \to \mathbb{C}$. Observemos que si $\chi$ es un carácter de $G$, entonces $\chi_H$ es un carácter de $H$, ya que cada representación de $G$ da, por restricción, una representación de $H$.

Tenemos, por otra parte, una aplicación $(-)^G : \mathscr{C}(H) \to \mathscr{C}(G)$, llamada *inducción*, definida como sigue. Para $\varphi \in \mathscr{C}(H)$, definimos la aplicación $\varphi^\bullet : G \to \mathbb{C}$ dada por $\varphi^\bullet(g) = \varphi(g)$ si $g \in H$, y $\varphi^\bullet(g) = 0$ si $g \notin H$. Definamos entonces $\varphi^G : G \to \mathbb{C}$ por

$$\varphi^G(g) = \frac{1}{|H|} \sum_{x \in G} \varphi^\bullet(x^{-1} g x). \tag{2.7}$$

Supongamos que $x_1, \ldots, x_s \in G$ son representantes de las clases laterales módulo $H$, esto es,

$$G/\sim_H = \{x_1 H, \ldots, x_s H\},$$

donde $s = [G : H]$. Dado $x \in G$, tenemos un único $i \in \{1, \ldots, s\}$ tal que $x \in x_i H$. Es fácil comprobar que, para $g \in G$, la condición $x^{-1} g x \in H$ es equivalente a la condición

$x_i^{-1}gx_i \in H$. Usando esto, tenemos, para cualquier función de clase $\varphi$ de $H$,

$$\sum_{x\in G}\varphi^\bullet(x^{-1}gx) = \sum_{i=1}^{s}(\sum_{x\in x_iH}\varphi^\bullet(x^{-1}gx)) = \sum_{i=1}^{s}|H|\varphi^\bullet(x_i^{-1}gx_i) = |H|\sum_{i=1}^{s}\varphi^\bullet(x_i^{-1}gx_i).$$

De donde obtenemos la fórmula

$$\varphi^G(g) = \sum_{i=1}^{s}\varphi^\bullet(x_i^{-1}gx_i). \tag{2.8}$$

■ **Ejercicio 2.19** Demostrar que $\varphi^G \in \mathscr{C}(G)$ para cada $\varphi \in \mathscr{C}(H)$, y que

$$\varphi^G(1) = [G:H]\varphi(1).$$

Tenemos así definida una aplicación, que es lineal, $(-)^G : \mathscr{C}(H) \to \mathscr{C}(G)$. Recordemos que estos espacios de funciones de clase vienen dotados de sendos productos internos, que denotamos indistintamente por $(-,-)$.

**Proposición 2.6.1 — Reciprocidad de Frobenius.** Sea $H$ un subgrupo de $G$, $\varphi \in \mathscr{C}(H)$ y $\psi \in \mathscr{C}(G)$. Entonces

$$(\psi_H, \varphi) = (\psi, \varphi^G).$$

*Demostración.* La demostración consiste en el siguiente cálculo, cuya tercera igualdad usa que $\psi$ es constante sobre las clases de conjugación.

$$\begin{aligned}
(\psi,\varphi^G) &= \tfrac{1}{|G|}\textstyle\sum_{g\in G}\overline{\psi(g)}\varphi^G(g)\\
&= \tfrac{1}{|G|}\tfrac{1}{|H|}\textstyle\sum_{g\in G}\sum_{x\in G}\overline{\psi(g)}\varphi^\bullet(x^{-1}gx)\\
&= \tfrac{1}{|G|}\tfrac{1}{|H|}\textstyle\sum_{g\in G}\sum_{x\in G}\overline{\psi(x^{-1}gx)}\varphi^\bullet(x^{-1}gx)\\
&= \tfrac{1}{|G|}\tfrac{1}{|H|}\textstyle\sum_{x\in G}\sum_{y\in G}\overline{\psi(y)}\varphi^\bullet(y)\\
&= \tfrac{1}{|H|}\textstyle\sum_{y\in H}\overline{\psi(y)}\varphi(y)\\
&= (\psi_H,\varphi).
\end{aligned}$$

■

**Corolario 2.6.2** Si $\varphi$ es un carácter de $H$, entonces $\varphi^G$ es un carácter de $G$.

*Demostración.* Sea $\chi$ cualquier carácter irreducible de $G$. Entonces $(\chi,\varphi^G) = (\chi_H,\varphi)$, y éste último es un número entero no negativo. Como $\varphi^G \neq 0$ por el Ejercicio 2.19, deducimos que $\varphi^G$ es un carácter de $G$. ■

**Corolario 2.6.3** Sea $\varphi \in Irr(H)$. Existe $\chi \in Irr(G)$ tal que $\varphi$ es un constituyente de $\chi_H$.

*Demostración.* Tomemos $\chi \in Irr(G)$ una constituyente de $\varphi^G$. Entonces $0 \neq (\chi,\varphi^G) = (\chi_H,\varphi)$. ■

**Ejemplo 2.8** Consideremos $A_4$ como subgrupo de $A_5$. Entonces

$$A_5/\sim_{A_4} = \{(12345)^i A_4 : i = 0,1,2,3,4\}.$$

Consideremos la tabla de caracteres de $A_4$

| | 1 | 4 | 4 | 3 |
|---|---|---|---|---|
| $A_4$ | (1) | (123) | (132) | (12)(34) |
| $\xi_1$ | 1 | 1 | 1 | 1 |
| $\xi_2$ | 1 | $\omega$ | $\omega^2$ | 1 |
| $\xi_3$ | 1 | $\omega^2$ | $\omega$ | 1 |
| $\xi_4$ | 3 | 0 | 0 | $-1$ |

donde $\omega \in \mathbb{C}$ es una raíz cúbica primitiva de la unidad. Los correspondientes caracteres inducidos vienen recogidas en la siguiente tabla (que **no** es la tabla de caracteres de $A_5$):

| | 1 | 20 | 12 | 12 | 15 |
|---|---|---|---|---|---|
| $A_4^{A_5}$ | (1) | (123) | (12345) | (13524) | (12)(34) |
| $\xi_1^{A_5}$ | 5 | 2 | 0 | 0 | 1 |
| $\xi_2^{A_5}$ | 5 | $-1$ | 0 | 0 | 1 |
| $\xi_3^{A_5}$ | 5 | $-1$ | 0 | 0 | 1 |
| $\xi_4^{A_5}$ | 15 | 0 | 0 | 0 | $-1$ |

,

Puesto que $(\xi_2^{A_5}, \xi_2^{A_5}) = 1$, deducimos que se trata de un carácter irreducible de $A_5$. Por tanto, la tabla de caracteres de $A_5$ es de la forma

| | 1 | 20 | 12 | 12 | 15 |
|---|---|---|---|---|---|
| $A_5$ | (1) | (123) | (12345) | (13524) | (12)(34) |
| $\chi_1$ | 1 | 1 | 1 | 1 | 1 |
| $\chi_2$ | 3 | $x$ | $y$ | $z$ | $t$ |
| $\chi_3$ | 3 | $x'$ | $y'$ | $z'$ | $t'$ |
| $\chi_4$ | 4 | 1 | $-1$ | $-1$ | 0 |
| $\chi_5$ | 5 | $-1$ | 0 | 0 | 1 |

para números complejos $x,y,z,t,x',y',z',t'$ por determinar. Usando las relaciones de ortogonalidad, tenemos las ecuaciones

$$\begin{aligned} 3+20x+12y+12z+15t &= 0 \\ 12+20x-12y-12z &= 0 \\ 15-20x+15t &= 0 \\ 9+20|z|^2+12|y|^2+12|z|^2+15|t|^2 &= 60 \end{aligned}$$

Este sistema de ecuaciones es equivalente a

$$\begin{array}{lcl} x & = & 0 \\ t & = & -1 \\ y+z & = & 1 \\ |y|^2+|z|^2 & = & 3 \end{array}$$

Ahora, observemos que, para cada representante $g$ una clase de conjugación $C$ de $A_5$ listados en la tabla de caracteres de $A_5$, se tiene que $\overline{g^{-1}} \in C$. Por tanto, para cada carácter $\chi$, tenemos que $\chi(g) = \chi(g^{-1})$, luego $\chi(g) = \overline{\chi(g)}$. Deducimos que todos los caracteres de $A_5$ toman valores reales. Tenemos así que las dos últimas ecuaciones del sistema anterior dan

$$y^2 - y - 1 = 0,$$

cuyas soluciones son $y = \frac{1\pm\sqrt{5}}{2}$. Teniendo en cuenta que $x', y', z', t'$ satisfacen las mismas ecuaciones, podemos escoger una de las dos soluciones, por ejemplo $y = \frac{1+\sqrt{5}}{2}$, y asignar $y' = \frac{1-\sqrt{5}}{2}$.

Obtenemos así

| | 1 | 20 | 12 | 12 | 15 |
|---|---|---|---|---|---|
| $A_5$ | (1) | (123) | (12345) | (13524) | (12)(34) |
| $\chi_1$ | 1 | 1 | 1 | 1 | 1 |
| $\chi_2$ | 3 | 0 | $\frac{1+\sqrt{5}}{2}$ | $\frac{1-\sqrt{5}}{2}$ | $-1$ |
| $\chi_3$ | 3 | 0 | $\frac{1-\sqrt{5}}{2}$ | $\frac{1+\sqrt{5}}{2}$ | $-1$ |
| $\chi_4$ | 4 | 1 | $-1$ | $-1$ | 0 |
| $\chi_5$ | 5 | $-1$ | 0 | 0 | 1 |

■

■ **Ejercicio 2.20** * Sea $G$ un grupo abeliano finito, y $H$ un subgrupo de $G$. Demostrar que la aplicación $(-)_H : \mathscr{C}(G) \to \mathscr{C}(H)$ es sobreyectiva. Identificar su núcleo.

■ **Ejercicio 2.21** * Sea $\mathbb{F}_5$ el cuerpo de 5 elementos y

$$G = \{\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} : a, b \in \mathbb{F}_5, a \neq 0\}.$$

Comprobar que $G$ es un subgrupo de $GL_2(\mathbb{F}_5)$ y calcular razonadamente la tabla de caracteres de $G$.

## 2.7 Enteros algebraicos y caracteres

Vamos a necesitar unos resultados básicos sobre números enteros algebraicos.

**Definición 2.7.1** Un *entero algebraico* es un número $z \in \mathbb{C}$ tal que $f(z) = 0$ para algún $f(X) \in \mathbb{Z}[X]$ **mónico**.

Obviamente, cada $n \in \mathbb{Z}$ es un entero algebraico. En este contexto, los números enteros se suelen llamar enteros racionales. La razón de este nombre está contenida en el siguiente ejercicio.

■ **Ejercicio 2.22** Si $q \in \mathbb{Q}$ es un entero algebraico, entonces $q \in \mathbb{Z}$.

**Ejemplo 2.9** El número real $\gamma = (1+\sqrt{5})/2$ es un entero algebraico, ya que su polinomio mínimo sobre $\mathbb{Q}$ es $X^2 - X - 1$. ■

**Ejemplo 2.10** El número real $\alpha = (1+\sqrt{3})/2$ no es un entero algebraico, ya que su polinomio mínimo sobre $\mathbb{Q}$ es $X^2 - X - 1/2$. ■

Recordemos que, para $b \in \mathbb{C}$, la notación $\mathbb{Z}[b]$ se refiere al menor subanillo de $\mathbb{C}$ que contiene a $b$.

**Proposición 2.7.1** Las siguientes condiciones son equivalentes para $b \in \mathbb{C}$.

1. $b$ es un entero algebraico;
2. $\mathbb{Z}[b]$ es, como grupo aditivo, finitamente generado;
3. existe un subanillo $B$ de $\mathbb{C}$ que es finitamente generado como grupo aditivo y tal que $b \in B$.

*Demostración.* (1) $\Rightarrow$ (2). Sabemos que

$$b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0$$

para ciertos $a_i \in \mathbb{Z}$. Así,

$$b^n = -a_{n-1}b^{n-1} - \cdots - a_1 b - a_0,$$

de donde deducimos que cada elemento de $\mathbb{Z}[b]$ se escribe combinación lineal con coeficientes enteros de $1, b, \ldots, b^{n-1}$. Esto es, $\mathbb{Z}[b]$ está generado, como grupo aditivo, por $\{1, b, \ldots, b^{n-1}\}$.
(2) $\Rightarrow$ (3). Tómese $B = \mathbb{Z}[b]$.
(3) $\Rightarrow$ (1). Sean $x_1, \ldots, x_n$ generadores de $B$ como grupo aditivo. Entonces, para cada $i = 1, \ldots, n$, tenemos que $bx_i = \sum_{j=1}^{n} a_{ij}x_j$ para ciertos $a_{ij} \in \mathbb{Z}$. Dicho de otra forma, el vector columna

$$\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

es un vector propio con valor propio $b$ para la matrix $A = (a_{ij})$. Por tanto, $b$ es solución de la ecuación característica de $A$, que es una ecuación polinómica mónica con coeficientes enteros ($A$ tiene coeficientes enteros). ■

Aunque, a primera vista, puede parecer sorprendente, la suma y el producto de enteros algebraicos produce enteros algebraicos. Pero esto es así, de acuerdo con el siguiente teorema.

**Teorema 2.7.2** El conjunto de los enteros algebraicos es un subanillo de $\mathbb{C}$.

*Demostración.* Hemos de comprobar que, si $b, c \in \mathbb{C}$ son enteros algebraicos, entonces $b+c$ y $bc$ siguen siendo enteros algebraicos. Bastará, de acuerdo con la Proposición 2.7.1,

con que demostremos que el menor subanillo $\mathbb{Z}[b,c]$ de $\mathbb{C}$ que contiene a $b$ y $c$, es, visto como grupo aditivo, finitamente generado.

Como $b,c$ son enteros algebraicos, sabemos que $b^n = \sum_{i=0}^{n-1} b_i b^i$, y $c^m = \sum_{j=0}^{m-1} c_j c^j$, para ciertos $b_0,\dots,b_{n-1},c_0,\dots,c_{m-1} \in \mathbb{Z}$. De aquí es fácil comprobar que cada elemento de la forma $b^u c^v$, con $u,v > 0$, se escribe como combinación lineal con coeficientes enteros de elementos de la forma $b^i c^j$ con $0 \le i \le n-1, 0 \le j \le m-1$. Pero todo elemento de $\mathbb{Z}[b,c]$ es una combinación lineal con coeficientes enteros de "monomios" de la forma $b^u c^v$. Concluyendo, vemos que el conjunto

$$\{b^i c^j : 0 \le i \le n-1, 0 \le j \le m-1\}$$

genera $\mathbb{Z}[b,c]$ como grupo aditivo, lo que concluye la demostración. ■

La consecuencia que nos interesa es la siguiente.

**Corolario 2.7.3** Sea $\chi$ un carácter de un grupo finito $G$. Entonces $\chi(g)$ es un entero algebraico para todo $g \in G$.

*Demostración.* Por la Proposición 2.3.2, $\chi(g)$ es una suma de raíces de la unidad. Como cada una de éstas es un entero algebraico, deducimos del Teorema 2.7.2 que $\chi(g)$ lo es. ■

Para nuestros propósitos, necesitamos demostrar no sólo que las entradas de la tabla de caracteres de $G$ son enteros algebraicos, como indica el Corolario 2.7.3, sino que ciertos múltiplos racionales de los mismos lo son. Mantenemos la notación de la Sección 2.3.

**Proposición 2.7.4** Sea $G$ un grupo finito. Para cada $i = 1,\dots,t$, existen enteros no negativos $m_{jkl}$, con $j,k,l = 1,\dots,t$, tales que

$$\frac{h_j \chi_{ij}}{n_i} \frac{h_k \chi_{ik}}{n_i} = \sum_{l=1}^{t} m_{jkl} \frac{h_l \chi_{il}}{n_i}. \tag{2.9}$$

Además, los números $\frac{h_j \chi_{ij}}{n_i}$ son enteros algebraicos para todo $i,j = 1,\dots,t$.

*Demostración.* Recordemos que si $\mathscr{C}_1,\dots,\mathscr{C}_t$ son las clases de conjugación de $G$, y definimos $c_i = \sum_{g \in \mathscr{C}_i} g$ para $i = 1,\dots,t$, entonces, como se probó en la demostración de la Proposición 2.2.4, $\{c_1,\dots,c_t\}$ es una base de $Z(\mathbb{C}G)$. Por tanto, existen números complejos $m_{jkl}$ para $j,k,l = 1,\dots,t$ tales que

$$c_j c_k = \sum_{l=1}^{t} m_{jkl} c_l, \qquad j,k = 1,\dots,t. \tag{2.10}$$

Pero, por la forma que tienen $c_j, c_k$, los coeficientes $m_{jkl}$ han de ser claramente enteros no negativos.

Tomemos ahora la representación irreducible $(V_i,\rho_i)$ de $G$ que proporciona el carácter $\chi_i$, para $i = 1,\dots,t$. La ecuación (2.10) implica que

$$\widetilde{\rho}_i(c_j) \circ \widetilde{\rho}_i(c_k) = \sum_{l=1}^{t} m_{jkl} \widetilde{\rho}_i(c_l) \tag{2.11}$$

Por otra parte, cada aplicación lineal $\widetilde{\rho}_i(c_j) : V_i \to V_i$ verifica que, para cada $a \in \mathbb{C}G$, y cada $v \in V_i$, se tiene

$$\widetilde{\rho}_i(c_j)(av) = c_j av = ac_j v = a\widetilde{\rho}_i(c_j)(v),$$

esto es, $\widetilde{\rho}_i(c_j) \in \mathrm{End}_{\mathbb{C}G}(V_i)$.

Por el Lema de Schur, $\mathrm{End}_{\mathbb{C}G}(V_i)$ es un álgebra de división compleja de dimensión finita. Por el Corolario 1.8.3, ha de ser isomorfa a $\mathbb{C}$. Eso significa que existe $z_{ij} \in \mathbb{C}$ tal que $\widetilde{\rho}_i(c_j) = z_{ij} id_{V_i}$. Identifiquemos este número: tomando trazas, obtengo que $\widetilde{\chi}_i(c_j) = n_i z_{ij}$, donde $n_i$ es el grado de $\rho_i$. Luego

$$\widetilde{\rho}_i(c_j) = \frac{\widetilde{\chi}_i(c_j)}{n_i} id_{V_i}. \tag{2.12}$$

Por otra parte,

$$\widetilde{\chi}_i(c_j) = \widetilde{\chi}_i(\sum_{g \in \mathscr{C}_j} g) = \sum_{g \in \mathscr{C}_j} \widetilde{\chi}_i(g) = h_j \chi_{ij}. \tag{2.13}$$

De las ecuaciones (2.11), (2.12) y (2.13), deducimos que

$$\frac{h_j \chi_{ij}}{n_i} \frac{h_k \chi_{ik}}{n_i} = \sum_{l=1}^{t} m_{jkl} \frac{h_l \chi_{il}}{n_i},$$

como queríamos demostrar.

Para mostrar que los elementos $\frac{h_j \chi_{ij}}{n_i}$ son enteros algebraicos, fijemos $i \in \{1, \ldots, t\}$, y llamemos entonces $x_j = \frac{h_j \chi_{ij}}{n_i}$ para cada $j = 1, \ldots, t$. En virtud de la Proposición 2.7.1, es suficiente con demostrar que el menor subanillo $\mathbb{Z}[x_1, \ldots, x_t]$ que contiene a $x_1, \ldots, x_t$ es finitamente generado en tanto que grupo aditivo. Pero es es consecuencia de las identidades (2.9) ya demostradas. ■

## 2.8 El Teorema $p^aq^b$ de Burnside

Concluimos el curso con la prueba de un resultado no trivial sobre grupos finitos que usa la teoría de caracteres desarrollada. Necesitaremos unos resultados previos.

**Lema 2.8.1** Sea $\chi$ un carácter irreducible de $G$ proporcionado por una representación $(V, \rho)$. Sea $\mathscr{C}$ una clase de conjugación de $G$ tal que $mcd(|\mathscr{C}|, \chi(1)) = 1$. Entonces, para cada $g \in \mathscr{C}$, se tiene que, o bien $\chi(g) = 0$, o bien $\rho(g)$ está en el centro del grupo $GL(V)$.

*Demostración.* Pongamos $n = \chi(1)$. Existen $u, v \in \mathbb{Z}$ tales que

$$1 = u|\mathscr{C}| + vn. \tag{2.14}$$

Multiplicando (2.14) por $\chi(g)/n$, obtenemos

$$\frac{\chi(g)}{n} = u|\mathscr{C}|\frac{\chi(g)}{n} + v\chi(g). \tag{2.15}$$

Por el Corolario 2.7.3, $\chi(g)$ es un entero algebraico, y $|\mathscr{C}|\chi(g)/n$ lo es por la Proposición 2.7.4. Por tanto, (2.15) implica que $\chi(g)/n$ es un entero algebraico. Recordemos de la

Proposición 2.3.2 que $\chi(g)$ es suma de $n$ raíces de la unidad, así que podemos tomar una extensión ciclotómica $F$ de $\mathbb{Q}$ tal que $\chi(g) \in F$. Además, $|\chi(g)| \leq n$. Por tanto, $a = \chi(g)/n \in F$ y $|a| \leq 1$.

Sea $H$ el grupo de Galois de $F/\mathbb{Q}$, y $\sigma \in H$. Como $\sigma(\chi(g))$ es también suma de $n$ raíces de la unidad, tenemos que $|\sigma(a)| \leq 1$. Además, $\sigma(a)$ es también un entero algebraico (satisface la misma ecuación que $a$). En consecuencia,

$$N_{F/\mathbb{Q}}(a) = \prod_{\sigma \in H} \sigma(a)$$

es un entero algebraico y $|N_{F/\mathbb{Q}}(a)| \leq 1$. Pero $N_{F/\mathbb{Q}}(a)$ es invariante bajo la acción de $H$, así que ha de ser un número racional. Por tanto, $N_{F/\mathbb{Q}}(a)$ es un número entero de módulo menor o igual que 1. Hay sólo dos posibilidades: o bien $N_{F/\mathbb{Q}}(a) = 0$, lo que implica que $a = 0$, o bien $|N_{F/\mathbb{Q}}(a)| = 1$, lo que implica que $|a| = 1$, ya que $|\sigma(a)| \leq 1$ para todo $\sigma \in H$. En el primer caso, $\chi(g) = 0$. En el segundo caso, $|\chi(g)| = n$ lo que implica, según la Proposición 2.3.3, que $\rho(g) = \omega\, id_V$ para $\omega \in \mathbb{C}$ una raíz de la unidad. Como consecuencia, $\rho(g)$ está en el centro de $GL(V)$. ■

**Teorema 2.8.2** Sea $G$ un grupo no abeliano simple. Ninguna clase de conjugación de $G$ tiene cardinal de la forma $p^a$ para $p$ primo y $a > 0$.

*Demostración.* Supongamos que existiese una clase de conjugación $\mathscr{C}$ tal que $|\mathscr{C}| = p^a$, para $p$ primo y $a > 0$.

Mantenemos la notación introducida cuando definimos la tabla de caracteres, esto es, $\mathscr{C}_1, \ldots, \mathscr{C}_t$ son las clases de conjugación y $\chi_1, \ldots, \chi_t$ los caracteres irreducibles. Suponemos que $\mathscr{C}_1$ es la clase de conjugación del elemento neutro del grupo $G$, en tanto $\chi_1$ es el carácter trivial. También, seguimos denotando or $(V_i, \rho_i)$ la representación irreducible que proporciona el carácter $\chi_i$ y $n_i = \chi_i(1)$ para $i = 1, \ldots, t$.

Vamos a demostrar primero que, si $i \in \{2, \ldots, t\}$ es tal que $p$ no divide a $n_i$, se tiene que $\chi_i(g) = 0$ para todo $g \in \mathscr{C}$. Sea $i \in \{2, \ldots, t\}$ un tal índice, $Z_i = Z(GL(V_i))$ y $G_i = \{h \in G : \rho_i(h) \in Z_i\}$. Es fácil ver que $G_i$ es un subgrupo normal de $G$. Si $\chi(g) \neq 0$ para algún $g \in \mathscr{C}$, entonces, por el Lema 2.8.1, tenemos que $g \in G_i$. Como $g \neq 1$, deducimos de la simplicidad que $G_i = G$. Por tanto, $\rho_i(G) \subseteq Z_i$, y es un grupo abeliano. Pero, al ser $G$ simple, $G \cong \rho_i(G)$, en contra de nuestra hipótesis.

De las relaciones de ortogonalidad por columnas (ver Teorema 2.4.1), obtenemos la igualdad, para $g \in \mathscr{C}$

$$0 = \sum_{i=1}^{t} \chi_i(g)\overline{\chi_i(1)} = \sum_{i=1}^{t} \chi_i(g) n_i,$$

que podemos reescribir como

$$0 = 1 + \sum_{i=2}^{t} \chi_i(g) n_i.$$

De la anterior discusión deducimos que existen $m_2, \ldots, m_t$ enteros no negativos tales que

$$0 = 1 + \sum_{i=2}^{t} m_i p \chi_i(g).$$

De donde

$$\frac{1}{p} = -\sum_{i=2}^{t} m_i \chi_i(g).$$

En virtud del Corolario 2.7.3, cada $\chi_i(g)$ es un entero algebraico, por lo que, según el Teorema 2.7.2, $1/p$ es un entero algebraico. Eso es una contradicción, así que no puede existir una clase de conjugación con $p^a$ elementos. ■

**Teorema 2.8.3** Sea $G$ un grupo finito tal que $|G| = p^a q^b$, para $p, q$ números primos y $a, b \geq 0$. Entonces $G$ es soluble.

*Demostración.* Haremos inducción sobre $|G|$. Obviamente, el enunciado es cierto para $|G| = 1$, así que supongamos que $|G| > 1$.

Sea $N$ un subgrupo normal maximal[3] de $G$. Si $N \neq \{1\}$, entonces tanto $N$ como $G/N$ son solubles por hipótesis de inducción. Por tanto, $G$ es soluble.

Si $N = \{1\}$ es porque $G$ es simple. Tomamos $P$ un $p$–subgrupo de Sylow de $G$. Sabemos[4] que $Z(P)$ es no trivial, luego podemos tomar $1 \neq g \in Z(P)$. Entonces, el centralizador $c(g)$ de $g$ en $G$ contiene a $P$. Por tanto, $|G : c(g)|$ divide a $|G : P| = q^b$. Pero sabemos que $|G : c(g)| = |\mathscr{C}|$, donde $\mathscr{C}$ denota la clase de conjugación de $g$ en $G$. Eso significa que $|\mathscr{C}|$ es un divisor de $q^b$. Según el Teorema 2.8.2 esto no es posible salvo que $b = 0$ o $G$ sea abeliano. En el primer caso, $P = G$ y $Z(P) = G$, por ser $G$ simple. Luego, en ambos casos, $G$ es simple abeliano, lo que concluye la prueba. ■

[3] Es decir $N$ es maximal entre los subgrupos normales propios de $G$.

[4] La ecuación de clases da, en este caso, $|P| \equiv |Z(P)| (\text{mod } p)$.

# Bibliografía


[Góm20] J. Gómez-Torrecillas. *Álgebra I*. 2.ª edición. Universidad de Granada, 2020. URL: http://hdl.handle.net/10481/59620 (véase páginas 5, 17, 18, 33).

[Isa76] I. M. Isaacs. *Character Theory of Finite Groups*. New York: Academic Press, 1976 (véase página 5).

[Jac80] N. Jacobson. *Basic Algebra II*. San Francisco: Freeman y Co., 1980 (véase página 5).