Teoría de Módulos Ilustrada

Parte I

Notas del curso *Álgebra Moderna* impartido en la Universidad de Granada durante los cursos académicos 20/21,21/22, 22/23 y 23/24.

José Gómez-Torrecillas

Versión 2.0, 2024

Índice general

Parte I

Teoría Básica de Módulos

Capítulo 1

Teorema Chino del Resto

1.1. Conceptos básicos

Un *anillo* es un grupo aditivo $(A, +, 0)$ dotado de una segunda operación binaria $\cdot : A \times A \to A$, llamada producto o multiplicación, que satisface, para cualesquiera $a, b, c \in A$,

1. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
2. $a \cdot (b + c) = a \cdot b + a \cdot c$.
3. $(b + c) \cdot a = b \cdot a + c \cdot a$.

Sólo consideraremos anillos unitales, en el sentido de que existe un elemento $1 \in A$ tal que $1 \cdot a = a = a \cdot 1$ para todo $a \in A$.

La primera es la propiedad asociativa del producto, en tanto que nos referiremos a la segunda y la tercera como propiedades distributivas. El elemento 1 de la cuarta propiedad se llama *uno* del anillo A. Es usual usar la notación abreviada $ab = a \cdot b$, para $a, b \in A$.

Un anillo A se dice *conmutativo* si $ab = ba$ para todo $a, b \in A$.

Ejercicio 1. Sea A un anillo. Diremos que A es *trivial* si $A = \{0\}$. Demostrar que A es trivial si, y sólo si, $1 = 0$.

Ejemplos.

1.1.1. Ejemplos básicos de anillos conmutativos son $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

1.1.2. También son anillos conmutativos los cuerpos finitos $\mathbb{F}_q$, con q una potencia de un número primo.

1.1.3. Dado un anillo conmutativo A, tenemos el anillo de polinomios $A[X]$ en la indeterminada X.

1.1.4. Dado un anillo A y un número natural $n \geq 1$ el conjunto $M_n(A) = \{(a_{ij}) : 1 \leq i, j \leq n\}$ de las matrices cuadradas de tamaño n con entradas en A es un anillo con las operaciones suma y producto definidas como sigue:

$$(a_{ij}) + (b_{ij}) = (s_{ij}), \quad s_{ij} = a_{ij} + b_{ij}; \qquad (a_{ij})(b_{ij}) = (p_{ij}), \quad p_{ij} = \sum_{k=0}^{n} a_{ik} b_{kj}.$$

Si A es no conmutativo o $n > 1$, entonces $M_n(A)$ es no conmutativo.

Recordamos seguidamente dos procedimientos para construir anillos a partir de anillos ya conocidos: los subanillos y los anillos cocientes.

Definición 1. Un subgrupo aditivo S de una anillo A se dice un *subanillo* si $st \in S$ para todo $s, t \in S$ y $1 \in S$. Obviamente, S es así un anillo.

Definición 2. Un ideal de un anillo A es un subgrupo aditivo I de A tal que $ar, ra \in I$ para todo $r \in I$ y todo $a \in A$. Bajo estas condiciones, el grupo cociente A/I es un anillo con el producto definido por $(a+I)(b+I) = ab+I$, para $a, b \in A$.

Los conceptos de subanillo y anillo cociente pueden modelarse conjuntamente a través de la noción de homomorfismo de anillo, que recordamos seguidamente.

Definición 3. Sean A, B anillos. Una aplicación $f : A \to B$ es un homomorfismo de anillos si es un homomorfismo de grupos aditivos tal que $f(aa') = f(a)f(a')$ para todo $a, a' \in A$ y $f(1) = 1$.

Son ejemplos de homorfismos de anillos la aplicación inclusión $\iota : S \to A$ de un subanillo S de A y la proyección canónica $\pi : A \to A/I$ de un anillo sobre su conciente por un ideal.

El núcleo de f, definido como

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

es un ideal de A. Por otra parte, es fácil ver que $\operatorname{Im} f = \{f(a) : a \in A\}$ es un subanillo de B.

Teorema 1.1.5 (Teorema de isomorfía)**.** *Sea $f : A \to B$ un homomorfismo de anillos e I un ideal de A. Si $I \subseteq \operatorname{Ker} f$, entonces existe un único homomorfismo de anillos $\widetilde{f} : A/I \to B$ tal que*

$$\widetilde{f}(a + I) = f(a),$$

para todo $a \in A$. Además, $\widetilde{f}$ es inyectivo si, y sólo si, $I = \operatorname{Ker} f$. En tal caso, $\widetilde{f}$ proporciona un isomorfismo de anillos

$$A/\operatorname{Ker} f \cong \operatorname{Im} f$$

1.2. Teorema Chino del Resto

Vamos a dar una versión general del conocido Teorema Chino del Resto en el contexto general de anillos cualesquiera. Para ello, recordemos que si $A_1, \ldots, A_n$ son anillos, entonces el producto cartesiano $A_1 \times \cdots \times A_n$ es un anillo con las operaciones suma y producto definidas componente a componente a partir de las de $A_1, \ldots, A_n$. Recordemos también que, dados ideales I, J de un anillo A, los subgrupos aditivos suma $I + J$ e intersección $I \cap J$ de A son ideales. Para tres ideales I, J, K usaremos la convención $I + J \cap K = I + (J \cap K)$.

Definición 4. Dos ideales I, J de un anillo A se dicen *coprimos* si $I + J = A$. Equivalentemente, existen $x \in I, y \in J$ tales que $x + y = 1$.

Lema 1.2.1. *Sean* I, J, K *ideales de un anillo* A*. Se verifica que*

$$I + J = I + K = A$$

si, y sólo si,

$$I + J \cap K = A.$$

Más en general, si $I_1, \ldots, I_t$ *son ideales de* A*, con* $t \geq 2$*, se tiene que* $I_1 + I_j = A$ *para todo* $j = 2, \ldots, t$ *si, y sólo si,* $I_1 + \bigcap_{j=2}^{t} I_j = A$.

Demostración. Supongamos que $I + J = I + K = A$. Entonces existen $x, x' \in I, y \in J, z \in K$ tales que $1 = x + y$ y $1 = x' + z$. Así,

$$1 = x + y = x + y(x' + z) = x + yx' + yz \in I + J \cap K.$$

Por tanto, $I + J \cap K = A$.

Recíprocamente, supongamos que $A = I + J \cap K$. Entonces $I + J \supseteq I + J \cap K = A$, por lo que $I + J = A$. Análogamente, $I + K = A$.

Vayamos con la segunda afirmación. Comencemos demostrando por inducción sobre t que, si $I_1 + I_j = A$ para todo $j = 2, \ldots, t$, entonces $I_1 + \bigcap_{j=2}^{t} I_j = A$. Dicha implicación es trivial para $t = 2$. Partiendo de $I_1 + I_j = A$ para todo $j = 2, \ldots, t+1$, pongamos $I = I_1, J = \bigcap_{j=2}^{t} I_j, K = I_{t+1}$. Tenemos entonces, por hipótesis de inducción, que $I + J = A$. Como $I + K = A$, deducimos de lo demostrado antes que $I + J \cap K = A$. Pero $J \cap K = \bigcap_{j=2}^{t+1} I_j$, lo que completa la inducción.

La implicación recíproca es, como antes, muy fácil. □

Teorema 1.2.2 (Teorema Chino del Resto)**.** *Sean* $f_i : A \to A_i$*, con* $i = 1, \ldots, t$*, con* $t \geq 2$*, homomorfismos de anillos y definamos la aplicación*

$$f : A \to \operatorname{Im} f_1 \times \cdots \times \operatorname{Im} f_t, \qquad (f(a) = (f_1(a), \ldots, f_t(a))),$$

que es un homomorfismo de anillos. Llamamos $I_i = \operatorname{Ker} f_i$ *para* $i = 1, \ldots, t$*, con lo que el núcleo de* f *es* $I = I_1 \cap \cdots \cap I_t$*. En virtud del Teorema 1.1.5,* f *induce en el cociente* A/I *un homomorfismo inyectivo de anillos*

$$\widetilde{f} : A/I \to \operatorname{Im} f_1 \times \cdots \times \operatorname{Im} f_t, \qquad (\widetilde{f}(a + I) = (f_1(a), \ldots, f_t(a))).$$

Se tiene que $\widetilde{f}$ *es un isomorfismo de anillos si, y sólo si,* $I_i + I_j = A$ *para todo* $i \neq j$.

Demostración. Que f es un homomorfismo de anillos es una comprobación rutinaria.

Para $a \in A$, tenemos que $a \in \operatorname{Ker} f$ si, y sólo si, $a \in I_i$ para todo $i = 1, \ldots, t$. Por tanto, $\operatorname{Ker} f = I$.

El Teorema 1.1.5 da ahora el homomorfismo inyectivo $\widetilde{f}$. Por otra parte, $\widetilde{f}$ es biyectivo si, y sólo si, f es sobreyectivo. Vamos a caracterizar, por tanto, esta propiedad.

Supongamos que f es sobreyectiva. Dado $i \in \{1, \ldots, t\}$, tomamos $x \in A$ tal que $f_j(x) = 0$ para $j \neq i$ y $f_i(x) = 1$. Tenemos así que $x - 1 \in I_i$, mientras que $x \in \bigcap_{j \neq i} I_j$. Esto es, $1 = 1 - x + x \in I_i + \bigcap_{j \neq i} I_j$. Por el Lema 1.2.1, $I_j + I_i = A$ para todo $j \neq i$.

Recíprocamente, supongamos que los ideales I_i son coprimos dos a dos. Por el Lema 1.2.1, para todo $i = 1, \ldots, t$, tenemos que $I_i + \bigcap_{j \neq i} I_j = A$. Para cada $i = 1, \ldots, t$, tomamos una descomposición $1 = a_i + p_i$, donde $a_i \in I_i$ y $p_i \in \bigcap_{j \neq i} I_j$. Dados valores cualesquiera $b_1, \ldots, b_t \in A$, pongamos $x = \sum_{i=1}^{t} b_i p_i \in A$. Así, para cada $j = 1, \ldots, t$, tenemos

$$f_j(x) = \sum_{i=1}^{t} f_j(b_i p_i) \overset{(*)}{=} f_j(b_j p_j) = f_j(b_j(1 - a_j)) = f_j(b_j) - f_j(b_j a_j) \overset{(**)}{=} f_j(b_j). \qquad (1.1)$$

En el anterior cálculo, la igualdad $(*)$ viene de que $p_i \in \bigcap_{k \neq i} I_k \subseteq I_j$ para todo $j \neq i$. La igualdad $(**)$ ocurre porque $a_j \in I_j$. Como (1.1) dice que $f(x) = (f_1(b_1), \ldots, f_t(b_t))$, concluimos que f es sobreyectiva. □

1.3. Interpolación polinómica y transformada discreta de Fourier.

Aplicaremos el Teorama Chino del Resto a un anillo de polinomios, y obtendremos herramientas de utilidad en otros campos del saber.

1.3.1. Interpolación polinómica

Consideremos un cuerpo K, y el anillo de polinomios en una indeterminada $K[X]$. Dados valores $\alpha_0, \ldots, \alpha_{n-1} \in K$, consideramos los homomorfismos de evaluación

$$\chi_i : K[X] \longrightarrow K, \qquad (\chi_i(f) = f(\alpha_i)).$$

El núcleo de χ_i es $\langle X - \alpha_i \rangle$, el ideal de $K[X]$ generado por $X - \alpha_i$.

Tenemos así un homomorfismo de anillos

$$\chi : K[X] \longrightarrow K^n, \qquad (\chi(f) = (f(\alpha_0), \ldots, f(\alpha_{n-1})),$$

cuyo núcleo es $\bigcap_{i=0}^{n-1}\langle X-\alpha_i\rangle$. El Teorema 1.2.2 muestra que χ es sobreyectiva si, y sólo si, $\alpha_i \neq \alpha_j$ siempre que $i \neq j$. Como, en tal caso, $\bigcap_{i=0}^{n-1}\langle X-\alpha_i\rangle = \langle p(X)\rangle$ para

$$p(X) = \prod_{i=0}^{n-1}(X-\alpha_i),$$

obtenemos un isomorfismo de anilllos

$$\widetilde{\chi} : \frac{K[X]}{\langle p(X)\rangle} \longrightarrow K^n, \qquad \widetilde{\chi}(f(x)) = (f(\alpha_0),\ldots,f(\alpha_{n-1})). \tag{1.2}$$

Aquí, estamos usando la notación $x = X + \langle p(X)\rangle$. Observemos que x puede interpretarse consistentemente como una variable que puede tomar los valores $\alpha_0,\ldots,\alpha_{n-1}$, y $f(x)$ es una función polinómica de grado menor que n.

Una interpretación del isomorfismo (1.2) es que, para cada

$$y_0,\ldots,y_{n-1} \in K$$

existe una única función polinómica $g(x)$ con coeficientes en K de grado menor que n tal que $g(\alpha_i) = y_i$ para todo $i = 0,\ldots,n-1$. Para obtener dicho polinomio de interpolación, basta con calcular $\widetilde{\chi}^{-1}(y_0,\ldots,y_{n-1})$. Puesto que $\widetilde{\chi}$ es K–lineal, basta con calcular $L_i(x) = \widetilde{\chi}^{-1}(e_i)$, para los vectores e_i de la base canónica de K^n. Concretamente,

$$L_i(x) = \frac{p_i(x)}{p_i(\alpha_i)},$$

para

$$p_i(x) = \frac{p(x)}{x-\alpha_i}.$$

De esa forma, obtenemos la fórmula de interpolación de Lagrange:

$$g(x) = \sum_{i=0}^{n-1} y_i L_i(x).$$

La matriz que representa[1] a $\widetilde{\chi}$ con respecto de las K–bases

$$\{1, x, \ldots, x^{n-1}\}$$

y

$$\{e_0, e_1, \ldots, e_{n-1}\}$$

es

$$M = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_0 & \alpha_1 & \cdots & \alpha_{n-1} \\ \vdots & \vdots & & \vdots \\ \alpha_0^{n-1} & \alpha_1^{n-1} & \cdots & \alpha_{n-1}^{n-1} \end{pmatrix}, \tag{1.3}$$

cuya inversa es, en ciertos casos que trataremos más abajo, fácil de expresar.

[1] Representamos las coordenadas como vectores fila.

1.3.2. Transformada discreta de Fourier

Supongamos que K contiene una raíz n–ésima primitiva de la unidad ω. Esto significa que $1, \omega, \ldots, \omega^{n-1}$ son raíces distintas de $X^n - 1$. En particular, la derivada de este polinomio es no nula, es decir, n no es un múltiplo de la característica de K.

Si tomamos $\alpha_i = \omega^i$ para $i = 0, \ldots, n-1$, la matriz M en (1.3) adopta la forma

$$W_\omega = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \omega^0 & \omega^1 & \cdots & \omega^{n-1} \\ \vdots & \vdots & & \vdots \\ (\omega^0)^{n-1} & (\omega^1)^{n-1} & \cdots & (\omega^{n-1})^{n-1} \end{pmatrix}, \tag{1.4}$$

o, de manera más compacta,

$$W_\omega = \left(\omega^{ij}\right)_{0 \le i,j \le n-1}. \tag{1.5}$$

Sea $\mathfrak{p} : K^n \to K[X]/\langle X^n - 1\rangle$ el isomorfismo K–lineal dado por

$$\mathfrak{p}(s_0, \ldots, s_{n-1}) = \sum_{i=0}^{n-1} s_i x^i,$$

y $\chi_\omega : K[X]/\langle X^n - 1\rangle \to K^n$ el homomorfismo de evaluación

$$\chi_\omega(f(x)) = (f(1), f(\omega), \ldots, f(\omega^{n-1})).$$

Entonces el isomorfismo K–lineal

$$K^n \xrightarrow{\mathfrak{p}} \frac{K[X]}{\langle X^n - 1\rangle} \xrightarrow{\chi_\omega} K^n$$

viene dado por $\chi_\omega \mathfrak{p}(s) = sW_\omega$, para $s = (s_0, \ldots, s_{n-1})$. Su inverso

$$\mathcal{F}_\omega = \mathfrak{p}^{-1}\chi_\omega^{-1}$$

se llama *transformada de Fourier discreta* (con respecto de ω).

Observemos que, para $0 < i \le n-1$, ω^i es raíz del polinomio[2] $X^{n-1} + \cdots + X + 1$, esto es,

$$\sum_{k=0}^{n-1} \omega^{ik} = 0. \tag{1.6}$$

De (1.6) deducimos que, para $i, j \in 0, \ldots, n-1$, distintos,

$$\left(1, \omega^i, \omega^{2i}, \ldots, \omega^{(n-1)i}\right) \begin{pmatrix} 1 \\ \omega^{-j} \\ \omega^{-2j} \\ \vdots \\ \omega^{-(n-1)j} \end{pmatrix} = \sum_{k=0}^{n-1} \omega^{(i-j)k} = 0,$$

[2] observemos que $X^n - 1 = (X-1)(X^{n-1} + \cdots + X + 1)$

puesto que $\omega^m = \omega^l$ para $m \equiv l \pmod{n}$. Deducimos que

$$W_\omega \cdot W_{\omega^{-1}} = nI_n,$$

o, alternativamente,

$$W_\omega^{-1} = \frac{1}{n} W_{\omega^{-1}}. \tag{1.7}$$

De modo que

$$\mathcal{F}_\omega(y) = \frac{1}{n} y W_{\omega^{-1}}.$$

Así, escribiendo

$$\mathcal{F}_\omega(y) = (\widehat{y}_0, \widehat{y}_1, \ldots, \widehat{y}_{n-1}),$$

tenemos

$$\widehat{y}_j = \frac{1}{n} \sum_{k=0}^{n-1} y_k \omega^{-jk}. \tag{1.8}$$

De esta forma, el polinomio interpolador de los datos $y = (y_0, y_1, \ldots, y_{n-1}) \in K^n$ en los nodos $1, \omega, \ldots, \omega^{n-1}$ está dado por

$$h(x) = \sum_{j=0}^{n-1} \widehat{y}_j x^j. \tag{1.9}$$

Una forma alternativa de escribir (1.7) es

$$\mathcal{F}_\omega^{-1} = n\mathcal{F}_{\omega^{-1}}.$$

El isomorfismo K–lineal $\mathfrak{p} : K^n \to K[X]/\langle X^n - 1\rangle$ permite trasladar el producto del segundo anillo al llamado producto de convolución en K^n. Es cómodo para describir este producto considerar $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ con la estructura de grupo cíclico de orden n proporcionada por la suma módulo n. Así, el producto de convolución viene dado, para $u, v \in K^n$ por $z = u * v$, donde

$$z_k = \sum_{j \in \mathbb{Z}_n} u_j v_{k-j}.$$

Esta estructura de anillo se denotará por $(K^n, *)$, en tanto que la dada por el producto cartesiano de anillos lo será por $(K^n, \cdot)$.

Teorema 1.3.1. *Si K contiene una raíz primitiva n–ésima de la unidad ω, entonces*

$$\mathcal{F}_\omega(uv) = \mathcal{F}_\omega(u) * \mathcal{F}_\omega(v),$$

y

$$\mathcal{F}_\omega(u * v) = n\mathcal{F}_\omega(u)\mathcal{F}_\omega(v),$$

para cualesquiera $u, v \in K^n$.

Demostración. La primera identidad es, simplemente, escribir que $\mathcal{F}_\omega : (K^n, \cdot) \to (K^n, *)$ es un homomorfismo de anillos.

Para la segunda, consideremos el cálculo

$$\mathcal{F}_\omega(u * v) = \frac{1}{n}\mathcal{F}_{\omega^{-1}}^{-1}(u * v) = \frac{1}{n}\mathcal{F}_{\omega^{-1}}^{-1}(u)\mathcal{F}_{\omega^{-1}}^{-1}(v) = n\mathcal{F}_\omega(u)\mathcal{F}_\omega(v).$$

□

Transformada de Fourier Discreta Clásica

Si ahora tomamos $K = \mathbb{C}$ y $\omega = e^{\mathbf{i}2\pi/n}$, entonces (1.8) adopta la forma

$$\widehat{y}_j = \frac{1}{n}\sum_{k=0}^{n-1} y_k e^{-\mathbf{i}2\pi jk/n},$$

que no es otra cosa que la transformada discreta de Fourier. De hecho, si tomamos una función $f : [0, 2\pi] \to \mathbb{C}$ tal que $f(0) = f(2\pi)$, y tenemos una muestra de tamaño n en puntos equidistantes

$$y_l = f(2\pi l/n), \qquad l = 0, \ldots, n-1,$$

podemos considerar la función $g : [0, 2\pi] \to \mathbb{C}$ dada por

$$g(t) = \sum_{j=0}^{n-1} \widehat{y}_j e^{\mathbf{i}jt}$$

Usando (1.9), obtenemos

$$g(2\pi l/n) = \sum_{j=0}^{n-1} \widehat{y}_j e^{\mathbf{i}j2\pi l/n} = \sum_{j=0}^{n-1} \widehat{y}_j (e^{\mathbf{i}2\pi l/n})^j = y_l = f(2\pi l/n),$$

para $l = 0, \ldots, n-1$.

Ejercicio 2. Sea A un anillo y $R = \{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in A\}$. Comprobar que R es un subanillo de $M_2(A)$. Comprobar que $J = \{\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} : b \in A\}$ es un ideal de R. Buscar dos homomorfismos de anillos $f_1, f_2 : R \to A$ de manera que, al aplicarles el Teorema Chino del Resto, obtengamos un isomorfismo de anillos $R/J \cong A \times A$.

Ejercicio 3. Sea $\mathbb{F}_q$ el cuerpo finito de q elementos y $\mathbb{F}_q \leq \mathbb{F}_{q^m}$ una extensión de grado m. Supongamos un natural n tal que $\mathbb{F}_{q^m}$ contiene una raíz n–ésima primitiva de la unidad ω. Sea $y = (y_0, \ldots, y_{n-1}) \in \mathbb{F}_{q^m}^n$, e $\widehat{y} = (\widehat{y}_0, \ldots, \widehat{y}_{n-1}) \in \mathbb{F}_{q^m}^n$ su transformada de Fourier. Demostrar que $y \in \mathbb{F}_q^n$ si, y sólo si, $\widehat{y}_j^q = \widehat{y}_{jq}$ para todo $j \in \mathbb{Z}_n$.

Ejercicio 4. Dotar a $\mathbb{C}^n$ de un producto interno de manera que la transformada de Fourier discreta sea una isometría.

Capítulo 2

Módulos

2.1. Noción de módulo sobre un anillo

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. Si N es un segundo grupo aditivo, entonces el conjunto

$$\hom(M,N) = \{f : M \to N \mid f \text{ es homomorfismo de grupos}\}$$

es un grupo aditivo con la siguiente operación: Para $f, g \in \hom(M,N)$ definimos $f + g : M \to N$ por

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

El elemento neutro de este grupo es el homomorfismo $0 : M \to N$ definido por $0(m) = 0$ para todo $m \in M$.

Consideremos el grupo aditivo

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

Si $f, g \in \mathrm{End}(M)$, entonces $f \circ g \in \mathrm{End}(M)$. De esta manera, la composición dota a $\mathrm{End}(M)$ de una segunda operación binaria. Obviamente, la aplicación identidad $\mathrm{id}_M : M \to M$ es un elemento neutro para la composición.

Proposición 2.1.1. *Si M es un grupo aditivo, entonces*

$$(\mathrm{End}(M), +, 0, \circ, \mathrm{id}_M)$$

es un anillo.

Demostración. Es una comprobación rutinaria recomendable para principiantes. □

Definición 5. El anillo definido obtenido en la Proposición 2.1.1 se llama *anillo de endomorfismos de* M.

Observación 1. Si $M = \{0\}$, entonces $\mathrm{End}(M) = \{0\}$. En este caso, $\mathrm{id}_M = 0$, claro.

Estamos preparados para dar una definición fundamental en este texto.

Definición 6. 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 φ es inyectivo.

Ejemplos. Los ejemplos más elementales de módulo son los siguientes.

2.1.2. Grupos aditivos. 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 $\chi(1) = \mathrm{id}_M$. Vemos, así, que M tiene una (única) estructura de $\mathbb{Z}$–módulo.

2.1.3. Espacios vectoriales. 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 que φ es un homomorfismo de anillos. Por tanto, V es un K–módulo. De hecho, un K–módulo es, exactamente, un K–espacio vectorial, como se deduce de la Proposición 2.1.4 más abajo.

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 2.1.4. *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*[1]*:*
   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* $m \in M$.

[1]Desde esta perspectiva, los módulos que hemos definido se suelen llamar *módulos a izquierda* en la literatura

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 es una comprobación rutinaria. Comprobemos, por ejemplo, 2*c*): 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 φ 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 2*a*), 2*b*), 2*c*) y 2*d*) se comprueba sin dificultad que φ ciertamente define un homomorfismo de anillos. Por ejemplo, que $\varphi(a) \in \mathrm{End}(M)$ para todo $a \in A$ se deduce de 2*a*). □

Observación 2. 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. También usaremos la abreviatura ${}_AM$ para indicar que M es un A–módulo.

Ejemplos. Los que siguen son ejemplos de procedimientos abstractos de construcción de módulos.

2.1.5. 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".

2.1.6. 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*.

En particular, el A–módulo regular A resulta ser un R–módulo. Concretamente, la acción de R sobre A viene dada, a la luz de la Proposición 2.1.4, por

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

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

2.1.7. Ideal anulador. Dado un módulo ${}_AM$, el núcleo del homomorfismo de anillos correspondiente $\varphi : A \to \mathrm{End}(M)$ es, como sabemos, un ideal de A. Dicho núcleo se llama *anulador de* M, denotado por $\mathrm{Ann}_A(M)$. Tenemos que

$$\mathrm{Ann}_A(M) = \{a \in A \mid am = 0, \text{ para todo } m \in M\},$$

y el primer teorema del isomorfismo nos da que M es un $A/\mathrm{Ann}_A(M)$–módulo fiel con la acción

$$(a + \mathrm{Ann}_A(M))m = am,$$

para todo $a \in A, m \in M$.

Ejercicio 5. Completar la demostración de la Proposición 2.1.4.

2.1.1. Módulos sobre un anillo de polinomios

Sea V un K–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

$$f(T) = f_0\mathrm{id}_V + f_1T + \cdots + f_nT^n.$$

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. Sea $C^\infty(\mathbb{R})$ el espacio 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.

Ejercicio 6. Demostrar que si, en el Ejemplo 2.1.1, el K–espacio vectorial V tiene dimensión finita, entonces $\mathrm{Ann}_{K[X]}(V) = \langle \mu(X) \rangle$ para cierto polinomio no nulo $\mu(X) \in K[X]$. Éste es el llamado *polinomio mínimo de* T.

Ejercicio 7. Sea M un grupo aditivo finito. Describir $\mathrm{Ann}_{\mathbb{Z}}(M)$. Calcular este anulador para $M = \mathbb{Z}_6 \times \mathbb{Z}_8$.

2.2. Submódulos, homomorfismos, cocientes

2.2.1. Submódulos

Comencemos con la definición de submódulo, que generaliza la de subespacio vectorial.

Definición 7. Si ${}_AM$ es un módulo, un subgrupo aditivo N de M es un *submódulo* de M si $ax \in N$ para todo $x \in N$, $a \in A$. Los submódulos de A se llaman *ideales a izquierda de* A.

Observación 3. Los ideales a izquierda de un anillo conmutativo no son más que sus ideales.

Los submódulos triviales de un módulo M son el submódulo cero $\{0\}$ y el submódulo total M.

Ejercicio 8. Sea $T : V \to V$ una transformación lineal en un K–espacio vectorial V. Un subespacio vectorial W de V se dice T–*invariante* si $T(W) \subseteq W$. Demostrar que los subespacios T–invariantes de V son, exactamente, los $K[X]$–submódulos de V. Demostrar que, si $V \neq \{0\}$ y $\{0\}$ y V son los únicos subespacios T–invariantes de V, entonces el polinomio mínimo de T es irreducible en $K[X]$. Mostrar que el recíproco no es cierto mediante un contraejemplo.

Cada elemento $m \in M$ genera el llamado submódulo cíclico Am dado por

$$Am = \{am \mid a \in A\}.$$

Se trata del menor submódulo de M, en el sentido de la inclusión, que contiene a m.

Ejemplo. El submódulo cíclico del $\mathbb{R}[X]$–módulo $C^\infty(\mathbb{R})$ (ver Ejemplo 2.1.1) generado por $\sin t$ es el $\mathbb{R}$–subespacio vectorial que tiene como base $\{\sin t, \cos t\}$.

Ejemplo. El propio anillo A es un A–módulo cíclico generado por $1 \in A$.

Más generalmente, dados $m_1, \ldots, m_n \in M$ en cantidad finita, definimos

$$Am_1 + \cdots + Am_n = \{a_1m_1 + \cdots + a_nm_n \mid a_1, \ldots, a_n \in A\}. \tag{2.1}$$

Es fácil comprobar que se trata de un submódulo de M, llamado *submódulo de* M generado por el *conjunto de generadores* $m_1, \ldots, m_n$.

Definición 8. Un módulo ${}_AM$ se dice *finitamente generado* si existen $m_1, \ldots, m_n \in M$ tales que $M = Am_1 + \cdots + Am_n$.

El símbolo "+" a la izquierda de la igualdad (2.1) tiene también el sentido de suma de submódulos, de acuerdo con la siguiente observación: si $N_1, \ldots, N_n$ son submódulos de M, entonces

$$N_1 + \cdots + N_n = \{m_1 + \cdots + m_n \mid m_i \in N_i\}$$

es un submódulo de M. Este submódulo también se denotará como $\sum_{i=1}^{n} N_i$ o, simplemente, por $\sum_i N_i$, si el contexto lo permite.

Discutamos ahora la noción de suma directa interna.

Proposición 2.2.1. *Supongamos una familia finita* $N_1, \ldots, N_t$ *de sumódulos de un módulo* ${}_AM$*. Son equivalentes:*

(I) Para cada $i = 1, \ldots, t$, $N_i \cap \sum_{j \neq i} N_j = \{0\}$*;*

(II) si $0 = n_1 + \cdots + n_t$ *con* $n_i \in N_i$*, entonces* $n_i = 0$ *para todo* $i = 1, \ldots, t$*;*

(III) cada $n \in N_1 + \cdots + N_t$ *admite una única expresión como* $n = n_1 + \cdots + n_t$ *con* $n_i \in N_i$*.*

Demostración. (I) $\Rightarrow$ (II). Como, para cada $i = 1, \ldots, n$, tenemos que

$$-n_i = \sum_{j \neq i} n_j \in N_i \cap \sum_{j \neq i} N_j = \{0\},$$

deducimos que $n_i = 0$.

(II) $\Rightarrow$ (III). Si $n = n_1 + \cdots + n_t = n_1' + \cdots + n_t'$ con $n_i, n_i' \in N_i$, entonces

$$0 = (n_1 - n_1') + \cdots + (n_t - n_t'),$$

de donde, por la condición (II), obtenemos $n_i = n_i'$ para $i = 1, \ldots, t$.

(III) $\Rightarrow$ (I). Si, dado $i = 1, \ldots, t$, tomamos $n \in N_i \cap \sum_{j \neq i} N_j$, entonces

$$n = \sum_{j \neq i} n_j,$$

para ciertos $n_j \in N_j$. Pero, entonces,

$$0 = n - \sum_{j \neq i} n_j,$$

con lo que la unicidad supuesta aplicada a 0 da que $n = 0$. □

Definición 9. Si un módulo M se expresa como $M = N_1 + \cdots + N_t$, para ciertos submódulos N_i que satisfacen las condiciones equivalentes establecidas en la Proposición 2.2.1, diremos que M es *suma directa interna* de $N_1, \ldots, N_t$, y escribiremos

$$M = N_1 \dot{+} \cdots \dot{+} N_t.$$

Cada uno de los submódulos N_i se dice ser un *sumando directo* de M.

Observemos que, en la Definición 9, en ningún momento hemos supuesto que los submódulos N_i son no nulos. Obviamente, los casos interesantes no involucran sumandos nulos.

Definición 10. Si $N_1, \ldots, N_t$ son submódulos no nulos de un módulo ${}_AM$ y satisfacen las condiciones equivalentes de la Proposición 2.2.1, diremos que forman un conjunto de *submódulos independientes*.

Ejercicio 9. Sea M un módulo finitamente generado sobre un anillo conmutativo A. Si $m_1, \ldots, m_n \in M$ es un conjunto de generadores de M, demostrar que $\mathrm{Ann}_A(M) = \mathrm{ann}_A(m_1) \cap \cdots \cap \mathrm{ann}_A(m_n)$.

2.2.2. Descomposición primaria de módulos sobre un DIP

Consideraremos un módulo M sobre un DIP (dominio de ideales principales) A, con lo que los resultados obtenidos no sólo se aplicarán cuando $A = K[X]$, sino también en otros casos, como $A = \mathbb{Z}$.

Supondremos que M es *acotado* en el sentido de que $\mathrm{Ann}_A(M) = \langle \mu \rangle$ para $0 \neq \mu \in A$. Supongamos que $M \neq \{0\}$, con lo que μ no es una unidad de A. Así, tenemos una factorización completa

$$\mu = p_1^{e_1} \cdots p_t^{e_t}, \tag{2.2}$$

donde $p_1, \ldots, p_t \in A$ son irreducibles distintos y $e_1, \ldots, e_t$ son naturales no nulos. Para cada $i = 1, \ldots, t$, pongamos

$$q_i = \frac{\mu}{p_i^{e_i}},$$

y

$$M_i = \{q_i m : m \in M\}.$$

Cada M_i es un A–submódulo de M. Por otra parte, el máximo común divisor de $q_1, \ldots, q_t$ es 1, por lo que existen $a_i \in A$ tales que

$$1 = \sum_{i=1}^{t} a_i q_i.$$

De donde

$$m = \sum_i a_i q_i m, \tag{2.3}$$

para cada $m \in M$, lo que demuestra que $M = M_1 + \cdots + M_t$.

Observemos que $q_i q_j$ es un múltiplo de μ si $i \neq j$. De aquí que, para $m \in M_i$, se tenga que $q_j m = 0$ si $j \neq i$ (recordemos que $\langle \mu \rangle = \mathrm{Ann}_A(M)$). Deducimos así de (2.3) que, si $m \in M_i$, entonces $m = a_i q_i m$. De aquí,

$$M_i = \{m \in M \mid m = a_i q_i m\}. \tag{2.4}$$

Si ahora suponemos que $0 = \sum_i m_i$, para $m_i \in M_i$, hacemos actuar $a_j q_j$ para cada $j = 1, \ldots, t$ y obtenemos que $0 = a_j q_j m_j = m_j$. Por tanto, tenemos la descomposición del A–módulo

$$M = M_1 \dotplus \cdots \dotplus M_t. \tag{2.5}$$

La descomposición (2.5) se llama *descomposición primaria* de M, y el submódulo M_i se llama *componente* p_i*–primaria* de M.

Observemos, por último, que de (2.4) y (2.3) se deduce

$$M_i = \{m \in M \mid p_i^{e_i} m = 0\}.$$

Así, de (2.5), deducimos que

$$\langle \mu \rangle = \mathrm{Ann}_A M = \bigcap_i \mathrm{Ann}_A M_i \supseteq \bigcap_i \langle p_i^{e_i} \rangle = \langle \mu \rangle,$$

lo que implica que

$$\mathrm{Ann}_A M_i = \langle p_i^{e_i} \rangle$$

para $i = 1, \ldots, t$.

Ejemplo. Sea M un grupo aditivo finito. Esto implica que M es un $\mathbb{Z}$–módulo acotado. De hecho, $\mathrm{Ann}_{\mathbb{Z}} = \langle \mu \rangle$, para μ el mínimo común múltiplo de los órdenes de todos los elementos de M. Para cada divisor primo p de μ, la componente p–primaria de M es, precisamente, su p–subgrupo de Sylow.

Ejemplo. En términos del endomorfismo K–lineal T que hace de V en el Ejemplo 6 un $K[X]$–módulo, la descomposición

$$V = V_1 \dotplus \cdots \dotplus V_t,$$

para $V_i = \{v \in V \mid p_i^{e_i} v = 0\}$, proporcionada por la factorización completa (2.2) del polinomio mínimo μ de T, puede interpretarse como una suma directa de subespacios T–invariantes, ya que $T(V_i) \subseteq V_i$ para $i = 1, \ldots, t$. Tomando una base, como K–espacio vectorial, de cada V_i y reuniendo éstas en una base de V, obtenemos que la matriz de T con respecto de la misma es diagonal por bloques, siendo cada bloque la matriz que representa a la restricción $T : V_i \to V_i$. Volveremos sobre esto más adelante.

Ejercicio 10. Calcular la descomposición primaria de $\mathbb{Z}_{6000}$ usando la suma directa interna.

Ejercicio 11. Sea $T : V \to V$ una transformación lineal de un espacio vectorial V de dimensión finita sobre un cuerpo K y $\mu \in K[X]$ su polinomio mínimo. Demostrar que $\deg \mu \leq \dim_K V$ y que se da la igualdad si, y sólo si, V es un $K[X]$–módulo cíclico.

Ejercicio 12. Dado un endomorfismo lineal $T : V \to V$, para V un K–espacio vectorial de dimensión finita con polinomio mínimo $\mu \in K[X]$. Deducir de la descomposición primaria de V que μ se factoriza completamente como producto de polinomios lineales mónicos distintos si, y sólo si, T es diagonalizable.

Ejercicio 13. Tomemos un espacio euclídeo V de dimensión n y $T : V \to V$ una isometría. Demostrar que el ortogonal de cada $\mathbb{R}[X]$–submódulo de V es asimismo un $\mathbb{R}[X]$–submódulo. Aplicar esta observación para demostrar que V se descompone como suma directa de subespacios vectoriales invariantes por T de dimensiones 1 o 2. Deducir que existe una base ortonormal de V con respecto de la cual la matriz de T es diagonal por bloques de tamaño 1 o 2. ¿Qué aspecto tienen esos bloques?

2.2.3. Homomorfismos y módulos cociente

Puesto que el concepto de módulo cociente está íntimamente ligado al de homomorfismo, comencemos definiendo aquél. Por A, denotamos un anillo cualquiera. Si L es un submódulo de un módulo ${}_AM$, entonces el grupo aditivo cociente M/L tiene estructura de A–módulo dada por

$$a(m + L) = am + L,$$

para $a \in A$, $m + N \in M/N$. Resulta que la proyección canónica

$$p : M \to M/L, \qquad (p(m) = m + L)$$

es un homomorfismo de A–módulos en el sentido de la siguiente definición.

Definición 11. Sean M y N módulos sobre un anillo A. Un *homomorfismo de A–módulos de M a N* es una aplicación $f : M \to N$ tal que, para cualesquiera $m, m' \in M$ y $a \in A$, se verifica que

1. $f(m + m') = f(m) + f(m')$,
2. $f(am) = af(m)$.

Es fácil comprobar que, para módulos ${}_AM, {}_AN$, el conjunto

$$\mathsf{Mod}_A(M, N) = \{f : M \to N \mid f \text{ homomorfismo de } A\text{–módulos } \}$$

es un grupo aditivo con la suma definida declarando, para $f, g \in \mathsf{Mod}_A(M, N)$,

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

Diremos que un homomorfismo de módulos $f : M \to N$ es un isomorfismo cuando sea biyectivo. En este caso, $f^{-1} : N \to M$ es automáticamente un homomorfismo de módulos y, por tanto, un isomorfismo. Cuando exista un isomorfismo de módulos $f : M \to N$, diremos que M y N son módulos isomorfos y denotaremos este hecho por la notación $M \cong N$.

Los homomorfismos de módulos inyectivos se suelen llamar monomorfismos, en tanto que los sobreyectivos reciben el nombre de epimorfismos de módulos.

El teorema del isomorfismo admite también una versión para módulos.

Proposición 2.2.2 (Primer Teorema de Isomorfía)**.** *Dado $f \in \mathsf{Mod}_A(M, N)$, el núcleo $\operatorname{Ker} f$ es un A–submódulo de M, y la imagen $\operatorname{Im} f$ es un A–submódulo de N. Para cada submódulo $L \subseteq \operatorname{Ker} f$, existe un único homomorfismo de A–módulos $\widetilde{f} : M/L \to N$ tal que*

$$\widetilde{f}(m + L) = f(m),$$

para todo $m \in M$. Además, $\widetilde{f}$ es inyectivo si, y sólo si, $L = \operatorname{Ker} f$. En tal caso, $\widetilde{f}$ proporciona un isomorfismo de A–módulos

$$M/\operatorname{Ker} f \cong \operatorname{Im} f.$$

Demostración. Se deduce inmediatamente del Primer Teorema de isomorfía para grupos aditivos, sin más que observar que el homomorfismo de grupos $\widetilde{f}$ es ahora un homomorfismo de módulos. □

Ejemplos.

2.2.3. Anulador de un elemento. Dado un módulo ${}_AM$ y $m \in M$, tenemos el homomorfismo A–módulos $f : A \to M$ definido por $f(a) = am$ para todo $a \in A$. La imagen de f es, obviamente, Am, en tanto que el núcleo de f es

$$\mathrm{ann}_A(m) = \{a \in A \mid am = 0\}$$

que es un ideal a izquierda de A, llamado *anulador* de m. Tenemos el isomorfismo de A–módulos

$$A/\mathrm{ann}_A(m) \cong Am, \qquad (a + \mathrm{ann}_A(m) \mapsto am).$$

2.2.4. Sucesiones linealmente recursivas Consideremos, para un cuerpo K, el K–espacio vectorial

$$S = \{s : \mathbb{N} \to K\}$$

de todas las sucesiones con valores en K. Este espacio de sucesiones puede dotarse de estructura de $K[X]$–módulo declarando el operador lineal

$$Xs\,(n) = s(n+1)$$

para $s \in S$ y $n \in \mathbb{N}$. Explícitamente, para $s \in S$,

$$f = \sum_{i=0}^{l} f_i X^i \in K[X],$$

$$fs(n) = \sum_{i=0}^{l} f_i s(n+i), \qquad (n \in \mathbb{N}).$$

De modo que $\mathrm{ann}_{K[X]}(s) \neq \{0\}$ si, y sólo si, existen $f_0, \ldots, f_{l-1} \in K$ tales que[2]

$$s(n+l) = -\sum_{i=0}^{l-1} f_i s(n+i), \qquad (\text{ para todo } n \in \mathbb{N}). \tag{2.6}$$

Observemos que $\mathrm{ann}_{K[X]}(s) = \langle p(X) \rangle$, donde $p(X)$ es mónico de grado mínimo en $\mathrm{ann}_{K[X]}(s)$.

Una sucesión satisfaciendo una relación recursiva como (2.6) se suele llamar *linealmente recursiva*. El polinomio $p(X)$ se llama *polinomio de conexión* de la sucesión, en tanto que su grado es la *complejidad lineal* de la misma.

[2] siempre podemos tomar un polinomio mónico que anula a s

Por ejemplo, si $p(X) = X^2 - X - 1$, entonces tenemos la siguiente recursión lineal para una sucesión s anulada por $p(X)$

$$s(n+2) = s(n+1) + s(n), \qquad (n \in \mathbb{N}).$$

Iniciando $s(0) = s(1) = 1$, obtenemos la famosa sucesión de Fibonacci.

2.2.5. Ecuaciones diferenciales lineales. Tomemos ahora el espacio vectorial real $C^\infty(\mathbb{R})$ de las funciones definidas en la recta real $\mathbb{R}$ con valores reales que admiten derivadas de cualquier orden. Se trata de un $\mathbb{R}[X]$–módulo determinado por el operador lineal derivación $X\varphi = \varphi'$, para $\varphi \in C^\infty(\mathbb{R})$. Dado $f = \sum_{i=0}^{l} f_i X^i \in \mathbb{R}[X]$, tenemos que

$$f\varphi = \sum_{i=0}^{l} f_i \varphi^{(i)},$$

donde $\varphi^{(i)}$ denota la derivada de orden i de φ. De forma que la condición $\mathrm{ann}_{\mathbb{C}[X]}(\varphi) \neq \{0\}$ significa que φ satisface una ecuación diferencial lineal con coeficientes constantes. En tal caso,

$$\mathrm{ann}_{\mathbb{R}[X]}(\varphi) = \langle p(X) \rangle,$$

para $p(X)$ el polinomio no nulo de grado mínimo que anula a s.

Por ejemplo, si $\alpha = 1/2 + \sqrt{5}/2$, que raíz de $p(X) = X^2 - X - 1$, entonces

$$\varphi(t) = e^{\alpha t},$$

es solución de la ecuación diferencial

$$\varphi'' - \varphi' - \varphi = 0.$$

2.2.6. Funciones analíticas y sucesiones linealmente recursivas. La aplicación $\tau : C^\infty(\mathbb{R}) \to Map(\mathbb{N}, \mathbb{R})$ definida por $\tau(\varphi)(n) = \varphi^{(n)}(0)$ es un homomorfismo de $\mathbb{R}[X]$–módulos. Como consecuencia, para cada función φ se tiene que $\mathrm{ann}_{\mathbb{R}[X]}(\varphi) \subseteq \mathrm{ann}_{\mathbb{R}[X]}(\tau(\varphi))$. Además, se tiene la igualdad si φ es analítica en $\mathbb{R}$, ya que, en tal caso, φ está determinada por $\tau(\varphi)$.

2.2.4. Ejercicios

Ejercicio 14. Calcular todas las funciones $f \in C^\infty(\mathbb{R})$ tales que $\mathrm{ann}_{\mathbb{R}}(f) \in \langle X^3 - X \rangle$, con la estructura de $\mathbb{R}[X]$–módulo dada por el operador lineal derivada.

Ejercicio 15. Demostrar que una sucesión s es linealmente recursiva si, y sólo si, $K[X]s$ es un K–espacio vectorial de dimensión finita.

Ejercicio 16 (Segundo Teorema de Isomorfía)**.** Supongamos submódulos $L \subseteq K \subseteq M$. Deducir del Primer Teorema de Isomorfía que existe un isomorfismo de módulos

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

Demostrar que todo submódulo de M/L es de la forma K/L para cierto submódulo $K \subseteq M$ que contiene a L.

Ejercicio 17 (Tercer Teorema de Isomorfía)**.** Supongamos submódulos L, N de un módulo M. Deducir del Primer Teorema de Isomorfía que existe un isomorfismo

$$(L + N)/L \cong N/(L \cap N).$$

Ejercicio 18. Para K un anillo conmutativo, consideremos el anillo de polinomios $K[X]$. Establecer que dar un $K[X]$–módulo es equivalente a dar un K–módulo M junto con un endomorfismo de K–módulos $T : M \to M$.

2.2.5. Suma directa externa y sucesiones exactas

Dados A–módulos $M_1, \ldots, M_n$, el producto cartesiano

$$M_1 \times \cdots \times M_n = \{(m_1, \ldots, m_n) : m_i \in M_i\}$$

es un A–módulo con la suma definida "componente a componente" y la acción de A dada por

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

Este módulo se llama *suma directa externa* de $M_1, \ldots, M_n$. Usaremos la notación

$$M_1 \oplus \cdots \oplus M_n$$

para designarlo.

En el caso especial en que $M_1 = \cdots = M_n = M$, esta suma directa será denotada por M^n. En particular, tenemos el módulo A^n que, como veremos, tiene un papel relevante. Este módulo es finitamente generado, ya que un conjunto de generadores es $e_1, \ldots, e_n$, donde e_i es la n-tupla todas cuyas componentes son 0, salvo la i–ésima, que es 1.

Ejercicio 19. Sean $N_1, \ldots, N_t$ submódulos de un módulo M. Demostrar que existe un homomorfismo sobreyectivo de módulos $N_1 \oplus \cdots \oplus N_t \to N_1 + \cdots + N_t$ que es un isomorfismo si, y sólo si, la suma $N_1 + \cdots + N_t$ es una suma directa interna.

Proposición 2.2.7. *Sea ${}_AM$ un módulo, y $m_1, \ldots, m_n \in M$. Existe un único homomorfismo de módulos $f : A^n \to M$ tal que $f(e_i) = m_i$ para $i = 1, \ldots, n$. Como consecuencia, todo A–módulo finitamente generado es isomorfo a un módulo de la forma A^n/L para cierto $n \in \mathbb{N}$ y L un submódulo A^n.*

Demostración. Un elemento de A^n se escribe de forma única como $\sum_i a_i e_i$ para ciertos $a_i \in A$. Como consecuencia, la única definición posible para un homomorfismo de A–módulos como el del enunciado es

$$f(\sum_i a_i e_i) = \sum_i a_i m_i.$$

Un cálculo rutinario muestra que esta definición da realmente un homomorfismo de A–módulos.

Si ahora $m_1, \ldots, m_n$ constituyen un conjunto de generadores de M, entonces el homomorfismo $f : A^n \to M$ es sobreyectivo. La última afirmación del enunciado es ahora consecuencia directa de la Proposición 2.2.2 tomando $L = \ker f$. □

La Proposición 2.2.2 admite una formulación más abstracta, en términos de las llamadas sucesiones exactas de módulos. Veamos primero su definición.

Definición 12. Una sucesión de homomorfismos de módulos

$$\cdots \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \xrightarrow{f_{i+1}} M_{i+2} \xrightarrow{f_{i+2}} \cdots$$

se llama *exacta en* M_{i+1} si $\operatorname{Im} f_i = \ker f_{i+1}$. La sucesión es *exacta* si es exacta en todo M_i. Una sucesión exacta de la forma

$$0 \longrightarrow L \xrightarrow{\alpha} M \xrightarrow{\beta} N \longrightarrow 0$$

se llama *sucesión exacta corta*. Esto significa, ni más, ni menos, que α es inyectivo, β es sobreyectivo e $\operatorname{Im} \alpha = \ker \beta$. Observemos que estamos denotando por 0 es grupo aditivo con un único elemento, el 0, que es un módulo sobre cualquier anillo.

Por ejemplo, dado un homomorfismo de módulos $f : M \to N$, se tiene una sucesión exacta corta

$$0 \longrightarrow \ker f \longrightarrow M \longrightarrow \operatorname{Im} f \longrightarrow 0$$

donde el morfismo $\ker f \to M$ no es más que la inclusión, y $M \to \operatorname{Im} f$ es la correstricción de f.

Proposición 2.2.8. *Sea* $0 \longrightarrow L \xrightarrow{\psi} M \xrightarrow{\varphi} N \longrightarrow 0$ *una sucesión exacta de* A*–módulos.*

1. *Si* M *es finitamente generado, entonces* N *es finitamente generado.*

2. *Si* L *y* N *son finitamente generados, entonces* M *es finitamente generado.*

Demostración. 1. Puesto que φ es sobreyectivo, cualquier conjunto de generadores $\{m_1, \ldots, m_t\}$ de M da un conjunto de generadores $\{\varphi(m_1), \ldots, \varphi(m_t)\}$ para N.
2. Sea $\{n_1, \ldots, n_s\}$ un conjunto de generadores de N y escojamos, puesto que φ es sobreyectiva, $\{m_1, \ldots, m_s\} \subseteq M$ tal que

$$\varphi(m_i) = n_i \quad \text{para todo } i = 1, \ldots, s.$$

Sea $\{l_1, \ldots, l_t\}$ un conjunto de generadores de L. Si $m \in M$, entonces

$$\varphi(m) = \sum_i r_i n_i = \varphi(\sum_i r_i m_i)$$

para ciertos $r_1, \ldots, r_s \in R$. De esta forma,

$$m - \sum_i r_i m_i \in \ker \varphi.$$

Puesto que $\ker \varphi = \operatorname{Im} \psi$, vemos que existen $u_1, \ldots, u_t \in R$ tales que

$$m - \sum_i r_i m_i = \sum_j u_j \psi(l_j)$$

En resumen,

$$m = \sum_i r_i m_i + \sum_j u_j \psi(l_j),$$

de donde $\{m_1, \ldots, m_s, \psi(l_1), \ldots, \psi(l_t)\}$ es un conjunto de generadores de M. □

Merece la pena mencionar aquí que un submódulo de un módulo finitamente generado puede no ser finitamente generado, como muestra el siguiente ejercicio.

Ejercicio 20. Consideremos un anillo no trivial R y un conjunto infinito I. El anillo producto $R^I = \{(x_i)_{i \in I} : x_i \in R\}$ tiene como ideal al conjunto $R^{(I)}$ de las I–tuplas $(x_i)_{i \in I}$ tales que $x_i = 0$ salvo para un conjunto finito de índices i. En fácil ver que $R^{(I)}$, como ideal a izquierda de R^I, no es finitamente generado.

2.3. Condiciones de cadena

El Ejemplo 20 sugiere que, para algunos anillos, el concepto de módulo finitamente generado no es suficientemente bueno con respecto de las sucesiones exactas.

2.3.1. Módulos noetherianos

Definición 13. Un módulo M se dice *noetheriano* si todo submódulo de M es finitamente generado.

Por $\mathcal{L}(M)$ denotamos el conjunto de todos los submódulos de un módulo M. Consideramos dicho conjunto ordenado por inclusión.

Proposición 2.3.1. *Las siguientes condiciones son equivalentes para un módulo M:*

1. *M es noetheriano;*
2. *cualquier cadena $L_1 \subseteq L_1 \subseteq \cdots \subseteq L_n \subseteq \cdots$ de submódulos de M se estabiliza, esto es, existe $m \geq 1$ tal que $L_n = L_m$ para todo $n \geq m$;*
3. *cualquier subconjunto no vacío $\Gamma \subseteq \mathcal{L}(M)$ tiene un elemento maximal.*

Demostración. (1) $\Rightarrow$ (2). Dada la cadena $L_1 \subseteq L_2 \subseteq \cdots \subseteq L_n \subseteq \cdots$, tenemos el submódulo[3] $L = \bigcup_{n\geq 1} L_n$ de M. Si F es un conjunto finito de generadores de L entonces $F \subseteq L_m$ para algún m. Claramente, $L_m = L$, lo que implica $L_n = L_m$ para todo $n \geq m$.
(2) $\Rightarrow$ (3). Supongamos que existe $\Gamma \subseteq \mathcal{L}(M)$ no vacío sin elementos maximales. Dado $L_1 \in \Gamma$, L_1 no es maximal en Γ, de manera que existe $L_2 \in \Gamma$ que contiene propiamente a L_1. De esta manera, vemos que existe una cadena $L_1 \subset L_2 \cdots \subset L_n \subset \cdots$ de elementos de Γ con todas las inclusiones estrictas.
(3) $\Rightarrow$ (1). Denotemos por R el anillo. Dado un submódulo L de M, consideremos Γ el conjunto de todos los submódulos finitamente generados de L, y L' un elemento maximal de Γ. Si $L' \neq L$, tenemos la inclusión estricta $L' \subset L' + Rl$ para algún $l \in L \backslash L'$. Puesto que $L' + Rl$ es un submódulo finitamente generado de L, obtenemos que L' no es maximal, una contradicción. Así, $L = L'$ y L es finitamente generado. □

Proposición 2.3.2. *Sea $0 \longrightarrow L \xrightarrow{\psi} M \xrightarrow{\varphi} N \longrightarrow 0$ una sucesión exacta de módulos. Entonces M es noetheriano si y sólo si N y L son noetherianos.*

Demostración. Supongamos que M es noetheriano. Tenemos que $L \cong \operatorname{Im}\psi$ e $\operatorname{Im}\psi$ es un submódulo de M. Claramente, cualquier cadena de submódulos de $\operatorname{Im}\psi$ lo es de M y, al ser éste noetheriano, ha de estabilizarse. Esto prueba que $\operatorname{Im}\psi$ y, por tanto, L, es noetheriano.

Por otra parte, si

$$N_1 \subseteq N_2 \subseteq \cdots \subseteq N_n \subseteq \cdots$$

[3]En general, la unión de submódulos no es un submódulo, pero sí en el caso especial en que los submódulos forman una cadena para la inclusión.

es una cadena de submódulos de N, entonces

$$\varphi^{-1}(N_1) \subseteq \varphi^{-1}(N_2) \subseteq \cdots \subseteq \varphi^{-1}(N_n) \subseteq \cdots$$

es una cadena de submódulos de M. Como M es noetheriano, existe $m \geq 1$ tal que $\varphi^{-1}(N_n) = \varphi^{-1}(N_m)$ para todo $m \geq n$. Por tanto, $N_n = \varphi(\varphi^{-1}(N_n)) = \varphi(\varphi^{-1}(N_m)) = N_m$ para todo $n \geq m$.

Recíprocamente, supongamos que tanto L como N son noetherianos y consideremos una cadena $M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n \subseteq \cdots$ de submódulos de M. Usando que N y L son noetherianos, existe $m \geq 1$ tal que $\varphi(M_n) = \varphi(M_m)$ e $\operatorname{Im}\psi \cap M_n = \operatorname{Im}\psi \cap M_m$ para todo $n \geq m$. Ahora, tomado $x \in M_n$ con $n \geq m$, tenemos $\varphi(x) \in \varphi(M_n) = \varphi(M_m)$, luego $\varphi(x) = \varphi(y)$ para cierto $y \in M_m$. Por tanto, $x - y \in \ker\varphi \cap M_n = \operatorname{Im}\psi \cap M_n = \operatorname{Im}\psi \cap M_m$. Esto implica que $x \in M_m$. □

Corolario 2.3.3. *Sean M_1, M_2 dos módulos. Entonces $M_1 \oplus M_2$ es noetheriano si y sólo si M_1 y M_2 son noetherianos.*

Demostración. Tenemos la sucesión exacta

$$0 \longrightarrow M_1 \xrightarrow{\psi} M_1 \oplus M_2 \xrightarrow{\varphi} M_2 \longrightarrow 0\,,$$

donde $\psi(m_1) = (m_1, 0)$ para todo $m_1 \in M_1$, y $\varphi(m_1, m_2) = m_2$ para todo $(m_1, m_2) \in M_1 \oplus M_2$. El corolario se sigue ahora de la Proposición 2.3.2. □

Definición 14. Un anillo A es noetheriano a izquierda si ${}_AA$ es noetheriano.

El siguiente teorema muestra quizás la propiedad más interesante de los anillos noetherianos a izquierda.

Teorema 2.3.4. *Un anillo A es noetheriano a izquierda si y sólo si todo A–módulo finitamente generado es noetheriano.*

Demostración. Supongamos que ${}_AM$ es finitamente generado y que ${}_AA$ es noetheriano. En virtud de la Proposición 2.2.7, existe una sucesión exacta de A–módulos

$$0 \longrightarrow L \longrightarrow A^m \longrightarrow M \longrightarrow 0\,.$$

Por el Corolario 2.3.3, A^m es noetheriano y M deviene noetheriano por la Proposición 2.3.2. □

Corolario 2.3.5. *Sea $0 \longrightarrow L \xrightarrow{\psi} M \xrightarrow{\varphi} N \longrightarrow 0$ una sucesión exacta de módulos sobre un anillo noetheriano a izquierda. Entonces M es finitamente generado si y sólo si N y L son finitamente generados.*

Demostración. Se deduce del Teorema 2.3.4, junto con la Proposición 2.3.2. □

Ejemplo. Todo DIP es un anillo noetheriano.

2.3.2. Módulos artinianos

Existe una noción dual de la de módulo noetheriano, que pasamos a estudiar brevemente.

Proposición 2.3.6. *Las siguientes condiciones son equivalentes para un módulo* M*:*

1. M *satisface la condición de cadena descendente para submódulos, esto es, para cadena de submódulos de* M *de la forma*

$$N_1 \supseteq N_2 \supseteq \cdots \supseteq N_n \supseteq \cdots$$

existe un índice m *tal que* $N_n = N_m$ *para todo* $n \geq m$*;*

2. *todo subconjunto no vacío* $\Gamma \subseteq \mathcal{L}(M)$ *tiene un elemento minimal.*

Demostración. Se deja como ejercicio. □

Definición 15. Un módulo ${}_RM$ se dice *artiniano* si satisface las condiciones equivalentes de la Proposición 2.3.6.

Proposición 2.3.7. *Dada una sucesión exacta*

$$0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0\,,$$

se tiene que M *es artiniano si, y sólo si,* L *y* N *son artinianos.*

Demostración. Similar a la de la Proposición 2.3.2 □

Ejercicio 21. Sea p un número primo, y consideremos el conjunto

$$C_{p^\infty} = \{z \in \mathbb{C} : z^{p^n} = 1 \text{ para algún } n \geq 1\}$$

Comprobar que C_{p^∞} es un subgrupo del grupo multiplicativo

$$S^1 = \{z \in \mathbb{C} : |z| = 1\}.$$

Por tanto, C_{p^∞} es un grupo abeliano, que puede considerarse canónicamente como un $\mathbb{Z}$–módulo. Demostrar que C_{p^∞} es un $\mathbb{Z}$–módulo artiniano pero no es finitamente generado.

Ejercicio 22. Sea A un dominio de integridad conmutativo. Demostrar que, si el módulo regular A es artiniano, entonces A es un cuerpo.

Ejercicio 23. Sea K un cuerpo de característica 0 y $K[X]$ el anillo de polinomios. Consideremos la aplicación lineal $T : K[X] \to K[X]$ dada por $T(f) = f'$. Así que tenemos, sobre $K[X]$, definida una estructura de $K[X]$–módulo a través de T. Demostrar que, con esta estructura, $K[X]$ es un $K[X]$–módulo artiniano. Deducir que $K[X]$, con la estructura de $K[X]$–módulo descrita, no es isomorfo al $K[X]$–módulo regular.

2.4. Módulos de longitud finita

Vamos a introducir una clase de módulos de las mejor conocidas, sobre algunos anillos, eso sí.

Definición 16. Un módulo se dice *simple* si tiene, exactamente, dos submódulos (el submódulo cero y el total). Observemos que entendemos que un módulo simple es no nulo.

Ejemplo. Los espacios vectoriales simples son, precisamente, los de dimensión 1.

Ejemplo. Consideremos el $\mathbb{R}[X]$–módulo $(\mathbb{R}^3, T)$, donde T es el giro de ángulo $\pi/3$ en el espacio euclidiano $\mathbb{R}^3$ con eje de giro "vertical". Observemos que, tanto este eje, como el plano perpendicular al mismo, son $\mathbb{R}[X]$–módulos simples, bien que de dimensión real distinta.

Definición 17. Una cadena estricta de submódulos de un módulo M

$$\{0\} = M_0 \subset M_1 \subset \cdots \subset M_n = M \tag{2.7}$$

se dirá una *serie de composición*[4] *de* M si M_i/M_{i-1} es un módulo simple para todo $i = 1, \ldots, n$. El número n se llama longitud de la serie de composición.

Ejemplo. Para el módulo del Ejercicio 2.4 se pueden identificar dos series de composición.

Proposición 2.4.1. *Un módulo no nulo* M *admite una serie de composición si, y sólo si,* M *es noetheriano y artiniano.*

Demostración. Supongamos que M admite una serie de composición de longitud n. Argumentaremos por inducción sobre n. Si $n = 1$, entonces M es simple, lo que implica obviamente que es tanto noetheriano como artiniano. Supongamos ahora que $n > 1$, y consideremos una serie de composición de M como en (2.7). Entonces M_{n-1} admite una serie de composición de longitud $n - 1$, con lo que es noetheriano y artiniano por hipótesis de inducción, en tanto que M_n/M_{n-1} es simple, luego noetheriano y artiniano. Las proposiciones 2.3.2 y 2.3.7 implican que M es noetheriano y artiniano.

Recíprocamente, supongamos que M es tanto noetheriano como artiniano. Por ser artiniano, M contiene un módulo simple M_1 (es decir, un módulo minimal entre todos los módulos no nulos de M). Si ahora $M_1 \neq M$, tomamos M_2 minimal entre todos los módulos que contienen estrictamente a M_1, entonces M_2/M_1 es simple. De esta forma, vemos que existe una cadena

$$0 \subset M_1 \subset M_2 \subset \cdots$$

[4] sólo consideraremos series de composición finitas

que ha de terminar por ser M noetheriano. Por construcción, esta cadena habrá terminado cuando $M_n = M$ para algún n. Habremos así obtenido una serie de composición para M. □

Corolario 2.4.2. *Si*

$$0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$$

es una sucesión exacta de módulos no nulos, entonces M *admite una serie de composición si, y sólo si,* L *y* N *admiten sendas series de composición.*

Demostración. Consecuencia de las proposiciones 2.4.1, 2.3.2 y 2.3.7. □

Corolario 2.4.3. *Si* M_1 *y* M_2 *son módulos no nulos, entonces* $M_1 \oplus M_2$ *admite una serie de composición si, y sólo si, la admite tanto* M_1 *como* M_2*.*

Teorema 2.4.4 (Jordan-Hölder)**.** *Supongamos que un módulo* M *admite dos series de composición*

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

y

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

Entonces $n = m$ *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. 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 2.1. 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 σ 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 el Corolario 2.4.2, 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 derecha de la Figura 2.1. El segundo teorema de isomorfía (Ejercicio 17) 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

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

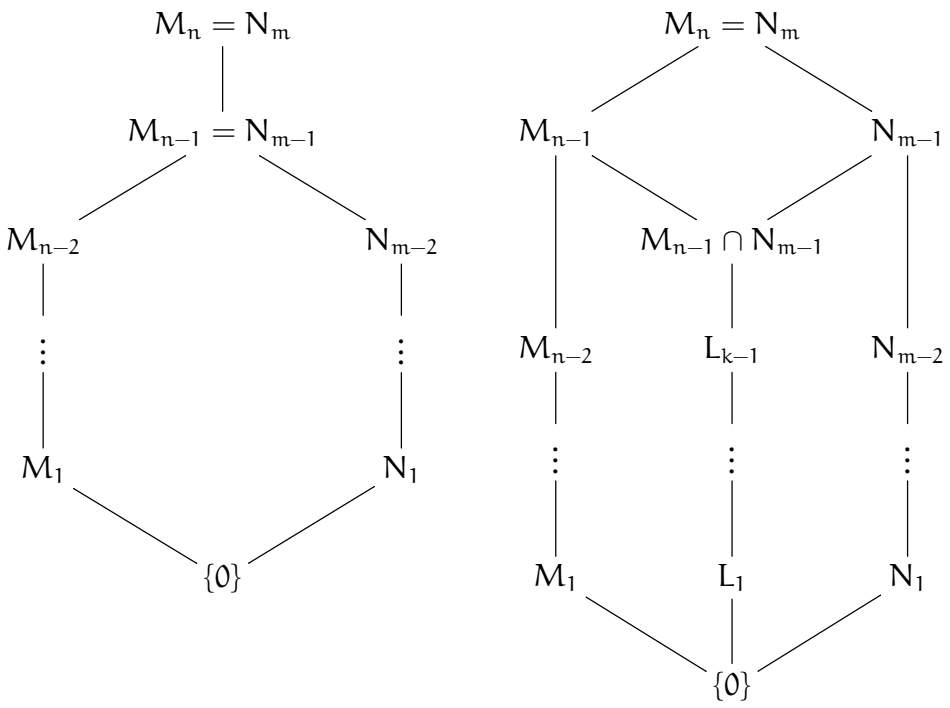


Figura 2.1: Diagramas de Hasse que describen el Caso 1 (izquierda) y el Caso 2 (derecha).

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

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

por lo que podemos aplicar de nuevo la hipótesis de inducción para obtener que $n-1 = m-1$ y la existencia de una permutación

$$\rho : \{1,\dots,n-1\} \to \{1,\dots,n-1\}$$

tal que $L_i/L_{i-1} \cong N_{\rho(i)}/N_{\rho(i)-1}$ para $i = 1,\dots,n-2$ 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 $\sigma : \{1,\dots,n\} \to \{1,\dots,n\}$ definida por

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

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 18. Diremos que un módulo M tiene *longitud finita* si es noetheriano y artiniano. En tal caso, definimos la *longitud* de M, denotada como $\ell(M)$, como la longitud de cualquiera de sus series de composición, cuando el módulo es no nulo. Entendemos que $\ell(\{0\}) = 0$.

Ejercicio 24. Demostrar que un espacio vectorial sobre un cuerpo es de longitud finita si, y sólo si, es de dimensión finita. ¿Qué relación hay entre longitud y dimensión?

Definición 19. 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 el Teorema de Jordan-Hölder muestra que están determinados, salvo isomorfismo y reordenación, por el propio módulo de longitud finita M.

Ejemplo. La longitud del grupo aditivo $\mathbb{Z}_n$ es la suma de las multiplicidades de cada primo en la descomposición completa de n.

Ejercicio 25. Sea ${}_AM$ un módulo no nulo. Demostrar que M es simple si, y sólo si, $\mathrm{ann}_A(m)$ es un ideal a izquierda maximal de A para todo elemento no nulo $m \in M$.

Ejercicio 26. Calcular todas las series de composición del $\mathbb{Z}$–módulo $\mathbb{Z}_2 \oplus \mathbb{Z}_4$.

2.4.1. El zócalo de un módulo de longitud finita

Cada módulo contiene un submódulo especialmente sencillo, llamado zócalo. Para definirlo, observemos que, si M es cualquier módulo y $\Gamma \subseteq \mathcal{L}(M)$ un subconjunto no vacío, entonces $\bigcap_{N\in\Gamma} N \in \mathcal{L}(M)$. Observemos que estamos afirmando que $\bigcap_{N\in\Gamma} N$ es un submódulo de M, pero no que pertenezca a Γ. Normalmente, esta observación se usa como sigue: se define Γ como la familia de los submódulos de M que verifican cierta propiedad que se mantiene por intersecciones, con lo que obtenemos el menor submódulo de M que posee esa propiedad.

Definición 20. El *zócalo* de un módulo M es el menor submódulo, en el sentido de la inclusión, de M que contiene a todos los submódulos simples de M. Usaremos la notación $\mathrm{Soc}(M)$ para referirnos al mismo. Si M no contiene ningún submódulo simple, entonces definimos $\mathrm{Soc}(M) = \{0\}$.

Ejercicio 27. Demostrar que $\mathrm{Soc}({}_AA) = \{0\}$ para todo dominio de integridad conmutativo A que no sea un cuerpo.

Ejercicio 28. Demostrar que $\mathrm{Soc}(V) = V$ para todo espacio vectorial V.

Seguidamente, nos interesamos en estudiar el zócalo de un módulo de longitud finita.

Proposición 2.4.5. *Sea M un módulo no nulo de longitud finita. Entonces existen submódulos simples $S_1, \ldots, S_n$ de M tales que $\mathrm{Soc}(M) = S_1 \dotplus \cdots \dotplus S_n$. Además, si $\mathrm{Soc}(M) = T_1 \dotplus \cdots \dotplus T_m$ para $T_1, \ldots, T_m$ submódulos simples de M, entonces $m = n$ y, tras eventual reordenación, $S_i \cong T_i$ para todo $i = 1, \ldots, n$.*

Demostración. Consideremos el conjunto Γ de submódulos de M de la forma $S_1 \dotplus \cdots \dotplus S_t$, para $S_1, \ldots, S_t$ submódulos simples de M. Puesto que M es de longitud finita no nulo, ha de contener al menos un módulo simple, ya que tiene una serie de composición. Por tanto, Γ es no vacío. Por la Proposición 2.4.1, M es noetheriano, así que Γ tiene un elemento maximal, digamos $S_1 \dotplus \cdots \dotplus S_n$. Por definición de zócalo, $S_1 \dotplus \cdots \dotplus S_n \subseteq \mathrm{Soc}(M)$.

Razonemos la inclusión recíproca. Si S es cualquier submódulo simple de M, y $S \cap (S_1 \dotplus \cdots \dotplus S_n) = \{0\}$, entonces $S \dotplus S_1 \dotplus \cdots \dotplus S_n \in \Gamma$. Pero esto contradice la maximalidad, así que $S \cap (S_1 \dotplus \cdots \dotplus S_n) \neq \{0\}$. Al ser S simple, esto implica que $S \subseteq S_1 \dotplus \cdots \dotplus S_n$ y, al ser S arbitrario, que $\mathrm{Soc}(M) \subseteq S_1 \dotplus \cdots \dotplus S_n$.

En lo que a la afirmación sobre la unicidad respecta, basta con aplicar el Teorema de Jordan-Hölder a las dos series de composición de $\mathrm{Soc}(M)$ dadas por

$$\{0\} \subset S_1 \subset S_1 \dotplus S_2 \subset \cdots \subset S_1 \dotplus \cdots \dotplus S_n = \mathrm{Soc}(M)$$

y

$$\{0\} \subset T_1 \subset T_1 \dotplus T_2 \subset \cdots \subset T_1 \dotplus \cdots \dotplus T_m = \mathrm{Soc}(M).$$

□

Definición 21. Un módulo se llama *semisimple* si $M = \mathrm{Soc}(M)$.

La Proposición 2.4.5 muestra que un módulo semisimple no nulo de longitud finita es isomorfo a una suma directa finita de módulos simples determinados salvo isomorfismo.

Ejercicio 29. Un anillo A se dice ser un *anillo de división* si todo elemento no nulo a de A tiene un inverso multiplicativo, esto es, un elemento $b \in A$ tal que $ab = ba = 1$. Demostrar que A es un anillo de división si, y sólo si, ${}_AA$ es simple.

Ejercicio 30. Sea

$$0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$$

una sucesión exacta corta de módulos de longitud finita. Demostrar que $\ell(M) = \ell(L) + \ell(N)$.

Ejercicio 31. Sean L, N submódulos de un módulo de longitud finita M. Demostrar que

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

Ejercicio 32. Dado un grupo cíclico de orden finito m, visto como $\mathbb{Z}$–módulo, calcular su longitud y sus factores de composición.

Ejercicio 33. Sea A un dominio de ideales principales. Demostrar que ${}_AA$ es de longitud finita si, y sólo si, A es un cuerpo. Demostrar que, si I es un ideal no nulo de A, entonces el A–módulo A/I es de longitud finita. ¿Puedo deducir la longitud y los factores de composición de A/I a partir de un generador del ideal I?.

Ejercicio 34. Sea $A = M_2(K)$ el anillo de matrices de orden 2 con coeficientes en un cuerpo K. Tomamos $m = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in A$. Calcular $\mathrm{ann}_A(m)$ y $\mathrm{Ann}_A(Am)$.

Ejercicio 35. Demostrar que el anillo de matrices $M_2(\mathbb{Q})$, visto como módulo regular, tiene un número infinito de series de composición, a pesar de que su longitud es 2.

Ejercicio 36. Sea K un cuerpo y

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

Comprobar que R es un subanillo de $M_2(K)$ y que los subconjuntos

$$F = \begin{pmatrix} K & K \\ 0 & 0 \end{pmatrix}, \quad C = \begin{pmatrix} 0 & K \\ 0 & K \end{pmatrix}$$

son ideales de R. ¿A qué anillo son isomorfos los anillos cocientes R/F y R/C? ¿Y el anillo $R/(F \cap C)$?

Ejercicio 37. Con la notación del Ejercicio 36. Comprobar que, para W un subespacio vectorial de K^2, el conjunto

$$\begin{pmatrix} W \\ 0 \end{pmatrix} = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : (a,b) \in W \right\}$$

es un ideal a izquierda de $R = \begin{pmatrix} K & K \\ 0 & K \end{pmatrix}$. Demostrar que todo ideal a izquierda de R que no es de esa forma ha de ser R o bien $C = \begin{pmatrix} 0 & K \\ 0 & K \end{pmatrix}$. Calcular $\mathrm{Soc}({}_R R)$.

Ejercicio 38. Con la notación del Ejercicio 36. Calcular todos los homomorfismos de R–módulos $f : R/F \to R$.

Ejercicio 39. Con la notación del Ejercicio 36. Sea $T : Y \to X$ un homomorfismo de K–espacios vectoriales. Definimos

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + bf(y) \\ cy \end{pmatrix},$$

para $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in R = \begin{pmatrix} K & K \\ 0 & K \end{pmatrix}$ y $\begin{pmatrix} x \\ y \end{pmatrix} \in X \oplus Y$. Demostrar que el K–espacio vectorial $X \oplus Y$ es, de esta forma, un R–módulo.

Ejercicio 40. Demostrar que todo R–módulo es isomorfo a uno de los definidos en el Ejercicio 39.

2.5. Estructura de los módulos de longitud finita sobre un DIP

En esta sección, vamos a desentrañar la estructura de los módulos de longitud finita sobre un DIP. Comencemos conectando la noción de longitud finita y los módulos acotados, para los que ya establecimos su descomposición primaria en el Ejemplo 2.2.2.

A lo largo de esta sección A denotará un DIP que no es un cuerpo.

Lema 2.5.1. *Un módulo ${}_A M$ es de longitud finita si, y sólo si, es finitamente generado y acotado.*

Demostración. Como los módulos de longitud finita son siempre finitamente generados, podemos suponer que M lo es, y tomar generadores $m_1, \ldots, m_s \in M$, esto es,

$$M = Am_1 + \cdots + Am_s.$$

Deducimos que

$$\mathrm{Ann}_A(M) = \mathrm{ann}_A(m_1) \cap \cdots \cap \mathrm{ann}_A(m_s). \tag{2.8}$$

Como A es un DIP, existen $f_1, \ldots, f_s \in A$ tales que $\mathrm{ann}_A(m_i) = \langle f_i \rangle$ para $i = 1, \ldots, s$. Deducimos entonces de (2.8) que

$$\mathrm{Ann}_A(M) = \bigcap_{i=1}^{s} \langle f_i \rangle = \langle \mu \rangle, \tag{2.9}$$

para μ un mínimo común múltiplo de $f_1, \ldots, f_s$.

Si M es de longitud finita, entonces lo es cada $Am_i \cong A/\langle f_i \rangle$. De acuerdo con el Ejercicio 33, cada $f_i \neq 0$, lo que implica que $\mu \neq 0$, es decir, M es acotado.

Recíprocamente, si M es acotado, entonces $\mu \neq 0$. Esto sólo es posible si $f_i \neq 0$ para todo $i = 1, \ldots, s$. Como cada $Am_i \cong A/\langle f_i \rangle$, deducimos del Ejercicio 33 que los módulos cíclicos $Am_1, \ldots, Am_s$ son todos de longitud finita. Ahora, tomemos el epimorfismo de módulos

$$Am_1 \oplus \cdots \oplus Am_s \to Am_1 + \cdots + Am_s, \quad ((a_1 m_1, \ldots, a_s m_s) \mapsto a_1 m_1 + \cdots + a_s m_s),$$

que muestra que $M = Am_1 + \cdots + Am_s$ es de longitud finita. □

Vamos ahora a indagar sobre la estructura de las componentes primarias establecidas en la Sección 2.2.2.

Definición 22. Tomemos un primo $p \in A$. Diremos que M es p–*primario* si $\mathrm{Ann}_A(M) = \langle p^t \rangle$ para cierto $t \geq 1$.

Observación 4. Para un A–módulo p–primario de longitud finita M, existe $x \in M$ tal que $\mathrm{Ann}_A(M) = \mathrm{ann}_A(x)$. En efecto, si $\mathrm{Ann}_A(M) = \langle p^t \rangle$ y $m \in M$, entonces $\mathrm{ann}_A(m) \supseteq \langle p^t \rangle$, por lo que $\mathrm{ann}_A(m) = \langle p^r \rangle$ para cierto $r \leq t$. En vista de (2.8), alguno de los generadores m_i de M ha de verificar que $\langle p^t \rangle = \mathrm{ann}_A(m_i)$. Tómese $x = m_i$.

Lema 2.5.2. *Sea M un A–módulo p–primario de longitud finita. Se tiene que*

$$\mathrm{Soc}(M) = \{m \in M : pm = 0\}. \tag{2.10}$$

Demostración. Si $0 \neq m \in M$ es tal que $pm = 0$, entonces, puesto que $\langle p \rangle$ es un ideal maximal, deducimos que $\mathrm{ann}_A(m) = \langle p \rangle$. Por tanto, Am es simple y $Am \subseteq \mathrm{Soc}(M)$. Para razonar el recíproco, tenemos, por la Proposición 2.4.5, que $\mathrm{Soc}(M) = S_1 \dotplus \cdots \dotplus S_t$ para ciertos submódulos simples S_i de M. Deducimos que

$$\langle p^t \rangle = \mathrm{Ann}_A(M) \subseteq \mathrm{Ann}_A(\mathrm{Soc}(M)) = \mathrm{Ann}_A(S_1) \cap \cdots \cap \mathrm{Ann}_A(S_t).$$

Así, cada $\mathrm{Ann}_A(S_i)$ es un ideal maximal de A que contiene a $\langle p^t \rangle$, luego $\mathrm{Ann}_A(\mathrm{Soc}(M))\langle p \rangle$. Deducimos que $\mathrm{Ann}_A(\mathrm{Soc}(M)) = \langle p \rangle$. De aquí, $pm = 0$ para todo $m \in \mathrm{Soc}(M)$. □

Proposición 2.5.3. *Supongamos que* M *es* p*–primario de longitud finita con* $\mathrm{Ann}_A(M) = \langle p^t \rangle$*. Si* $x \in M$ *es tal que* $\mathrm{ann}_A(x) = \langle p^t \rangle$*, entonces* Ax *es un sumando directo de* M*.*

Demostración. Expondremos una demostración por inducción sobre $\ell(M)$, la longitud de M. Si $\ell(M) = 1$, entonces $M = Ax$ y no hay nada que demostrar. Supongamos, pues, que $\ell(M) > 1$. De nuevo, si $Ax = M$, no tenemos que demostrar nada, así que supongamos que $Ax \neq M$.

Razonemos primero que existe $y \in M$ tal que $y \notin Ax$ y $\mathrm{ann}_A(y) = \langle p \rangle$. Como M/Ax es un módulo no nulo de longitud finita, contiene algún A–submódulo simple, digamos S. Tomemos $s \in S$ tal que $S = As$. Tenemos que

$$\langle p^t \rangle = \mathrm{Ann}_A(M) \subseteq \mathrm{Ann}_A(M/Ax) \subseteq \mathrm{Ann}_A(S) = \mathrm{ann}_A(s).$$

Puesto que S es simple, $\mathrm{ann}_A(s)$ es un ideal maximal de A lo que, en la situación presente, implica que $\mathrm{ann}_A(s) = \langle p \rangle$.

Tomemos ahora $z \in M$ tal que $s = z + Ax$. Tenemos que $pz \in Ax$, por lo que existe $a \in A$ tal que $pz = ax$. Observemos que $p^{t-1}ax = p^t z = 0$, con lo que $p^{t-1}a \in \mathrm{ann}_A(x) = \langle p^t \rangle$. Por tanto, $a = pa'$ para cierto $a' \in A$. Luego $pz = pa'x$, de donde $p(z - a'x) = 0$. Tomamos, pues, $y = z - a'x \neq 0$, elemento no nulo porque $z \notin Ax$.

Como Ay es simple (puesto que $\mathrm{ann}_A(y) = \langle p \rangle$), e $y \notin Ax$, deducimos que $Ax \cap Ay = \{0\}$. Así,

$$Ax \cong \frac{Ax}{Ax \cap Ay} \cong \frac{Ax + Ay}{Ay} = A(x + Ay) \subseteq \frac{M}{Ay}.$$

Como consecuencia,

$$\langle p^t \rangle = \mathrm{ann}_A(x) = \mathrm{Ann}_A(A(x + Ay)) \supseteq \mathrm{Ann}_A(M/Ay) \supseteq \mathrm{Ann}_A(M) = \langle p^t \rangle.$$

Deducimos que $x + Ay$ y M/Ay están bajo las mismas hipótesis que x y M, pero $\ell(M/Ay) < \ell(M)$. Por tanto, podemos aplicar la hipótesis de inducción, lo que nos da un submódulo N de M tal que $Ay \subseteq N$ y

$$\frac{M}{Ay} = \frac{Ax + Ay}{Ay} \dotplus \frac{N}{Ay}. \tag{2.11}$$

Deducimos de aquí que

$$M = Ax + Ay + N = Ax + N.$$

Puesto que la suma (2.11) es directa, tenemos también que

$$Ax \cap N \subseteq (Ax + Ay) \cap N = Ay.$$

De donde

$$Ax \cap N = Ax \cap N \cap Ay \subseteq Ax \cap Ay = \{0\}.$$

Concluimos, así, que $M = Ax \dotplus N$. □

Estamos preparados para obtener la descomposición cíclica de un módulo primario.

Teorema 2.5.4. *Sea* M *un* A*–módulo* p*–primario no nulo de longitud finita, para* p *un primo de* A*. Entonces existen elementos no nulos* $x_1, \ldots, x_n \in M$ *tales que*

$$M = Ax_1 \dotplus \cdots \dotplus Ax_n \tag{2.12}$$

y

$$\mathrm{Ann}_A(M) = \mathrm{ann}_A(x_1) \subseteq \mathrm{ann}_A(x_2) \subseteq \cdots \subseteq \mathrm{ann}_A(x_n). \tag{2.13}$$

Además, si $y_1, \ldots, y_m \in M$ *son elementos no nulos tales que*

$$M = Ay_1 \dotplus \cdots \dotplus Ay_m \tag{2.14}$$

con

$$\mathrm{ann}_A(y_1) \subseteq \mathrm{ann}_A(y_2) \subseteq \cdots \subseteq \mathrm{ann}_A(y_m), \tag{2.15}$$

entonces $m = n$ *y* $\mathrm{ann}_A(y_i) = \mathrm{ann}_A(x_i)$ *para* $i = 1, \ldots, n$*.*

Demostración. Sea $x_1 \in M$ tal que $\mathrm{Ann}_A(M) = \mathrm{ann}_A(x_1)$, que existe en virtud de la Observación 4. Por la Proposición 2.5.3, $M = Ax_1 \dotplus N$ para cierto A–submódulo N de M. Si $Ax_1 = M$, no hay nada que demostrar, en lo que concierne a la existencia de la descomposición en suma directa interna (2.12). Si $Ax_1 \neq M$ tenemos, argumentando por inducción sobre la longitud, que

$$N = Ax_2 \dotplus \cdots \dotplus Ax_n$$

para ciertos elementos no nulos $x_2, \ldots, x_n \in N$ tales que

$$\mathrm{Ann}_A(N) = \mathrm{ann}_A(x_2) \subseteq \cdots \subseteq \mathrm{ann}_A(x_n).$$

Como $\mathrm{Ann}_A(M) \subseteq \mathrm{Ann}_A(N)$, concluimos que $\mathrm{ann}_A(x_1) \subseteq \mathrm{ann}_A(x_2)$.

Razonemos la unicidad por inducción sobre la longitud de M. Si M es simple, entonces $M = Ax_1 = Ay_1$ y, por tanto, $\mathrm{ann}_A(x_1) = \langle p \rangle = \mathrm{ann}_A(y_1)$. Supongamos, pues, que M no es simple.

El A–módulo M/pM es semisimple en virtud del Lema 2.5.2, puesto que $\mathrm{Ann}_A(M/pM) = \langle p \rangle$. El homomorfismo

$$M \to \frac{Ax_1}{Apx_1} \oplus \cdots \oplus \frac{Ax_n}{Apx_n}$$

dado por

$$\sum_{i=1}^{n} a_i x_i \mapsto (a_1 x_1 + Apx_1, \ldots, a_n x_n + Apx_n)$$

es sobreyectivo y tiene por núcleo[5] pM. Tenemos así un isomorfismo de A–módulos

$$\frac{M}{pM} \cong \frac{Ax_1}{Apx_1} \oplus \cdots \oplus \frac{Ax_n}{Apx_n}.$$

Puesto que Ax_i/Apx_i es cíclico no nulo generado por $x_i + Apx_i$ y $\mathrm{ann}_A(x_i + Apx_i) = \langle p \rangle$, deducimos que es simple para todo $i = 1, \ldots, n$. Esto demuestra que n es, precisamente, la longitud de M/pM. Como el anterior razonamiento es aplicable también a la descomposición (2.14), deducimos que $n = m$.

Si $pM = \{0\}$, deducimos del Lema 2.5.2 que todos los anuladores que aparecen en (2.13) y (2.15) son iguales a $\langle p \rangle$.

Tratemos ahora el caso $pM \neq \{0\}$. Este módulo tiene longitud menor que la de M (ya que $pM \neq M$). Tenemos que

$$pM = Apx_1 \dotplus \cdots \dotplus Apx_r$$

para un índice $r \leq n$ tal que $\mathrm{ann}_A(x_i) = \langle p \rangle$ si, y sólo si, $i > r$. Asimismo,

$$pM = Apy_1 \dotplus \cdots \dotplus Apy_s$$

para $s \leq n$ tal que $\mathrm{ann}_A(y_i) = \langle p \rangle$ si, y sólo si, $i > s$. Escribamos, para $1 \leq i \leq r$, $\mathrm{ann}_A(x_i) = \langle p^{t_i} \rangle$, con $t_i > 1$. Tenemos, así, que $\mathrm{ann}_A(px_i) = \langle p^{t_i - 1} \rangle$. Como consecuencia,

$$\mathrm{ann}_A(px_1) \subseteq \cdots \subseteq \mathrm{ann}_A(px_r).$$

Análogamente, escribiendo $\mathrm{ann}_A(y_i) = \langle p^{s_i} \rangle$, vemos que $\mathrm{ann}_A(py_i) = \langle p^{s_i - 1} \rangle$ para $1 \leq i \leq s$ y

$$\mathrm{ann}_A(py_1) \subseteq \cdots \subseteq \mathrm{ann}_A(py_s).$$

Por hipótesis de inducción, $r = s$ y $\mathrm{ann}_A(px_i) = \mathrm{ann}_A(py_i)$ para todo $1 \leq i \leq r$. De aquí se completa fácilmente la inducción. □

Corolario 2.5.5. *Si M es un A–módulo p–primario de longitud finita, entonces*

$$M \cong C_1 \oplus \cdots \oplus C_n$$

para $C_1, \ldots, C_n$ módulos cíclicos. Además, si

$$M \cong D_1 \oplus \cdots \oplus D_m$$

para $D_1, \ldots, D_m$ cíclicos, entonces $n = m$ y, tras eventual reordenación, $C_i \cong D_i$ para todo $i = 1, \ldots, n$.

Demostración. El isomorfismo

$$M \cong C_1 \oplus \cdots \oplus C_n$$

[5] Comprobar

permite dar $x_1, \dots, x_n \in M$ tales que

$$M = Ax_1 \dotplus \cdots \dotplus Ax_n$$

con $Ax_i \cong C_i$ para $i = 1, \dots, n$. Además, puesto que M es p–primario, así lo son todos estos módulos cíclicos, luego podemos, tras eventual reordenación, suponer que $\operatorname{ann}_A(x_1) \subseteq \cdots \subseteq \operatorname{ann}_A(x_n)$. Razonando de igual forma para el isomorfismo $M \cong D_1 \oplus \cdots \oplus D_m$, obtenemos $y_1, \cdots, y_m \in M$ también en las condiciones del Teorema 2.5.4 tales que $D_i \cong Ay_i$ para $i = 1, \dots, m$. El citado teorema implica que $n = m$ y que $\operatorname{ann}_A(x_i) = \operatorname{ann}_A(y_i)$ para $i = 1, \dots, n$. Así, para cada $i = 1, \dots, n$,

$$C_i \cong Ax_i \cong A/\operatorname{ann}_A(x_i) = A/\operatorname{ann}_A(y_i) \cong Ay_i \cong D_i,$$

lo que concluye la prueba. □

Ejercicio 41. Un módulo M se dice indescomponible si $M = N \dotplus L$ implica $N = \{0\}$ o $L = \{0\}$. Demostrar que si un módulo de longitud finita primario M sobre un DIP se descompone como $M \cong C_1 \oplus \cdots \oplus C_n$, para $C_1, \dots, C_n$ cíclicos, entonces estos cíclicos son indescomponibles.

Ejemplo. Si M es un grupo abeliano de longitud finita y p–primario, deducimos del Corolario 2.5.5 que $M \cong C_1 \oplus \cdots \oplus C_n$, para $C_1, \dots, C_n$ cíclicos p–primarios. Así, existen enteros positivos únicos $m_1, \dots, m_n$ tal que

$$M \cong \mathbb{Z}_{p^{m_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{m_n}}.$$

Observemos que M ha de ser finito.

Vamos seguidamente a considerar A–módulos de longitud finita no necesariamente primarios.

Teorema 2.5.6. *Sea M un módulo no nulo de longitud finita sobre un dominio de ideales principales A. Existen irreducibles $p_1, \dots, p_r \in A$ y números naturales no nulos $n_1, \dots, n_r$ y $e_{i1} \geq \cdots \geq e_{in_i}$ para $i = 1, \dots, r$, determinados unívocamente por M, tales que*

$$M = \dotplus_{i=1}^{r} \left(\dotplus_{j=1}^{n_i} Ax_{ij} \right), \tag{2.16}$$

para $x_{ij} \in M$ que verifican $\operatorname{ann}_A(x_{ij}) = \langle p_i^{e_{ij}} \rangle$ para todo $i = 1, \dots, r; j = 1, \dots, n_i$.

Estos parámetros determinan M salvo isomorfismos.

Demostración. Sea $\mu \in A$ la cota de M. Vimos en el Ejemplo 2.2.2 que, si $\mu = p_1^{e_1} \cdots p_r^{e_r}$ es la descomposición completa de μ, entonces tenemos una descomposición

$$M = M_1 \dotplus \cdots \dotplus M_r, \tag{2.17}$$

donde M_i es un submódulo p_i–primario de M para $i = 1, \dots, r$. Si ahora descomponemos cada componente primaria de acuerdo con el Teorema 2.5.4, obtenemos una descomposición como la de (2.16).

Seguidamente, hemos de discutir que los parámetros enunciados están determinados por el módulo M. Comencemos viendo de la descomposición primaria (2.17) es única. De hecho, si $M = N_1 \dotplus \cdots \dotplus N_t$, con $\mathrm{Ann}_A(N_i) = \langle s_i^{f_i} \rangle$, para $s_1, \ldots, s_t \in$ irreducibles distintos, entonces

$$\langle \mu \rangle = \mathrm{Ann}_A(M) = \bigcap_{i=1}^{t} \mathrm{Ann}_A(N_i) = \bigcap_{i=1}^{t} \langle s_i^{f_i} \rangle = \langle s_1^{f_1} \cdots s_t^{f_t} \rangle.$$

Por unicidad de la descomposición completa de μ en nuestro DIP, deducimos que, tras eventual reordenación, $t = r$, $s_i = p_i$ para $i = 1, \ldots, r$ y $f_i = e_i$ para $i = 1, \ldots, r$. De esta forma, tenemos que, para cada $i = 1, \ldots, r$,

$$N_i \subseteq \{m \in M : p^{e_i} m = 0\} = M_i,$$

donde la igualdad de la derecha se probó en el Ejemplo 2.2.2. Deducimos, pues, que $N_i = M_i$ para todo $i = 1, \ldots, r$.

Lo anterior puede aplicarse en particular a una descomposición como la de (2.16), con lo que obtenemos que, necesariamente,

$$M_i = \dotplus_{j=1}^{n_i} Ax_{ij}$$

para cada $i = 1, \ldots, r$. Deducimos, pues, que los parámetros $r, p_1, \ldots, p_r$ y $e_{11} = e_1, \ldots, e_{r1} = e_r$ están determinados por M.

El resto de los parámetros e_{ij} con $i = 1, \ldots, r$ y $j = 2, \ldots, n_r$ son unívocamente determinados por cada M_i en virtud del Teorema 2.5.4 □

Definición 23. La descomposición (2.16) se llama *descomposición cíclica primaria* de M. También se suele llamar así a cualquier descomposición establecida por un isomorfismo como suma directa externa de módulos cíclicos primarios. Los elementos $p_i^{e_{ij}} \in A$ se llaman *divisores elementales* de M.

Observación 5. Durante la demostración del Teorema 2.5.6, hemos probado que los irreducibles $p_1, \cdots, p_r \in A$ y los naturales $e_{11}, \ldots, e_{r1}$ vienen determinados por la factorización completa de la cota μ de M.

Ejercicio 42. Dado un módulo M de longitud finita sobre un DIP, expresar $\mathrm{Soc}(M)$ en términos de su descomposición cíclica primaria.

2.5.1. Estructura de un grupo abeliano finito

Supongamos un grupo abeliano finito M con $m \geq 2$ elementos. Visto como $\mathbb{Z}$–módulo, M es, obviamente, de longitud finita y se tiene que $m \in \mathrm{Ann}_{\mathbb{Z}}(M)$. Por tanto, $\mathrm{Ann}_{\mathbb{Z}}(M) = \langle \mu \rangle$ para un divisor μ de m. Más adelante veremos cómo calcular μ, si disponemos de información suficiente sobre M.

Podemos aplicar el Teorema 2.5.6 a M. A partir de esa descomposición interna, obtenemos que, si $\mu = p_1^{e_1} \cdots p_r^{e_r}$ es una descomposición completa de la cota, obtendremos que

$$M \cong \bigoplus_{i=1}^{r} \bigoplus_{j=1}^{n_i} \mathbb{Z}_{p^{e_{ij}}},$$

isomorfismo de grupos, para ciertos naturales $e_i = e_{i1} \geq \cdots \geq e_{in_i} \geq 1$. Comparando cardinales,

$$m = \prod_{i=1}^{r} \prod_{j=1}^{n_i} p_i^{e_{ij}},$$

de donde, si $m = p_1^{f_1} \cdots p_r^{f_r}$ es una factorización completa, se tiene que

$$f_i = \sum_{j=1}^{n_i} e_{ij}, \qquad (i = 1, \ldots, r).$$

Por ejemplo, si M tiene cardinal 12, entonces ha de ser isomorfo a uno de los dos siguientes grupos:

$$\mathbb{Z}_4 \oplus \mathbb{Z}_3, \qquad \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3.$$

El primero de ellos tiene anulador generado por 12, en tanto que el segundo tiene anulador $6\mathbb{Z}$.

2.5.2. Sucesiones linealmente recursivas

Consideremos el K–espacio vectorial $\mathcal{M} = Map(\mathbb{N}, K)$ de las sucesiones con valores en K, al que dotamos de estructura de $K[X]$–módulo mediante la regla

$$Xs(j) = s(j+1), \qquad s \in \mathcal{M}, \quad j \in \mathbb{N}.$$

Para $f \in K[X]$, ponemos $\mathcal{R}_f = \{s \in \mathcal{M} : fs = 0\}$, que es un $K[X]$–submódulo de $\mathcal{M}$.

Dado $f = \sum_{k=0}^{n} f_k X^k \in K[X]$, $s \in \mathcal{M}$, tenemos

$$fs(j) = \sum_{k=0}^{n} f_k s(j+k),$$

así, $fs = 0$ significa

$$f_n s(j+n) = -\sum_{k=0}^{n-1} f_k s(j+k),$$

y, si $f_n = 1$,

$$s(j+n) = -\sum_{k=0}^{n-1} f_k s(j+k), \qquad j \in \mathbb{N}. \tag{2.18}$$

Para cada natural $n \geq 1$, tenemos la aplicación K–lineal

$$r_n : \mathcal{M} \to K^n, \qquad s \mapsto (s(0), \ldots s(n-1)).$$

Lema 2.5.7. *Si* $f \in K[X]$ *tiene grado* $n \geq 1$ *entonces* $r_n : \mathcal{R}_f \to K^n$ *establece un isomorfismo de* K*–espacios vectoriales.*

Demostración. Como $\mathcal{R}_f$ es un K–subespacio vectorial de $\mathcal{M}$, deducimos que r_n es K–lineal. Que $r_n : \mathcal{R}_f \to K^n$ es biyectiva se deduce de (2.18). □

Proposición 2.5.8. *El* $K[X]$*–módulo* $\mathcal{R}_f$ *es cíclico e isomorfo a* $K[X]/\langle f\rangle$.

Demostración. Sea $s \in \mathcal{R}_f$ tal que $r_n(s) = (0, \ldots, 0, 1)$. Afirmamos que $\langle f\rangle = \operatorname{ann}_{K[X]}(s)$. Demostraremos que, si $g \in R$ es no nulo de grado $m < n$, entonces $gs \neq 0$. En efecto, si $g = \sum_{k=0}^{m} g_k X^k$, entonces

$$gs(n-1-m) = \sum_{k=0}^{m} g_k s(n-1-m+k) = g_m \neq 0.$$

Por tanto, f es de grado mínimo contenido en $\operatorname{ann}_{K[X]}(s)$, luego lo genera como ideal de $K[X]$. Tenemos así un isomorfismo de $K[X]$–módulos $K[X]/\langle f\rangle \cong K[X]s$. De esta forma, $K[X]s$ tiene dimensión n como K–espacio vectorial, que es, precisamente, la dimensión de $\mathcal{R}_f$, de acuerdo con el Lema 2.5.7. Por tanto, $K[X]s = \mathcal{R}_f$. □

Queremos dar una descripción más precisa de los módulos $\mathcal{R}_f$ para ciertos polinomios f. Consideremos un polinomio $p \in K[X]$, para K un cuerpo. Dicho polinomio define una función, que denotamos igual, $p : \mathbb{N} \to K$. Veamos que, si p tiene grado k, entonces $p \in \mathcal{R}_{(X-1)^{k+1}}$. Para ello, basta con que lo comprobemos para las funciones monomiales definidas por $m_k(j) = j^k$, para $j \in \mathbb{N}$. Observemos que

$$Xm_k - m_k = \sum_{l=0}^{k-1} \binom{k}{l} m_l,$$

lo que permite demostrar, por inducción sobre k, que $(X-1)^{k+1} m_k = 0$.

Se podría esperar, a primera vista, que $\{m_0, m_1, \ldots, m_k\}$ generasen el K–espacio vectorial $\mathcal{R}_{(X-1)^{k+1}}$. No obstante, esto no es cierto en general, ya que, por ejemplo, en característica 2, $m_2 = m_1$. Pasamos a describir una base que funciona en cualquier característica.

Para cada $k \in \mathbb{N}$, definimos la sucesión

$$d_k(j) = \binom{j+k}{k}, \quad (j \in \mathbb{N}).$$

Reduciendo módulo la característica, esta sucesión tiene sentido sobre cualquier cuerpo.

Se sigue de la identidad de Pascal que

$$Xd_k = d_k + Xd_{k-1}, \qquad (k \geq 0), \tag{2.19}$$

donde entendemos que $d_{-1} = 0$. Se deduce inmediatamente de (2.19) que

$$Xd_k = \sum_{l=0}^{k} d_l. \tag{2.20}$$

De aquí, se deduce fácilmente que $\{d_0, d_1, \ldots, d_k\}$ es una K–base de $\mathcal{R}_{(X-1)^{k+1}}$. Vamos a demostrar algo más general.

Para cada $\alpha \in K^\times$, definimos la sucesión $\gamma(\alpha) \in \mathcal{R}_{X-\alpha}$ por

$$\gamma(\alpha)(j) = \alpha^j, \qquad (j \in \mathbb{N}).$$

Proposición 2.5.9. *Una K–base de $\mathcal{R}_{(X-\alpha)^h}$ es $\{d_0\gamma(\alpha), \ldots, d_{h-1}\gamma(\alpha)\}$.*

Demostración. De (2.19), deducimos que, para $k \leq l$,

$$(X-1)^k d_l = X^k d_{l-k}. \tag{2.21}$$

La identidad (2.21) permite deducir, para $k \leq 1$, que

$$(X-1)^k d_{k-1} = (X-1)(X-1)^{k-1} d_{k-1} = (X-1)X^{k-1} d_0 = (X-1)d_0 = 0.$$

Por otra parte,

$$\begin{aligned}(X-\alpha)^k d_l\gamma(\alpha) &= (X-\alpha)^{k-1}(X-\alpha)d_l\gamma(\alpha)\\ &= (X-\alpha)^{k-1}(Xd_lX\gamma(\alpha) - \alpha d_l\gamma(\alpha))\\ &= (X-\alpha)^{k-1}(Xd_l - d_l)\alpha\gamma(\alpha)\\ &= (X-1)(X-\alpha)^{k-1}d_l\alpha\gamma(\alpha).\end{aligned}$$

Esta última igualdad permite demostrar, por inducción sobre k, que

$$(X-\alpha)^k d_l\gamma(\alpha) = (X-1)^k d_l\alpha^k\gamma(\alpha). \tag{2.22}$$

Deducimos de (2.22) y (2.19) que $\{d_0\gamma(\alpha), \ldots, d_{h-1}\gamma(\alpha)\} \subset M_{(X-\alpha)^h}$.

Para comprobar que se trata de un conjunto linealmente independiente, supongamos

$$s = \sum_{k=0}^{l} c_k d_k\gamma(\alpha) = 0$$

para $l \leq h-1$, $c_0, \ldots, c_l \in K$ con $c_l \neq 0$. Entonces

$$0 = (X-\alpha)^l s = c_l d_0 \alpha^l\gamma(\alpha) = c_l\alpha^l\gamma(\alpha) \neq 0.$$

Contradicción ésta que muestra la independencia lineal y termina la demostración. □

Proposición 2.5.10. *Si la característica de K es cero, entonces una K–base de $\mathcal{R}_{(X-\alpha)^h}$ es $\{m_0\gamma(\alpha), \ldots, m_{h-1}\gamma(\alpha)\}$.*

Demostración. Cada d_k es, en característica 0, una función polinómica y, por tanto, combinación K–lineal de $m_0, \ldots, m_{h-1}$. Ahora aplicamos la Proposición 2.5.9. □

2.5.3. Ecuaciones diferenciales lineales

Una función $\varphi : \mathbb{R} \to \mathbb{C}$, podemos escribirla en la forma $\varphi = \varphi_r + i\varphi_c$, donde $\varphi_r, \varphi_c : \mathbb{R} \to \mathbb{R}$ son las funciones parte real y parte imaginaria de φ. Entendemos que φ es derivable si lo son φ_r, φ_c. La derivada es $\varphi' = \varphi_r' + i\varphi_c'$. Para tratar simultáneamente los casos real y complejo, denotaremos por $\mathbb{K}$ un cuerpo que puede ser $\mathbb{R}$ o $\mathbb{C}$. Consideremos el conjunto $\mathcal{F}$ de todas las funciones $\varphi : \mathbb{R} \to \mathbb{K}$ que tienen derivadas de cualquier orden. Se trata de un espacio vectorial sobre $\mathbb{K}$ y la aplicación que asigna a cada $\varphi \in \mathcal{F}$ su derivada es lineal. Tenemos, por tanto, que $\mathcal{F}$ es un $\mathbb{K}[X]$–módulo.

La aplicación $\tau : \mathcal{F} \to Map(\mathbb{N}, \mathbb{K})$ dada por

$$\tau(\varphi)(j) = \varphi^{(j)}(0)$$

es un homomorfismo de $\mathbb{K}[X]$–módulos. Deducimos que, para $\varphi \in \mathcal{F}$, se verifica que $\operatorname{ann}_{\mathbb{K}[X]}(\varphi) \subseteq \operatorname{ann}_{\mathbb{K}[X]}(\tau(\varphi))$. Por tanto, por restricción de τ, tenemos, para cada $f \in \mathbb{K}[X]$, un homomorfismo de $\mathbb{K}[X]$–módulos

$$\tau : \mathcal{F}_f \to \mathcal{R}_f.$$

donde $\mathcal{F}_f = \{\varphi \in \mathcal{F}_f : f\varphi = 0\}$, que es un $\mathbb{K}[X]$–submódulo de $\mathcal{F}$. En el caso $f = (X - \alpha)^h$, para $\alpha \in \mathbb{K}$, podemos dar explícitamente algunas funciones en $\mathcal{F}_{(X-\alpha)^h}$. Así, para cada $k \in \mathbb{N}$, definimos

$$\varphi_k^\alpha(t) = t^k e^{\alpha t}, \qquad (t \in \mathbb{R}).$$

Un sencillo cálculo muestra que

$$(\varphi_k^\alpha)' = k\varphi_{k-1}^\alpha + \alpha\varphi_k^\alpha,$$

equivalentemente,

$$(X - \alpha)\varphi_k^\alpha = k\varphi_{k-1}^\alpha, \tag{2.23}$$

igualdad válida para todo $k \in \mathbb{N}$ tomando $\varphi_{-1} = 0$. Se deduce que

$$\{\varphi_0^\alpha, \ldots, \varphi_{h-1}^\alpha\} \subset \mathcal{F}_{(X-\alpha)^h}.$$

Lema 2.5.11. *La aplicación $\tau : \mathcal{F}_{(X-\alpha)^n} \to \mathcal{R}_{(X-\alpha)^h}$ es un isomorfismo de $\mathbb{K}[X]$–módulos y $\{\varphi_0^\alpha, \ldots, \varphi_{h-1}^\alpha\}$ es una base de $\mathcal{F}_{(X-\alpha)^h}$ como $\mathbb{K}$–espacio vectorial.*

Demostración. Denotemos $\varphi_k = \varphi_k^\alpha$ por simplicidad y definamos $s_k = \tau(\varphi_k)$ para $k \in \mathbb{N}$. Demostremos que $s_0, s_1, \ldots$ es un conjunto linealmente independiente. Observemos que $s_0 \neq 0$. Razonando inductivamente, supongamos que $s_0, s_1, \ldots, s_k$ es linealmente independiente y supongamos una combinación lineal

$$0 = \sum_{l=0}^{k+1} a_l s_l, \qquad (a_0, \ldots, a_{k+1} \in \mathbb{K}). \tag{2.24}$$

Puesto que τ es un homomorfismo de $\mathbb{K}[X]$–módulos, deducimos de (2.23) que

$$(X-\alpha)s_l = ls_{l-1},$$

para todo $l \in \mathbb{N}$. Aplicando el operador $X-\alpha$ en la igualdad (2.24), deducimos que

$$0 = \sum_{l=0}^{k+1} la_l s_{l-1}.$$

Por hipótesis de inducción, obtenemos que $la_{l-1} = 0$ para $1 \leq l \leq k+1$, de donde $a_l = 0$ para $1 \leq l \leq k+1$. Pero, así, $a_0 s_0 = 0$, de donde $a_0 = 0$, asimismo.

Puesto que la dimensión como K–espacio vectorial de $\mathcal{R}_{(X-1)^h}$ es h, deducimos que $\{s_0, \ldots, s_{h-1}\}$ es una base. Como consecuencia, $\{\varphi_0, \ldots, \varphi_{h-1}\}$ es una base y $\tau : \mathcal{F}_{(X-\alpha)^h} \to \mathcal{R}_{(X-\alpha)^h}$ es un isomorfismo. □

Lema 2.5.12. *Sea $p \in \mathbb{R}[X]$ un polinomio mónico irreducible de grado 2 con raíces complejas $\alpha, \overline{\alpha}$. La aplicación $\tau : \mathcal{F}^{\mathbb{R}}_{p^h} \to \mathcal{R}^{\mathbb{R}}_{p^h}$ es un isomorfismo de $\mathbb{R}[X]$–módulos y*

$$\{\varphi_0^{\alpha} + \varphi_0^{\overline{\alpha}}, \ldots, \varphi_{h-1}^{\alpha} + \varphi_{h-1}^{\overline{\alpha}}, i(\varphi_0^{\alpha} - \varphi_0^{\overline{\alpha}}), \ldots, i(\varphi_{h-1}^{\alpha} - \varphi_{h-1}^{\overline{\alpha}})\} \tag{2.25}$$

es una base de $\mathcal{F}^{\mathbb{R}}_{p^h}$ como $\mathbb{R}$–espacio vectorial.

Demostración. Tenemos la descomposición primaria de $\mathcal{F}^{\mathbb{C}}_{p^h} = \mathcal{F}^{\mathbb{C}}_{(X-\alpha)^h} \dotplus \mathcal{F}^{\mathbb{C}}_{(X-\overline{\alpha})^h}$. El Lema 2.5.11, junto con un cambio de coordenadas claro, da que (2.25) es una base del espacio complejo $\mathcal{F}^{\mathbb{C}}_{p^h}$. Cada una de estas funciones coincide con su conjugada, así que, realmente, forman un conjunto linealmente independiente de $\mathcal{F}^{\mathbb{R}}_{p^h}$. Tenemos el diagrama conmutativo de homomorfismos de espacios vectoriales reales

$$\begin{array}{ccc} \mathcal{F}^{\mathbb{R}}_{p^h} & \xrightarrow{\tau} & \mathcal{R}^{\mathbb{R}}_{p^h} \\ \downarrow & & \downarrow \\ \mathcal{F}^{\mathbb{C}}_{p^h} & \xrightarrow{\tau} & \mathcal{R}^{\mathbb{C}}_{p^h}, \end{array}$$

donde las flechas verticales denotan inclusiones. Observemos que la aplicación τ de la línea inferior es un homomorfismo de $\mathbb{C}[X]$–módulos y, mirando las descomposiciones primarias de ambos módulos y el Lema 2.5.11, deducimos que se trata de un isomorfismo. Esto implica que la aplicación τ de la línea superior es inyectiva y, al ser lineal, su imagen tiene dimensión al menos $2h$ como subespacio vectorial real de $\mathcal{R}^{\mathbb{R}}_{p^h}$. Pero este último es un espacio vectorial de la misma dimensión, lo que concluye la prueba. □

Teorema 2.5.13. *Para cada polinomio no nulo $f \in \mathbb{K}[X]$, la aplicación $\tau : \mathcal{F}_f \to \mathcal{R}_f$ es un isomorfismo de $\mathbb{K}[X]$–módulos.*

Demostración. Podemos suponer que f es mónico. Partimos de una descomposición completa $f = p_1^{h_1} \cdots p_r^{h_r}$ para $p_1, \cdots, p_r \in \mathbb{K}[X]$ irreducibles y mónicos. Esto da lugar a sendas descomposiciones primarias de $\mathcal{F}_f$ y $\mathcal{R}_f$ de manera que tenemos

$$\tau : \dot{+}_{k=1}^{r} \mathcal{F}_{p_k^{h_k}} \longrightarrow \dot{+}_{k=1}^{r} \mathcal{R}_{p_k^{h_k}}.$$

Como τ es homomorfismo de $\mathbb{K}[X]$–módulos, preserva las componentes primarias, esto es, por restricción, tenemos $\tau : \mathcal{F}_{p_k^{h_k}} \to \mathcal{R}_{p_k^{h_k}}$ para cada $k = 1, \ldots, r$. Como cada p_k tiene grado uno o dos, gracias al Teorema Fundamental del Álgebra, deducimos que estas restricciones son todas isomorfismos por aplicación de los lemas 2.5.11 y 2.5.12. Por tanto, $\tau : \mathcal{F}_f \to \mathcal{R}_f$ es un isomorfismo. □

Corolario 2.5.14. *Si $\varphi \in \mathcal{F}_f$ satisface las condiciones iniciales $\varphi(0) = \cdots = \varphi^{(n-1)}(0) = 0$, para $n = \deg f$, entonces $\varphi = 0$.*

2.5.4. Estructura de un endomorfismo lineal. Forma de Jordan.

Vectores cíclicos y matrices compañeras. Teorema de Cayley-Hamilton.

Tomemos un operador lineal $T : V \to V$ actuando sobre un espacio vectorial de dimensión finita n sobre un cuerpo K. Sabemos (ver Ejercicio 11) que V es un $K[X]$–módulo cíclico si, y sólo si, el grado de su polinomio mínimo $\mu \in K[X]$ es n. Tomemos un generador $v \in V$ como $K[X]$–módulo (es lo que se llama un *vector cíclico* de T). Entonces

$$\{v, Tv, \ldots, T^{n-1}v\} \tag{2.26}$$

es un conjunto linealmente independiente de vectores de V y, como tiene cardinal n, resulta ser una base.

La matriz que expresa T en coordenadas con respecto de esta base es

$$C(\mu) = \begin{pmatrix} 0 & \ldots & 0 & -\mu_0 \\ 1 & \ldots & 0 & -\mu_1 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \ldots & 1 & -\mu_{n-1}, \end{pmatrix}$$

si $\mu = \mu_0 + \mu_1 X + \cdots + \mu_{n-1} X^{n-1} + X^n$. Esta es la llamada *matriz compañera* del polinomio μ.

Lema 2.5.15. *Sea $\mu \in K[X]$ un polinomio mónico. El polinomio característico de $C(\mu)$ es μ.*

Demostración. Se puede razonar por inducción sobre el grado de μ a la vista de la igualdad

$$\begin{vmatrix} X & 0 & 0 & \cdots & 0 & 0 & \mu_0 \\ -1 & X & 0 & \cdots & 0 & 0 & \mu_1 \\ 0 & -1 & X & \cdots & & & \mu_2 \\ \vdots & & \ddots & \ddots & & & \vdots \\ \vdots & & & \ddots & \ddots & & \vdots \\ 0 & 0 & 0 & \cdots & -1 & X & \mu_{n-2} \\ 0 & 0 & 0 & \cdots & & -1 & X+\mu_{n-1} \end{vmatrix} =$$

$$X\begin{vmatrix} X & 0 & \cdots & 0 & 0 & \mu_1 \\ -1 & X & \cdots & & & \mu_2 \\ & \ddots & \ddots & & & \vdots \\ & & \ddots & \ddots & & \vdots \\ 0 & 0 & \cdots & -1 & X & \mu_{n-2} \\ 0 & 0 & \cdots & & -1 & X+\mu_{n-1} \end{vmatrix} + (-1)^n\mu_0 \begin{vmatrix} -1 & X & 0 & \cdots & 0 & 0 \\ 0 & -1 & X & \cdots & & \\ \vdots & & \ddots & \ddots & & \\ \vdots & & & \ddots & \ddots & \\ 0 & 0 & 0 & \cdots & -1 & X \\ 0 & 0 & 0 & \cdots & & -1 \end{vmatrix}.$$

□

Proposición 2.5.16. *Un endomorfismo de un espacio vectorial de dimensión finita admite un vector cíclico si, y sólo si, su polinomio característico es su polinomio mínimo.*

Demostración. Denotemos por V el $K[X]$ módulo de dimensión n dado por un endomorfismo K–lineal T. Si hay un vector cíclico es porque V es cíclico como $K[X]$–módulo y la matriz de T en coordenadas con respecto de la base (2.26) es $C(\mu)$ para μ su polinomio mínimo. Por el Lema 2.5.15, el polinomio característico de $C(\mu)$ es el polinomio mínimo. Recíprocamente, si el polinomio mínimo μ coincide con el característico, entonces el grado de μ es la dimensión n de V y, por el Ejercicio 11, V es cíclico. □

No todo endomorfismo T posee un vector cíclico. En el caso general, lo que siempre se puede conseguir es que V, en tanto que $K[X]$–módulo, se escriba como suma directa de submódulos cíclicos (por ejemplo, mediante su descomposición cíclica primaria). Si descomponemos $V = V_1 \dotplus \cdots \dotplus V_t$, para V_i submódulos cíclicos, cada restricción $T_{|V_i} : V_i \to V_i$ admitirá un vector cíclico v_i y una base de la forma $\{v_i, Tv_i, \ldots, T^{n_i-1}v_i\}$. Uniendo estas bases obtenemos una de V en cuyas coordenadas la matriz de T es una matriz diagonal por bloques de la forma

$$\begin{pmatrix} C(f_1) & & \\ & \ddots & \\ & & C(f_t) \end{pmatrix}, \tag{2.27}$$

para f_i el polinomio mínimo de $T_{|V_i}$.

Teorema 2.5.17 (Cayley-Hamilton)**.** *El polinomio mínimo de una transformación lineal* $T : V \to V$ *de un espacio vectorial* V *es un divisor del polinomio característico de* T*.*

Demostración. Descomponemos V como suma directa de subespacios cíclicos que proporcionan una base en cuyas coordenadas la matriz de T es de la forma (2.27). El producto $f_1 \cdots f_t$ está contenido en el anulador de V como $K[X]$–módulo, así que es un múltiplo del polinomio mínimo. Pero $f_1 \cdots f_t$ es el polinomio característico de (2.27) y, por tanto, de T. □

Ejercicio 43. Sea $B \in M_n(F)$ y $F \leq K$ una extensión de cuerpos. Entonces el polinomio mínimo de B, vista como matriz de $M_n(K)$ es el mismo que considerada en $M_n(F)$.

Forma canónica de Jordan.

Supongamos que el polinomio mínimo de T es $\mu = (X-\lambda)^n$, para cierto $\lambda \in K$. Si n es la dimensión del K–espacio vectorial V, tenemos que, en tanto que $K[X]$–módulo, V es cíclico. Vamos a describir una base especial: tomemos $v \in V$ tal que $\operatorname{ann}_{K[X]}(v) = \langle (X-\lambda)^n \rangle$, y observemos que $\{v, (T-\lambda)v, \ldots, (T-\lambda)^{n-1}v\}$ es un conjunto linealmente independiente de vectores y, por tanto, una base de V.

La igualdad

$$T(T-\lambda)^i v = (T-\lambda+\lambda)(T-\lambda)^i v = (T-\lambda)^{i+1}v + \lambda(T-\lambda)^i v,$$

para $i \geq 0$ muestra que la matriz de T con respecto de la K–base

$$\{v, (T-\lambda)v, \ldots, (T-\lambda)^{n-1}v\}$$

es

$$J_n(\lambda) = \begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & \ldots & \ldots & \lambda \end{pmatrix}.$$

Llamaremos a una matriz del tipo $J_n(\lambda)$ bloque de Jordan de tamaño n para el valor propio λ.

Ahora, supongamos que T tiene polinomio mínimo

$$\mu = (X-\lambda_1)^{e_1} \cdots (X-\lambda_r)^{e_r},$$

para $\lambda_1, \ldots, \lambda_r \in K$. En virtud de Teorema 2.5.6, tenemos una descomposición de V como $K[X]$–módulo

$$V = \dotplus_{i=1}^{r} \left(\dotplus_{j=1}^{n_i} K[X]x_{ij} \right).$$

Tomando en cada $V_i = K[X]x_{ij}$ la base

$$\{x_{ij}, (T-\lambda_i)x_{ij}, \cdots, (T-\lambda_i)^{e_{ij}-1}x_{ij}\},$$

obtenemos, reuniéndolas, una base de V, con respecto de la cual la matriz de T adopta la forma diagonal por bloques

$$J = \begin{pmatrix} J_{e_{11}}(\lambda_1) & & & & & & & \\ & \ddots & & & & & & \\ & & J_{e_{1n_1}}(\lambda_1) & & & & & \\ & & & \ddots & & & & \\ & & & & J_{e_{r1}}(\lambda_r) & & & \\ & & & & & \ddots & & \\ & & & & & & J_{e_{rn_r}}(\lambda_r) & \end{pmatrix}$$

Teorema 2.5.18. *Sea $B \in M_n(F)$ una matriz cuadrada con coeficientes en un cuerpo F. Sea K una extensión de F donde el polinomio mínimo de B tiene todas sus raíces. Entonces existe $P \in GL_n(K)$ tal que*

$$J = PBP^{-1}.$$

Demostración. Consecuencia del Lema 43 y el desarrollo inmediatamente anterior al mismo. □

La matriz J se llama forma canónica de Jordan de la matriz B.

Corolario 2.5.19. *Una matriz $B \in M_n(F)$ es diagonalizable en alguna extensión K de F si, y sólo si, su polinomio mínimo es separable.*

Demostración. Observemos que B es diagonalizable si, y sólo si, cada bloque de Jordan de J es de tamaño 1×1. Equivalentemente, $e_i = 1$ para todo $i = 1, \ldots, r$. □

Corolario 2.5.20. *Si $B \in M_n(F)$ tiene n valores propios distintos en una extensión K de F, entonces B es diagonalizable sobre K.*

2.5.5. Potenciación y exponenciación de matrices. Sistemas de ecuaciones diferenciales.

Comencemos por mostrar cómo el uso de la forma canónica de Jordan facilita el cálculo de las potencias sucesivas de una matriz B. Para ello, escribamos $B = PJP^{-1}$ como en el Teorema 2.5.18 y observemos que $B^m = PJ^mP^{-1}$ para todo $m \in \mathbb{N}$. Por tanto, sólo necesitamos calcular las potencias J^m y, dada la forma

diagonal por bloques de J, basta con calcular las potencias de un bloque de Jordan $J_n(\lambda)$. Podemos escribir

$$J_n(\lambda) = \lambda I_n + J_n(0).$$

Usando esta expresión, obtenemos

$$J_n(\lambda)^m = \sum_{j=0}^{m} \binom{m}{j} \lambda^{m-j} J_n(0)^j.$$

Recordemos que el $\mathbb{K}$–espacio vectorial de las funciones de $\mathbb{R} \to \mathbb{K}$ indefinidamente derivables es un $\mathbb{K}[X]$–módulo con la acción $X\varphi = \varphi'$. Más generalmente, una función indefinidamente derivable $\mathbf{y} : \mathbb{R} \to \mathbb{K}^n$ puede entenderse como un elemento de $\mathcal{F}^n$, esto es, $\mathbf{y} = (y_1, \ldots, y_n)$ para $y_1, \ldots, y_n \in \mathcal{F}$. De esta forma, obtenemos el $\mathbb{K}[X]$–módulo $\mathcal{F}^n$, resultando $X\mathbf{y} = \mathbf{y}'$.

Vamos a estudiar las soluciones de un sistema homogéneo de EDOs lineales con coeficientes constantes. Un tal sistema puede escribirse de manera compacta como la búsqueda de las funciones $\mathbf{y} = \mathcal{F}^n$ tales que

$$\mathbf{y}' = \mathbf{y}B. \tag{2.28}$$

para una cierta matriz de coeficientes $B \in M_n(\mathbb{K})$. Nuestra primera observación es que, si $B = PCP^{-1}$ para $C \in M_n(\mathbb{K})$ y $P \in GL_n(\mathbb{K})$, entonces, realizando el cambio de variables $\mathbf{z} = \mathbf{y}P$, tenemos que el sistema (2.28) es equivalente a

$$\mathbf{z}' = \mathbf{z}C.$$

Podemos establecer este hecho en términos de módulos como sigue. Por $\mathcal{F}(B)$ denotamos el conjunto de soluciones en $\mathcal{F}^n$ de (2.28).

Lema 2.5.21. *La aplicación $\mathcal{F}(B) \to \mathcal{F}(C)$ que envía $\mathbf{y}$ en $\mathbf{z} = \mathbf{y}P$ es un isomorfismo de $\mathbb{K}[X]$–módulos.*

Demostración. Observemos primero que $\mathcal{F}(B)$ y $\mathcal{F}(C)$ son $\mathbb{K}[X]$–submódulos de $\mathcal{F}^n$, lo que es fácil de comprobar. La aplicación $\mathbf{y} \mapsto \mathbf{z}$ es claramente lineal y biyectiva. También es claro que es un homomorfismo de $\mathbb{K}[X]$–módulos. □

El siguiente lema permite usar lo demostrado para ecuaciones diferenciales lineales en la teoría de sistemas.

Lema 2.5.22. *Sea μ el polinomio mínimo de B. Si B admite un vector cíclico, entonces los $\mathbb{K}[X]$–módulos $\mathcal{F}(C(\mu))$ y $\mathcal{F}_\mu$ son isomorfos.*

Demostración. Como B posee un vector cíclico, podemos encontrar una base de $\mathbb{K}^n$ de manera que la aplicación lineal dada por B se expresa, en coordenadas con respecto de la misma, como mediante la matriz compañera $C(\mu)$. Así,

$B = PC(\mu)P^{-1}$ para una matriz inversible P. De modo que, según el Lema 2.5.21, $\mathcal{F}(B)$ y $\mathcal{F}(C(\mu))$ son $\mathbb{K}[X]$–módulos isomorfos. Ahora, consideremos la aplicación $\mathcal{F}^n \to \mathcal{F}$ proyección en la primera componente, que es, claramente, un homomorfismo de $\mathbb{K}[X]$–módulos. Una mera comprobación muestra que, por restricción de esta proyección, obtenemos un homomorfismo inyectivo de $\mathbb{K}[X]$–módulos $\mathcal{F}(C(\mu)) \to \mathcal{F}_\mu$. Finalmente, si $\varphi \in \mathcal{F}_\mu$, entonces $(\varphi, \varphi', \ldots, \varphi^{(n-1)}) \in \mathcal{F}(C(\mu))$, lo que muestra que el homomorfismo de $\mathbb{K}[X]$–módulos considerado es sobreyectivo y, por tanto, un isomorfismo. □

Teorema 2.5.23. *Dada una matriz inversible* P *tal que* $PCP^{-1} = B$*, para*

$$C = \begin{pmatrix} C(f_1) & & \\ & \ddots & \\ & & C(f_t) \end{pmatrix},$$

se tiene un isomorfismo de $\mathbb{K}[X]$*–módulos*

$$\mathcal{F}(B) \cong \mathcal{F}_{f_1} \oplus \cdots \oplus \mathcal{F}_{f_t}.$$

Como consecuencia, $\dim_{\mathbb{K}} \mathcal{F}(B) = n$*.*

Demostración. El Lema 2.5.21 nos permite reducirnos al caso $\mathcal{F}(C)$. La estructura por bloques de C nos da una descomposición

$$\mathcal{F}(C) = \mathcal{F}(C(f_1)) \dotplus \cdots \dotplus \mathcal{F}(C(f_t)).$$

Aplicamos, para terminar, el Lema 2.5.22. □

Corolario 2.5.24. *La aplicación* $\mathcal{F}(B) \to \mathbb{K}^n$ *que envía* $\mathbf{y}$ *en* $\mathbf{y}(0)$ *es un isomorfismo de espacios vectoriales.*

Demostración. En vista del Teorema 2.5.23, basta con que probemos que la aplicación, que es obviamente lineal, es inyectiva. Podemos reducirnos al caso $\mathcal{F}(C)$, para C como en el Teorema 2.5.23. La descomposición

$$\mathcal{F}(C) = \mathcal{F}(C(f_1)) \dotplus \cdots \dotplus \mathcal{F}(C(f_t))$$

muestra entonces que podemos reducirnos al caso $\mathcal{F}(C(f_i)$. Pero, si $\mathbf{z} \in \mathcal{F}(C(f_i)$ es tal que $\mathbf{z}(0) = 0$ entonces, aplicando el Corolario 2.5.14, obtenemos que $\mathbf{z} = 0$. □

Definimos la función exponencial

$$e^{tB} = \sum_{m=0}^{\infty} \frac{t^m B^m}{m!}, \tag{2.29}$$

ya que esta serie es absolutamente convergente para cada $t \in \mathbb{R}$.

Teorema 2.5.25. *Si dotamos a $\mathbb{K}^n$ de la estructura de $\mathbb{K}[X]$–módulo dada por el endomorfismo $\mathbb{K}$–lineal de $\mathbb{K}^n$ definido por B, entonces la aplicación $L : \mathbb{K}^n \to \mathcal{F}^n$ definida por $L(\mathbf{x}) = \mathbf{x}e^{tB}$ es un homomorfismo inyectivo de $\mathbb{K}[X]$–módulos cuya imagen es el conjunto de todas las soluciones de (2.28).*

Demostración. Derivando término a término con respecto de t la serie (2.29) obtenemos que

$$(e^{tB})' = e^{tB}B = Be^{tB}.$$

La aplicación L es claramente $\mathbb{K}$–lineal e inyectiva. Tomado $\mathbf{x} \in \mathbb{K}^n$, tenemos que

$$XL(\mathbf{x}) = \mathbf{x}(e^{tB})' = \mathbf{x}Be^{tB} = L(\mathbf{x}B) = L(X\mathbf{x}).$$

Así que L es un homomorfismo de $\mathbb{K}[X]$–módulos. Además, $\mathbf{y} = L(\mathbf{x})$ es una solución de (2.28):

$$\mathbf{y}' = \mathbf{x}(e^{tB})' = \mathbf{x}e^{tB}B = \mathbf{y}B.$$

Si $\mathbf{y}$ es solución de (2.28), tomamos $\mathbf{x} = \mathbf{y}(0)$. Tenemos que $\mathbf{z} = \mathbf{y} - \mathbf{x}e^{tB}$ es solución de (2.28) y $\mathbf{z}(0) = (0, \dots, 0)$. Por el Corolario 2.5.24, $\mathbf{z} = (0, \dots, 0)$ e $\mathbf{y} = \mathbf{x}e^{tB} = L(\mathbf{x})$. □

La descomposición cíclica primaria del $\mathbb{K}[X]$–módulo $(\mathbb{K}^n, B)$ da ahora un método para describir todas las soluciones de (2.28). De hecho, si denotamos por $\mathcal{F}(B)$ a dicho conjunto, el Teorema 2.5.25 nos dice que se trata de un $\mathbb{K}[X]$–submódulo de $\mathcal{F}$ y que $L : (\mathbb{K}^n, B) \to \mathcal{F}(B)$ dado por $L(\mathbf{x}) = \mathbf{x}e^{tB}$ es un isomorfismo de $\mathbb{K}[X]$–módulos. Así, si Si $\mu \in \mathbb{K}[X]$ es el polinomio mínimo de la matriz B, entonces $\mathrm{Ann}_{\mathbb{K}[X]}(\mathcal{F}(B)) = \langle \mu \rangle$. La descomposición cíclica primaria de $(\mathbb{K}^n, B)$ se traslada, mediante L, a la de $\mathcal{F}(B)$.

Ahora, supongamos

$$\mu = (X - \lambda_1)^{e_1} \cdots (X - \lambda_r)^{e_r},$$

para $\lambda_1, \dots, \lambda_r \in \mathbb{K}$. En virtud de Teorema 2.5.6, tenemos una descomposición de $\mathbb{K}^n$ como $\mathbb{K}[X]$–módulo

$$\mathbb{K}^n = \dot{+}_{i=1}^{r} \left(\dot{+}_{j=1}^{n_i} \mathbb{K}[X]\mathbf{x}_{ij} \right).$$

Tomamos en cada $V_i = \mathbb{K}[X]\mathbf{x}_{ij}$ la base

$$\{\mathbf{x}_{ij}, \mathbf{x}_{ij}(B - \lambda_i), \cdots, \mathbf{x}_{ij}(B - \lambda_i)^{e_{ij}-1}\},$$

y tendremos que una base de $\mathcal{F}(B)$ se obtiene reuniendo todas las bases

$$\{L(\mathbf{x}_{ij}), L(\mathbf{x}_{ij}(B - \lambda_i)), \cdots, L(\mathbf{x}_{ij}(B - \lambda_i)^{e_{ij}-1})\}$$

Esto indica que hemos de calcular cada solución

$$\mathbf{y}_{ijk} = L(\mathbf{x}_{ij}(B - \lambda_i)^k) = \mathbf{x}_{ij}(B - \lambda_i)^k e^{tB} = \mathbf{x}_{ijk}e^{tB},$$

donde $\mathbf{x}_{ijk} = \mathbf{x}_{ij}(B - \lambda_i)^k$. Observemos que

$$\mathbf{x}_{ijk}(B - \lambda_i)^{e_{ij}-k} = \mathbf{x}_{ij}(B - \lambda_i)^{e_{ij}} = 0.$$

Observemos ahora que

$$\mathbf{x}_{ijk}e^{tB} = \mathbf{x}_{ijk}e^{t(B-\lambda_i)+t\lambda_i} = \mathbf{x}_{ijk}e^{t(B-\lambda_i)}e^{t\lambda_i} = \left(\sum_{\ell=0}^{e_{ij}-k-1} \frac{t^\ell}{\ell!}(B - \lambda_i)^\ell\right) e^{t\lambda_i}.$$

Ejemplo. Discutamos el cálculo de la exponencial para matrices de orden 2.

En el caso de que $J = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$, para $\lambda_1, \lambda_2 \in \mathbb{R}$, que corresponde a polinomios mínimos $(X - \lambda_1)(X - \lambda_2)$ o bien $X - \lambda$, tenemos que

$$e^{tJ} = \begin{pmatrix} e^{t\lambda_1} & 0 \\ 0 & e^{t\lambda_2} \end{pmatrix}.$$

Cuando $\mu = (X - \lambda)^2$,

$$J = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix},$$

con $\lambda \in \mathbb{R}$, para el que

$$e^{tJ} = \begin{pmatrix} e^{\lambda t} & te^{\lambda t} \\ 0 & e^{\lambda t} \end{pmatrix}.$$

Esta última igualdad es consecuencia de que las matrices

$$\begin{pmatrix} \lambda t & 0 \\ 0 & \lambda t \end{pmatrix}, \begin{pmatrix} 0 & t \\ 0 & 0 \end{pmatrix}$$

conmutan, por lo que

$$e^{tJ} = e^{\begin{pmatrix} \lambda t & 0 \\ 0 & \lambda t \end{pmatrix}} e^{\begin{pmatrix} 0 & t \\ 0 & 0 \end{pmatrix}}.$$

Por otra parte,

$$e^{\begin{pmatrix} 0 & t \\ 0 & 0 \end{pmatrix}} = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix},$$

ya que, en este caso, el cuadrado de la matriz de la que calculamos la exponencial es cero.

En el caso de que el polinomio mínimo sea cuadrático e irreducible, entonces ha de ser de la forma $(X - \lambda)(X - \overline{\lambda})$, para $\lambda \in \mathbb{C} \setminus \mathbb{R}$. En este caso,

$$e^{tJ} = \begin{pmatrix} e^{t\lambda} & 0 \\ 0 & e^{t\overline{\lambda}} \end{pmatrix}.$$

Alternativamente, si no queremos usar números complejos, pongamos

$$\mu = X^2 + bX + c,$$

y definamos $\alpha = \sqrt{c - b^2/4}, \beta = -b/2$. De esta forma,

$$\mu = X^2 - 2\beta X + \alpha^2 + \beta^2.$$

Sea

$$B = \begin{pmatrix} 0 & -\alpha^2 - \beta^2 \\ 1 & 2\beta \end{pmatrix}$$

Tomamos $V = \mathbb{R}^2$ y $T : V \to V$ definido por $T(\mathbf{x}) = \mathbf{x}B$, para $\mathbf{x} \in V$.

Tomado un vector no nulo $v \in V$, tenemos la $\mathbb{R}$–base $\{-\alpha v, (T - \beta)v\}$ de V. Puesto que

$$T(-\alpha v) = -\alpha(T - \beta)v - \beta\alpha v,$$
$$T(T - \beta)v = (T^2 - \beta T)v = (2\beta T - \beta^2 - \alpha^2 - \beta T)v = \beta(T - \beta)v - \alpha\alpha v,$$

tenemos que la matriz de T con respecto de esta base es

$$C = \begin{pmatrix} \beta & -\alpha \\ \alpha & \beta \end{pmatrix}.$$

Puesto que

$$C = \begin{pmatrix} \beta & 0 \\ 0 & \beta \end{pmatrix} + \begin{pmatrix} 0 & -\alpha \\ \alpha & 0 \end{pmatrix},$$

y los sumandos conmutan entre sí, tenemos que

$$e^{tC} = \begin{pmatrix} e^{\beta t} & 0 \\ 0 & e^{\beta t} \end{pmatrix} \begin{pmatrix} \cos \alpha t & -\sin \alpha t \\ \sin \alpha t & \cos \alpha t \end{pmatrix},$$

donde hemos hecho uso del desarrollo en serie de potencias de las funciones trigonométricas.

Ejemplo. Sea ν un número real, y consideremos la sucesión $c_k = \cos k\nu$, con $k \in \mathbb{N}$. Vamos a ver que se trata de una sucesión linealmente recursiva. Vista como sucesión de números complejos, podemos escribir

$$c_k = \frac{e^{ik\nu} + e^{-ik\nu}}{2}.$$

Esto permite ver que el polinomio

$$X^2 - 2\cos \nu X + 1 = (X - e^{i\nu})(X - e^{-i\nu})$$

está en el anulador en $\mathbb{R}[X]$ de c_k, por lo que éste es no nulo. De hecho, al ser irreducible dicho polinomio en $\mathbb{R}[X]$, deducimos que

$$\operatorname{ann}_{\mathbb{R}[X]}(c_k) = \langle X^2 - 2\cos \nu X + 1 \rangle.$$

Obtenemos así la fórmula recursiva

$$\cos(k + 2)\nu = 2\cos(k + 1)\nu \cos \nu - \cos k\nu, \qquad (k \in \mathbb{N}).$$

Capítulo 3

Álgebra Lineal Básica sobre un anillo

3.1. Módulos no finitamente generados

Recordemos que, para un módulo M sobre un anillo R, denotamos por $\mathcal{L}(M)$ el conjunto ordenado por inclusión de todos los submódulos de M. Sabemos también que si $\Gamma \subseteq \mathcal{L}(M)$, entonces

$$\bigcap_{L\in\Gamma} L$$

es un submódulo de M. De hecho, se trata del menor submódulo de M que contiene a todos los submódulos pertenecientes a Γ.

Definición 24. Sea X un subconjunto de un módulo ${}_RM$. El menor submódulo de M que contiene a X se llama *submódulo de* M *generado por* X. Usaremos la notación RX para referirnos a él.

Lema 3.1.1. *Si* X *es un subconjunto de* ${}_RM$*, entonces*

$$RX = \left\{ \sum_{x\in F} r_x x : F \subseteq X \textit{ finito}, \, r_x \in R \right\}.$$

Demostración. Es fácil ver que el conjunto $\left\{\sum_{x\in F} r_x x : F \subseteq X \text{ finito}, \, r_x \in R\right\}$ es un submódulo de M que contiene a X. Así que ha de contener a RX. Pero RX contiene a X, así que cada elemento de la forma $\sum_{x\in F} r_x x \in RX$. Lo que concluye la demostración. □

Ejemplo. Si $X = \{x_1, \ldots, x_n\}$, entonces $RX = Rx_1 + \cdots + Rx_n$. Por tanto, los R–módulos M para los cuales existe un conjunto finito $X \subseteq M$ tales que $RX = M$ son, exactamente, los finitamente generados.

Consideremos una familia de R–módulos $\{M_i : i \in I\}$ indexados por un conjunto (finito o infinito) I. El producto cartesiano

$$\prod_{i\in I} M_i = \{(m_i)_{i\in I} : m_i \in M_i\}$$

es un R–módulo con la suma y la acción de R definidas componente a componente. Para cada $j \in I$, tenemos la aplicación $\iota_j : M_j \to \prod_{i\in I} M_i$ que asigna a cada $m \in M_j$ la I–tupla $\iota_j(m) = (m_i)_{i\in I}$ dada por

$$m_i = \begin{cases} m & \text{si } i = j \\ 0 & \text{si } i \neq j \end{cases}.$$

Cada ι_j es un monomorfismo de R–módulos y, por tanto, $\iota_j(M_j)$ es un submódulo del producto isomorfo al propio M_j.

La *suma directa externa* $\oplus_{i\in I} M_i$ de los módulos $\{M_i : i \in I\}$ se define como el menor submódulo de $\prod_{i\in I} M_i$ que contiene a todos los submódulos $\iota_j(M_j)$ con $j \in I$. Si, para $x = (x_i)_{i\in I} \in \prod_{i\in I} M_i$ definimos su soporte como $\operatorname{sop}(x) = \{i \in I : x_i \neq 0\}$, entonces un argumento sencillo muestra que

$$\bigoplus_{i\in I} M_i = \left\{ x \in \prod_{i\in I} M_i : \operatorname{sop}(x) \text{ es finito } \right\}.$$

Supongamos ahora que tenemos un conjunto $\{N_i : i \in I\}$ de submódulos de un módulo M. Por $\sum_{i\in I} N_i$ denotamos el menor submódulo de M que contiene a N_i para todo $i \in I$. A partir del Lema 3.1.1, es fácil deducir que

$$\sum_{i\in I} N_i = \left\{ \sum_{i\in F} n_i : F \subseteq I \text{ finito }, n_i \in N_i \right\}.$$

En notación simplificada, escribiremos

$$\sum_{i\in F} n_i = \sum_{i\in I} n_i,$$

entendiendo siempre que la suma es finita (o, si se quiere, que $n_i = 0$ para $i \notin F$).

Lema 3.1.2. *Existe un único homomorfismo de módulos* $\theta : \bigoplus_{i\in I} N_i \to \sum_{i\in I} N_i$ *tal que* $\theta\, \iota_i(m) = m$ *para todo* $i \in I$ *y todo* $m \in N_i$.

Demostración. Sencilla. □

Proposición 3.1.3. *Las siguientes condiciones son equivalentes para* $\{N_i \mid i \in I\} \subseteq \mathcal{L}(M)$*:*

1. *Para todo* $j \in I$ *se verifica que* $N_j \cap \sum_{j \neq i \in I} N_i = \{0\}$.
2. *Para todo subconjunto finito* $F \subseteq I$, *y todo* $j \in F$, *se verifica que* $N_j \cap \sum_{j \neq i \in F} N_i = \{0\}$.
3. *La expresión de cada elemento* $m \in \sum_{i \in I} N_i$ *como* $m = \sum_{i \in I} m_i$, *con* $m_i \in M_i$ *es única.*
4. *Si* $0 = \sum_{i \in I} m_i$ *con* $m_i \in M_i$, *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* $J_1, J_2 \subseteq I$ *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). Supongamos dos expresiones de m como suma de elementos de los módulos de la familia.

$$m = \sum_{i \in I} m_i = \sum_{i \in I} m_i'. \tag{3.1}$$

Tomemos $F \subseteq I$ finito tal que $m_i = m_i' = 0$ para todo $i \neq F$. Para todo $j \in F$ deducimos de (3.1) 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 θ 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 $\bigoplus_{i \in I} M_i$ con 'soporte' distinto. Pero esto es imposible, ya que θ se supone inyectivo.
(vi) $\Rightarrow$ (i). Evidente. □

Definición 25. En caso de verificarse las condiciones equivalentes de la Proposición 3.1.3, diremos que el submódulo $\sum_{i \in I} N_i$ es *suma directa interna* de los submódulos $\{N_i \mid i \in I\}$. Usaremos la notación $\dot{+}_{i \in I} N_i$ para referirnos a esta situación.

Corolario 3.1.4. *Si* $\{N_i \mid i \in I\}$ *es una familia submódulos de* ${}_RM$ *que satisface las condiciones equivalentes de la Proposición 3.1.3 y* N *es un submódulo de* M *tal que* $N \cap \dot{+}_{i \in I} N_i = \{0\}$, *entonces* $\{N_i \mid i \in I\} \cup \{N\}$ *satisface las condiciones equivalentes de la Proposición 3.1.3*

Demostración. Supongamos $0 = n + \sum_{i\in I} n_i \in N + \dot{+}_{i\in I} N_i$. entonces $n = -\sum_{i\in I} n_i \in N \cap \dot{+}_{i\in I} N_i = \{0\}$, de donde $n = \sum_{i\in I} n_i = 0$. Se sigue que $n_i = 0$ para todo $i \in I$. □

Definición 26. 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 $N_j \cap \sum_{j\neq i\in I} N_i = \{0\}$.

Ejemplo. Sea M un módulo sobre un DIP A. Definimos

$$\mathbf{t}(M) = \{m \in M : \mathrm{ann}_A(m) \neq \{0\}\}.$$

Es fácil comprobar que $\mathbf{t}(M)$ es un submódulo de M, llamado *submódulo de torsión*.

Para $p \in A$ irreducible, definamos

$$M_p = \{m \in M : p^e m = 0 \text{ para algún } e \geq 1\}.$$

Se comprueba sin dificultad que M_p es un A–submódulo de $\mathbf{t}(M)$. Denotemos por $\mathcal{P}$ a un conjunto de representantes de las clases de equivalencia de los elementos irreducibles bajo la relación ser asociados. Afirmamos que

$$\mathbf{t}(M) = \dot{+}_{p\in\mathcal{P}} M_p.$$

En efecto, si $m \in \mathbf{t}(M)$, entonces Am es un módulo de longitud finita, y podemos tomar su descomposición primaria $Am = m_1 \dot{+} \cdots \dot{+} m_t$. Así, $m = n_1 + \cdots + n_t$ con el anulador de $n_i \in N_i$ primario. Por tanto, $\mathbf{t}(M) = \sum_{p\in\mathcal{P}} M_p$. Para ver que la suma es directa, supongamos $0 = m_1 + \cdots + m_r$, con $m_i \in M_{p_i}$ para $p_1, \ldots, p_r \in \mathcal{P}$. Pero $L = Am_1 + \cdots + Am_r$ es un módulo de longitud finita y cada Am_i es p_i–primario. Razonando como en la Sección 2.2.2, $m_i = 0$ para todo $i = 1, \ldots, r$.

3.2. Resoluciones libres

Si, en la construcción de la suma directa externa, tomamos $M_i = R$ para todo $i \in I$, entonces obtenemos un R–módulo que denotamos por $R^{(I)}$, y que viene dado por

$$R^{(I)} = \{\mathbf{r} \in R^I : \mathrm{sop}(\mathbf{r}) \text{ es finito}\}.$$

Si denotamos, para cada $i \in I$, por ϵ_i el elemento de $R^{(I)}$ todas cuyas componentes son 0, salvo la i–ésima, que vale 1, tenemos que cada elemento $\mathbf{r} \in R^{(I)}$ se expresa de manera única como

$$\mathbf{r} = \sum_{i\in\mathrm{sop}(\mathbf{r})} r_i \epsilon_i, \tag{3.2}$$

con $r_i \in R$. Como antes, es usual escribir la igualdad (3.2) como $\mathbf{r} = \sum_{i\in I} r_i \epsilon_i$, entendiendo que $r_i = 0$ si $i \notin \mathrm{sop}(\mathbf{r})$.

Proposición 3.2.1. *Sea* M *un* R*–módulo y* $\{m_i : i \in I\} \subseteq M$*. Existe un único homomorfismo de* R*–módulos* $f : R^{(I)} \to M$ *tal que* $f(\epsilon_i) = m_i$ *para todo* $i \in I$*.*

Demostración. Un homomorfismo f que satisfaga la condición enunciada ha de verificar que

$$f(\sum_{i\in I} r_i\epsilon_i) = \sum_{i\in I} r_i f(\epsilon_i) = \sum_{i\in I} r_i m_i, \tag{3.3}$$

lo que prueba la unicidad. Como la representación de un elemento de $R^{(I)}$ en la forma $\sum_{i\in I} r_i\epsilon_i$ es única, la expresión (3.3) define una aplicación $f : R^{(I)} \to M$. No entraña dificultad comprobar que, así definida, f es un homomorfismo de R–módulos. □

Definición 27. Diremos que $\{m_i : i \in I\}$ es un *conjunto linealmente independiente* si la aplicación f establecida en la Proposición 3.2.1 es inyectiva, equivalentemente, la igualdad $0 = \sum_{i\in I} r_i m_i$ sólo es posible cuando $r_i = 0$ para todo $i \in I$.

Ejercicio 44. Demostrar que un grupo abeliano finito, visto como $\mathbb{Z}$–módulo, carece de conjuntos linealmente independientes.

Definición 28. Un conjunto linealmente independiente de generadores de un módulo se llama una *base*. Un módulo que admita una base se llamará *libre*. Por conveniencia, consideraremos el módulo cero como libre con base vacía.

Ejercicio 45. Demostrar que un módulo libre es finitamente generado si, y sólo si, tiene una base finita.

Ejemplo. El módulo $R^{(I)}$ es libre con base $\{\epsilon_i : i \in I\}$. Se desprende de la Proposición 3.2.1, y de la propia definición, que cada módulo libre es isomorfo a un módulo de la forma $R^{(I)}$.

Ejercicio 46. Demostrar que un conjunto de elementos $\{e_i : i \in I\}$ de un R–módulo F es una base si, y sólo si, para cualquier otro R–módulo M y cualquier subconjunto $\{m_i : i \in I\} \subseteq M$, existe un único homomorfismo de R–módulos $f : F \to M$ tal que $f(e_i) = m_i$ para todo $i \in I$.

El Ejercicio 46 permite demostrar que todo módulo admite una resolución libre, en el sentido especificado más abajo.

Proposición 3.2.2. *Sea* M *un módulo. Existe una sucesión exacta*

$$\cdots \xrightarrow{f_{-2}} F_{-1} \xrightarrow{f_{-1}} F_0 \xrightarrow{f_0} M \longrightarrow 0\,, \tag{3.4}$$

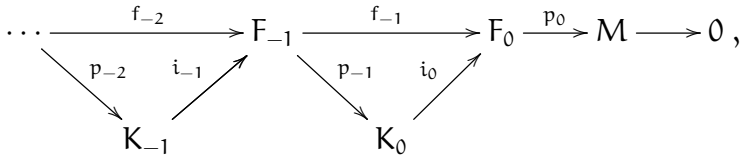
donde F_{-n} *es libre para todo* $n \in \mathbb{N}$*.*

Demostración. Dado un módulo M, podemos siempre tomar un conjunto de generadores $\{m_i : i \in I\}$ suyo. Tomemos un módulo libre F_0 con base $\{e_i : i \in I\}$. El Ejercicio 46 nos dice que existe un único homomorfismo de módulos $p_0 : F_0 \to M$ tal que $p_0(e_i) = m_i$ para todo $i \in I$, que resulta ser sobreyectivo de manera obvia. Si $K_0 = \ker p_0$, tenemos una sucesión exacta corta

$$0 \longrightarrow K_0 \longrightarrow F_0 \xrightarrow{p_0} M \longrightarrow 0\,, \tag{3.5}$$

que se llama *presentación libre* de M.

Podemos repetir el proceso para K_0, tomando un conjunto de generadores suyo, y construir una presentación libre de K_0, y, de hecho, podemos iterar el proceso para obtener la sucesión exacta que aparece en la fila de arriba del siguiente diagrama



donde

1. F_{-k} es un módulo libre para todo $k = 0, 1, 2, \ldots$,
2. $p_{-k} : F_{-k} \to K_{-k+1}$ es un homomorfismo sobreyectivo de módulos para $k = 1, 2, \ldots$,
3. K_{-k} es el núcleo de p_{-k} e i_{-k} denota la inclusión para $k = 0, 1, 2, \ldots$,
4. $f_{-k} = i_{-k+1} \circ p_{-k}$, para $k = 1, 2, \ldots$.

Llamando $f_0 = p_0$, obtenemos la sucesión exacta del enunciado. □

Definición 29. La sucesión exacta (3.4) se llama *resolución libre* de M. Obviamente, cada módulo tiene multitud de resoluciones libres. Si $F_{-n} = \{0\}$ para algún $n \geq 0$, diremos que la resolución es *finita*.

Ejercicio 47. Calcular una resolución libre finita para el $\mathbb{Z}$–módulo $\mathbb{Z}_2 \oplus \mathbb{Z}_4$.

Ejercicio 48. Demostrar, a partir su descomposición cíclica primaria, que un módulo de longitud finita M sobre un DIP admite una presentación libre finita de la forma

$$0 \longrightarrow F_{-1} \longrightarrow F_0 \longrightarrow M \longrightarrow 0$$

para F_{-1}, F_0 módulos libres con bases finitas.

3.3. Módulos finitamente presentados

Definición 30. Diremos que un módulo M es *finitamente presentado* si existe una resolución libre de M cuyos dos primeros términos F_0, F_{-1} son ambos libres finitamente generados, esto es, existe una sucesión exacta

$$F_{-1} \xrightarrow{f_{-1}} F_0 \xrightarrow{f_0} M \longrightarrow 0\,, \tag{3.6}$$

con F_{-1}, F_0 libres finitamente generados. Esta sucesión se llamará *presentación libre finita* de M.

Se desprende de la definición que todo módulo finitamente presentado es finitamente generado. El recíproco de esta afirmación no es cierto, como muestra la siguiente proposición.

Proposición 3.3.1. *Un anillo R es un noetheriano a izquierda si, y sólo si, todo módulo finitamente generado es finitamente presentado.*

Demostración. Supongamos que ${}_RM$ es finitamente generado y que ${}_RR$ es noetheriano.Tomamos una presentación libre de M de la forma (3.5) en la que que, por ser M finitamente generado, podemos suponer que F_0 es libre finitamente generado. Como R es noetheriano, tenemos que K_0 es también finitamente generado, luego, tomando de nuevo una presentación libre de K_0, obtenemos una presentación finita de M. Recíprocamente, necesitamos Schanuel. □

Si un R–módulo M es finitamente presentado y tenemos una presentación libre finita como (3.6), entonces el primer teorema de isomorfía nos da un isomorfismo de módulos

$$F_0/\operatorname{Im} f_{-1} \cong M.$$

Esto sugiere que si tenemos una representación suficientemente buena del homomorfismo f_{-1}, entonces dispondremos de un buen conocimiento del módulo M. Con esta motivación, pasaremos a estudiar la representación matricial de un homomorfismo entre dos módulos libres finitamente generados.

El conjunto de las matrices de tamaño $s \times t$ con coeficientes en R se denotará por $R^{s\times t}$. La suma de matrices, y el producto, cuando los tamaños de los factores lo permiten, se definen por las mismas reglas que en el caso usual de cuerpos.

Tomemos dos módulos libres finitamente generados E_s y F_t, y fijemos bases respectivas $e = \{e_1, \ldots, e_s\}$, $f = \{f_1, \ldots, f_t\}$. Cualquier homomorfismo de R–módulos $\psi : E_s \to F_t$ está determinado por una matriz $A_\psi = (a_{ij}) \in R^{s\times t}$ definida por las condiciones

$$\psi(e_i) = \sum_{j=1}^{t} a_{ij} f_j, \qquad (i = 1, \ldots, s).$$

Explícitamente, si $u = \sum_{i=1}^{s} x_i e_i$, entonces $\psi(u) = \sum_{j=1}^{t} y_j f_j$, donde $x = (x_1, \ldots, x_s) \in R^s$ e $y = (y_1, \ldots, y_t) \in R^t$ están relacionados por la igualdad

$$y = xA_\psi. \tag{3.7}$$

Si mejoramos un poco la notación, podemos llamar a x las *coordenadas* de u en la base $\{e_1, \ldots, e_s\}$, y usar la notación $u_e = x$. Esto da un isomorfismo de R–módulos $E_s \xrightarrow{(-)_e} R^s$. De este modo, (3.7) adopta la forma

$$\psi(u)_f = u_e A_\psi$$

o, más gráficamente, se tiene un diagrama conmutativo de homomorfismos de R–módulos

$$\begin{array}{ccc} E_s & \xrightarrow{\psi} & F_t \\ {\scriptstyle (-)_e}\downarrow & & \downarrow{\scriptstyle (-)_f} \\ R^s & \xrightarrow{\cdot A_\psi} & R^t \end{array}$$

es conmutativo. Aquí, el homomorfismo de la fila inferior viene dado por multiplicación a la derecha por la matriz A_ψ.

Ejercicio 49. Para una matrix $A \in R^{s\times t}$, denotamos por $row(A) \subseteq R^t$ el R–submódulo de R^t generado por las filas de A. Demostrar que existe un isomorfismo de R–módulos

$$\widetilde{f} : F_t/\operatorname{Im}\psi \to R^t/row(A_\psi)$$

que verifica

$$\widetilde{f}(v + \operatorname{Im}\psi) = v_f + row(A_\psi),$$

para todo $v \in R^t$.

Un cálculo sencillo muestra que, si

$$E_s \xrightarrow{\psi} F_t \xrightarrow{\phi} G_u$$

son homomorfismos entre módulos libres finitamente generados, entonces

$$A_{\phi\psi} = A_\psi A_\phi.$$

Ejemplo. Sea $T : V \to V$ una aplicación lineal definida sobre un K–espacio vectorial V. Consideremos V como $K[X]$–módulo y supongamos que V es de dimensión finita con base $\{v_1, \ldots, v_n\}$. Sea $B = (b_{ij}) \in K^{n\times n}$ la matriz que representa a T con respecto de la base fijada, esto es

$$T(v_i) = \sum_{j=1}^{n} b_{ij} v_j, \qquad (i = 1, \ldots, n). \tag{3.8}$$

Vamos a calcular una presentación libre finita de ${}_{K[X]}V$. Tomamos un $K[X]$–módulo libre F_n con base $\{f_1, \dots, f_n\}$. Definimos $\phi : F_n \to V$ por $\phi(f_i) = v_i$ para $i = 1, \dots, n$. Las igualdades (3.8) muestran que

$$Xf_i - \sum_{j=1}^{n} b_{ij} f_j \in \operatorname{Ker} \phi, \qquad (i = 1, \dots, n).$$

Vamos a demostrar que

$$\{Xf_i - \sum_{j=1}^{n} b_{ij} f_j : i = 1, \dots, n\} \tag{3.9}$$

es un conjunto de generadores de $\operatorname{Ker} \phi$.

Dado $x \in F_n$, tomemos su expresión única

$$x = \sum_{i=1}^{n} p_i(X) f_i, \qquad p_i(X) \in K[X].$$

Para cada $i = 1, \dots, n$, escribimos $p_i(X) = q_i(X)X + b_i$ para $q_i(X) \in K[X], b_i \in K$. Así,

$$x = \sum_{i=1}^{n} q_i(X) X f_i + \sum_{i=1}^{n} b_i f_i =$$
$$\sum_{i=1}^{n} \left\{ q_i(X) X f_i - q_i(X) \sum_{j=1}^{n} b_{ij} f_j + q_i(X) \sum_{j=1}^{n} b_{ij} f_j \right\} + \sum_{i=1}^{n} b_i f_i =$$
$$\sum_{i=1}^{n} q_i(X)(Xf_i - \sum_{j=1}^{n} b_{ij} f_j) + \sum_{j=1}^{n} (\sum_{i=1}^{n} b_{ij} q_i(X)) f_j + \sum_{i=1}^{n} b_i f_i.$$

Puesto que $\deg q_i(X) < \deg p_i(X)$ para cada i, podemos reiterar el proceso y obtener que

$$x = \sum_{i=1}^{n} r_i(X)(Xf_i - \sum_{j=1}^{n} b_{ij} f_j) + \sum_{i=1}^{n} a_i f_i,$$

para ciertos $r_i(X) \in K[X], a_i \in K$. Si $x \in \ker \phi$, deducimos que $\sum_{i=1}^{n} a_i v_i = 0$, lo que implica que $a_i = 0$ para $i = 1, \dots, n$. Así,

$$x = \sum_{i=1}^{n} r_i(X)(Xf_i - \sum_{j=1}^{n} b_{ij} f_j),$$

como queríamos.

Definimos ahora $\psi : F_n \to F_n$ por

$$\psi(f_i) = Xf_i - \sum_{j=1}^{n} b_{ij} f_j, \qquad (i = 1, \ldots, n).$$

Deducimos que

$$F_n \xrightarrow{\psi} F_n \xrightarrow{\phi} V \longrightarrow 0$$

es una presentación libre finita de ${}_{K[X]}V$. Observemos que

$$A_\psi = \begin{pmatrix} X - b_{11} & -b_{12} & \cdots & -b_{1n} \\ -b_{21} & X - b_{22} & \cdots & -b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -b_{n1} & -b_{n2} & \cdots & X - b_{nn} \end{pmatrix} \in K[X]^{n \times n},$$

la matriz característica de B. Usando la estructura de $K[X]$–módulo de $K[X]^{n\times n}$ como suma directa externa de copias del módulo regular $K[X]$, tenemos que

$$A_\psi = XI_n - B,$$

donde I_n denota la matriz identidad de tamaño $n \times n$.

Nuestro próximo objetivo es representar un homomorfismo entre módulos finitamente presentados sin necesidad de suponer que son libres. Necesitamos, para ello, establecer una propiedad fundamental de los módulos libres.

Lema 3.3.2. *Sea F un módulo libre, y $\varphi : M \to N$ un epimorfismo de módulos. Para cada homomorfismo $\alpha : F \to N$ existe un homomorfismo $\beta : F \to M$ tal que $\varphi\beta = \alpha$.*

Demostración. Tomemos una base $\{e_i : i \in I\}$ de F. Puesto que α es sobreyectivo, para cada $i \in I$, existe $m_i \in M$ tal que $\varphi(m_i) = \alpha(e_i)$. Por el Ejercicio 46, existe un homomorfismo de módulos $\beta : F \to M$ tal que $\beta(e_i) = m_i$ para todo $i \in I$. Observemos que, entonces

$$\varphi(\beta(e_i)) = \varphi(m_i) = \alpha(e_i),$$

para todo $i \in I$. Por tanto, $\varphi\beta = \alpha$. □

Consideremos un homomorfismo de R–módulos

$$M \xrightarrow{h} N$$

para módulos finitamente presentados M, N. Tomando presentaciones libres finitas de ambos, vamos a obtener un diagrama conmutativo de homomorfismos de módulos

$$\begin{array}{ccccccc} E_s & \xrightarrow{\psi} & F_t & \xrightarrow{\phi} & M & \longrightarrow & 0 \\ \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle q} & & \downarrow{\scriptstyle h} & & \\ E'_{s'} & \xrightarrow{\psi'} & F'_{t'} & \xrightarrow{\phi'} & N & \longrightarrow & 0\,. \end{array} \tag{3.10}$$

Describamos cómo se construyen p, q. Para la existencia de q tal que $\phi' q = h\phi$, aplicamos directamente el Lema 3.3.2.

Puesto que $\phi' q\psi = h\phi\psi = 0$, deducimos que $\operatorname{Im} q\psi \subseteq \ker \phi' = \operatorname{Im} \psi'$. Por tanto, podemos aplicar de nuevo el Lema 3.3.2 a la co-restricción de $q\psi$ a su imagen, y obtenemos la existencia de p tal que $\psi' p = q\psi$.

Recíprocamente, si nos dan homomorfismos p, q como en el diagrama (3.10) tales que $q\psi = \psi' p$, entonces definimos h como sigue: dado $m \in M$, tomo cualquier $u \in F_t$ tal que $\phi(u) = m$. Definimos entonces

$$h(m) = \phi'(q(u)).$$

Para comprobar que esta definición es consistente, supongamos $v \in F_t$ tal que $\phi(v) = \phi(u)$. Como $v - u \in \ker \phi$, existe $x \in E_s$ tal que $\psi(x) = v - u$. Por tanto,

$$\phi'(q(v) - q(u)) = \phi'(q(v-u))) = \phi'(q(\psi(x))) = \phi'(\psi'(p(x))) = 0,$$

con lo que $\phi'(q(v)) = \phi'(q(u))$.

Una vez comprobada la consistencia de la definición de h es rutinario verificar que se trata de un homomorfismo de módulos.

Hemos visto, pues, que definir un homomorfismo de módulos $h : M \to N$ es equivalente a dar una pareja de homomorfismos de módulos p, q como en el diagrama (3.10). Advirtamos, no obstante, la correspondencia descrita entre homomorfismos h y pares de homomorfismos p, q descrita no es biunívoca.

Tomando bases en los cuatro módulos libres involucrados, y representando así mediante matrices los homomorfismos, vemos que definir h es equivalente, con el matiz explicado, a dar matrices A_q, A_p tales que

$$A_\psi A_q = A_p A_{\psi'}.$$

Explícitamente, si las bases de F_t y $F'_{t'}$ son, respectivamente $f = \{f_1, \ldots, f_t\}$ y $f' = \{f'_1, \ldots, f'_{t'}\}$, y escribimos $m_i = \phi(f_i)$ para $i = 1, \ldots, t$, y $n_j = \phi'(f'_j)$ para $j = 1, \ldots, t'$ entonces, para $A_q = (q_{ij})$, tenemos que

$$h(m_i) = \sum_{j=1}^{t'} q_{ij} n_j.$$

Ejercicio 50. Con la notación anterior, demostrar que h es un epimorfismo si, y sólo si, $\operatorname{Im} q + \operatorname{Im} \psi' = F'_{t'}$.

Ejercicio 51. Con la notación anterior, demostrar que h es un monomorfismo si, y sólo si, $\operatorname{Im}\psi = \{x \in F_t : q(x) \in \operatorname{Im}\psi'\}$.

La primera aplicación que vamos a dar de este desarrollo abstracto es el siguiente teorema clásico del Álgebra Lineal.

Proposición 3.3.3 (Teorema de Cayley-Hamilton)**.** *Sea M un módulo finitamente generado sobre un anillo conmutativo K y $g : M \to M$ un homomorfismo de K–módulos. Dado un sistema de generadores $\{m_1, \ldots, m_n\}$ de M, tomamos $B = (b_{ij}) \in K^{n\times n}$ tal que $T(m_i) = \sum_{j=1}^{n} b_{ij} m_j$ para $j = 1, \ldots, t$. Si vemos M, g como un $K[X]$–módulo, entonces $\operatorname{Ann}_{K[X]}(M)$ contiene al polinomio característico $d(X)$ de B.*

Demostración. Tomemos V un K–módulo con base $\{v_1, \ldots, v_n\}$, y sea $\varphi : V \to M$ K–lineal dado por $\varphi(v_i) = m_i$ para $i = 1, \ldots, n$. Si definimos $T : V \to V$ por $T(v_i) = \sum_{j=1}^{n} b_{ij} e_j$, tenemos un diagrama conmutativo

$$\begin{array}{ccccc} V & \xrightarrow{\varphi} & M & \longrightarrow & 0 \\ \downarrow{\scriptstyle T} & & \downarrow{\scriptstyle g} & & \\ V & \xrightarrow{\varphi} & M & \longrightarrow & 0, \end{array}$$

que muestra que φ es un homomorfismo de $K[X]$–módulos de (V, T) a (M, g). Por tanto, $\operatorname{Ann}_{K[X]}(V) \subseteq \operatorname{Ann}_{K[X]}(M)$, por lo que basta con mostrar que $\operatorname{Ann}_{K[X]}(V)$ contiene al polinomio característico $d(X)$ de B.

Vemos V como $K[X]$–módulo y consideramos la presentación libre finita

$$F_n \xrightarrow{\psi} F_n \xrightarrow{\phi} V \longrightarrow 0$$

construida en el Ejemplo 49. Si P es la matriz adjunta de A_ψ, tenemos que $PA_\psi = d(X)I_n$. Recordemos que A_ψ es la matriz característica de B. Sea $\delta : F_n \to F_n$ el homomorfismo cuya matriz con respecto de la base $\{f_1, \ldots, f_n\}$ es $d(X)I_n$, es decir, $\delta(f_i) = d(X)f_i$ para $i = 1, \ldots, n$. Finalmente, sea $p : F_n \to F_n$ el homomorfismo de $K[X]$–módulos tal que $A_p = P$. Tenemos el diagrama conmutativo de homomorfismos de $K[X]$–módulos con filas exactas

$$\begin{array}{ccccccc} F_n & \xrightarrow{\delta} & F_n & \xrightarrow{\pi} & F_n/\operatorname{Im}(\delta) & \longrightarrow & 0\,, \\ \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle h} & & \\ F_n & \xrightarrow{\psi} & F_n & \xrightarrow{\phi} & V & \longrightarrow & 0 \end{array}$$

donde π es la proyección canónica y h es el homomorfismo determinado por el par de homomorfismos p, id. Puesto que ϕ es sobreyectivo, así lo es h. Esto implica que

$$d(X) \in \operatorname{Ann}_{K[X]}(F_n/\operatorname{Im}(\delta)) \subseteq \operatorname{Ann}_{K[X]}(V) \subseteq \operatorname{Ann}_{K[X]}(M).$$

□

Seguidamente, vamos a usar la representación del homomorfismo identidad de un módulo dado como herramienta para obtener información sobre la estructura del mismo.

Definición 31. Una matriz $A = (a_{ij}) \in R^{s\times t}$ se dice *cuasi-diagonal* si $a_{ij} = 0$ para todo $i \neq j$. Si denotamos por m el mínimo de s, t y escribimos $d_i = a_{ii}$ para $i = 1, \ldots, m$, entonces usamos la notación $A = diag_{s\times t}(d_1, \ldots, d_m)$.

Por $GL_n(R)$ denotamos el conjunto de las matrices $Q \in R^{n\times n}$ que son invertibles, esto es, para las que existe $Q^{-1} \in R^{n\times n}$ tal que $I_n = QQ^{-1} = Q^{-1}Q$. Este conjunto es un grupo, llamado *grupo lineal general de orden* n de R.

Proposición 3.3.4. *Supongamos dada una presentación finita*

$$E_s \xrightarrow{\psi} F_t \xrightarrow{\phi} M \longrightarrow 0$$

de un módulo ${}_RM$. *Supongamos que existen matrices* $P \in GL_s(R), Q \in GL_t(R)$, *y una matriz cuasi-diagonal* $D = diag_{s\times t}(d_1, \ldots, d_m) \in R^{s\times t}$ *tales que* $PA_\psi = DQ$. *Si* $\{m_1, \ldots, m_t\}$ *es el conjunto de generadores de* ${}_RM$ *dado por* $m_i = \phi(f_i)$ *para* $i = 1, \ldots, t$ *y escribimos*

$$x_i = \sum_{j=1}^{t} q_{ij}m_j, \qquad (i = 1, \ldots, t),$$

para $Q = (q_{ij})$, *entonces*

$$M = \dot{+}_{i=1}^{t} Rx_i,$$

con $\operatorname{ann}_R(x_i) = Rd_i$ *para* $i = 1, \ldots, m$, $\operatorname{ann}_R(x_i) = \{0\}$ *para* $i > m$, *si se da el caso.*

Demostración. Vamos a construir una segunda presentación libre finita de M

$$E_s \xrightarrow{\psi_1} F_t \xrightarrow{\phi_1} M \longrightarrow 0\,,$$

como sigue. Tomando isomorfismos p, q tales que $A_q = Q, A_p = P$, y un homomorfismo ψ_1 tal que $A_{\psi_1} = D$, tenemos el diagrama conmutativo

$$\begin{array}{ccccccc} E_s & \xrightarrow{\psi_1} & F_t & \xrightarrow{\phi_1} & M & \longrightarrow & 0\,. \\ \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle q} & & \downarrow{\scriptstyle id} & & \\ E_s & \xrightarrow{\psi} & F_t & \xrightarrow{\phi} & M & \longrightarrow & 0 \end{array}$$

Observemos que estamos definiendo $\phi_1 = \phi q$. Como q es un isomorfismo, obtenemos inmediatamente que ϕ_1 es sobreyectiva. Es también fácil deducir la exactitud en F_t de la primera fila de la de la segunda.

Tenemos, también, que $\phi_1(f_i) = \phi q(f_i) = x_i$, para $i = 1, \ldots, t$, lo que prueba que $\{x_1, \ldots, x_t\}$ es un conjunto de generadores de M.

Si $\sum_{i=1}^{t} r_i x_i = 0$, entonces $\sum_{i=1}^{t} r_i f_i \in \operatorname{Ker}\phi_1 = \operatorname{Im}\psi_1$. Observemos que

$$\operatorname{Im}\psi_1 = Rd_1f_1 \dotplus \cdots \dotplus Rd_mf_m.$$

Esto implica que $r_i \in Rd_i$ para $i = 1, \ldots, m$ y $r_i = 0$ para $i > m$. Por tanto, existen $a_1, \ldots, a_m \in R$ tales que $r_i = a_i d_i$ para $i = 1, \ldots, m$. En el siguiente cálculo, pondremos $d_i = 0$ para $i > m$, si se da el caso.

$$d_i x_i = d_i(\sum_{j=1}^{t} q_{ij} m_j) = d_i(\sum_{j=1}^{t} q_{ij}\phi(f_j)) = \phi(\sum_{j=1}^{t} d_i q_{ij} f_j) = \phi(q\psi_1(f_i)) = \phi(\psi p(f_i)) = 0.$$

Deducimos que

$$M = \dotplus_{i=1}^{t} Rx_i,$$

El anterior cálculo también demuestra que $\operatorname{ann}_R(x_i) = Rd_i$ para $i = 1, \ldots, m$, y $\operatorname{ann}_R(x_i) = \{0\}$ si $m < i \leq t$. □

Para un anillo general R, no tengo garantías de que existan P, Q y D como en el enunciado de la Proposición 3.3.4. No obstante, las herramientas básicas para intentar obtenerlas son las operaciones elementales sobre las filas y las columnas de la matriz A_ψ, que son el resultado de multiplicar a izquierda o a derecha por ciertas matrices invertibles llamadas elementales. Para describir esta relación, denotemos, sin especificar el tamaño, por E_{ij} a la matriz cuadrada cuyas componentes son todas 0 salvo la (i,j)–ésima, que vale 1. Tenemos que

$$E_{ij}E_{kl} = \begin{cases} E_{il} & \text{si } j = k \\ 0 & \text{si } j \neq k \end{cases}.$$

Para cada $r \in R$, la matriz $rE_{ij} = E_{ij}r$ tiene todas sus entradas nulas, salvo la (i,j)–ésima, que vale r.

La matriz $(I + rE_{ij})A$ es la matriz obtenida de A al sumarle a su fila i–ésima la fila j–ésima multiplicada por la izquierda por r. Análogamente, $A(I + rE_{ij})$ se obtiene de A sumándole a su columna j–ésima la columna i–ésima multiplicada por r por la derecha.

Para cada $r \in R$, e $i, j \in \{1, \ldots, n\}$ distintos, la matriz $I_n + rE_{ij} \in GL_n(R)$, siendo su inversa $I_n - rE_{ij}$.

Intercambiar las filas i–ésima y j–ésima de A es calcular

$$(I + E_{ij} + E_{ji} - E_{ii} - E_{jj})A.$$

Se tiene que $I + E_{ij} + E_{ji} - E_{ii} - E_{jj} \in GL_n(R)$. De hecho, su cuadrado es I. La misma matriz proporciona, multiplicando por la derecha, el intercambio de las columnas i–ésima y j–ésima.

Otra operación elemental sobre filas es multiplicar la fila i–ésima de A a la izquierda por una unidad $u \in U(R)$. El mismo efecto se obtiene realizando el producto matricial $(I + (u-1)E_{ii})A$. Observemos que

$$(I + (u-1)E_{ii})(I + (u^{-1}-1)E_{ii}) = I,$$

con lo que $(I + (u-1)E_{ii}) \in GL_n(R)$.

Análogamente, el producto de una columna por una unidad de R a la derecha se obtiene multiplicando por una tal matriz invertible.

Ejemplo. Supongamos que M es el grupo aditivo con generadores $\{m_1, m_2, m_3\}$ sujetos a las relaciones

$$\begin{aligned} 2m_1 + m_2 - m_3 &= 0 \\ 4m_1 + m_2 + 3m_3 &= 0. \end{aligned}$$

Esto significa, precisamente, que M admite una presentación como $\mathbb{Z}$–módulo de la forma

$$E_2 \xrightarrow{\psi} F_3 \xrightarrow{\phi} M \longrightarrow 0,$$

donde $m_i = \phi(f_i)$ para $\{f_1, f_2, f_3\}$ una base del $\mathbb{Z}$–módulo libre F_3, y

$$A_\psi = \begin{pmatrix} 2 & 1 & -1 \\ 4 & 1 & 3 \end{pmatrix}$$

la matriz de ψ con respecto de la base citada de F_3 y una base $\{e_1, e_2\}$ de E_2. Vamos a aplicar una sucesión de operaciones elementales sobre las filas y las columnas de A_ψ con objeto de buscar una presentación cuasi-diagonal.

$$\begin{pmatrix} 2 & 1 & -1 \\ 4 & 1 & 3 \end{pmatrix} \sim \begin{pmatrix} 2 & 1 & -1 \\ 0 & -1 & 5 \end{pmatrix} \sim \begin{pmatrix} 2 & 0 & 4 \\ 0 & -1 & 5 \end{pmatrix} \sim_{c_3 - 2c_2}$$
$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & -1 & 5 \end{pmatrix} \sim_{c_3 + 5c_2} \begin{pmatrix} 2 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix},$$

donde las operaciones sobre columnas son las dos últimas.

Obtenemos, pues, que existen matrices $P \in GL_2(\mathbb{Z}), Q^{-1} \in GL_3(\mathbb{Z})$ tales que

$$PA_\psi Q^{-1} = \begin{pmatrix} 2 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}.$$

Como hemos indicado las operaciones elementales sobre columnas usadas, sabemos que, aplicando las inversas en orden contrario a la identidad,

$$Q = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & -5 \\ 0 & 0 & 1 \end{pmatrix}.$$

Obtenemos, pues, unos nuevos generadores $\{x_1, x_2, x_3\}$ de M tales que $\mathrm{ann}_{\mathbb{Z}}(x_1) = 2\mathbb{Z}, \mathrm{ann}_{\mathbb{Z}}(x_2) = \mathbb{Z}, \mathrm{ann}_{\mathbb{Z}}(x_3) = \{0\}$. Desde luego, deducimos que $x_2 = 0$ y

$$\begin{array}{rcl} x_1 & = & m_1 + 2m_3 \\ x_3 & = & m_3 \end{array},$$

son tales que $M = \mathbb{Z}x_1 \dot{+} \mathbb{Z}x_3$ con $\mathbb{Z}x_1 \cong \mathbb{Z}_2, \mathbb{Z}x_3 \cong \mathbb{Z}$. Podemos escribir, pues, que $M \cong \mathbb{Z}_2 \oplus \mathbb{Z}$.

Ejemplo. Consideremos una aplicación lineal $T : V \to V$ para V un K–espacio vectorial de dimensión 3 con base $\{v_1, v_2, v_3\}$. Supongamos que la matriz de T con respecto de dicha base es

$$B = \begin{pmatrix} 1 & -1 & 1 \\ -1 & -1 & 1 \\ -1 & 1 & 1 \end{pmatrix}$$

La matriz característica de B es

$$A = \begin{pmatrix} X-1 & 1 & -1 \\ 1 & X+1 & -1 \\ 1 & -1 & X-1 \end{pmatrix}$$

Vamos a obtener una descomposción de V como suma directa de subespacios cíclicos. Para ello, diagonalizamos la matriz A. Lo haremos primero si la característica de K no es 2.

$$\begin{pmatrix} X-1 & 1 & -1 \\ 1 & X+1 & -1 \\ 1 & -1 & X-1 \end{pmatrix} \sim \begin{pmatrix} 1 & -1 & X-1 \\ 1 & X+1 & -1 \\ X-1 & 1 & -1 \end{pmatrix}$$

$$\sim \begin{pmatrix} 1 & -1 & X-1 \\ 0 & X+2 & -X \\ 0 & X & -X^2+2X-2 \end{pmatrix}$$

$$\sim \begin{pmatrix} 1 & -1 & X-1 \\ 0 & 2 & X^2-3X+2 \\ 0 & X & -X^2+2X-2 \end{pmatrix} \sim \begin{pmatrix} 1 & -1 & X-1 \\ 0 & 2 & X^2-3X+2 \\ 0 & 0 & -\frac{1}{2}X^3+\frac{1}{2}X^2+X-2 \end{pmatrix}$$

$$\sim \begin{pmatrix} 1 & -1 & X-1 \\ 0 & 2 & X^2-3X+2 \\ 0 & 0 & X^3-X^2-2X+4 \end{pmatrix} \sim_{c_2+c_1} \begin{pmatrix} 1 & 0 & X-1 \\ 0 & 2 & X^2-3X+2 \\ 0 & 0 & X^3-X^2-2X+4 \end{pmatrix}$$

$$\sim_{c_3-(X-1)c_1} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & X^2-3X+2 \\ 0 & 0 & X^3-X^2-2X+4 \end{pmatrix}$$

$$\sim_{c_3-\frac{1}{2}(X^2-3X+2)c_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & X^3-X^2-2X+4 \end{pmatrix}$$

La matriz Q que permite calcular los nuevos generadores de V es

$$Q = \begin{pmatrix} 1 & 1 & X-1 \\ 0 & 1 & \frac{1}{2}(X^2-3X+2) \\ 0 & 0 & 1 \end{pmatrix}.$$

De hecho, en vista de los elementos diagonales de la matriz

$$D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & X^3-X^2-2X+4 \end{pmatrix}$$

sólo nos interesa la última fila de Q. Tenemos que $x_1 = 0, x_2 = 0, x_3 = v_3$, es decir, $V = K[X]v_3$, y el polinomio mínimo de T es

$$\mu(X) = X^3 - X^2 - 2X + 4,$$

ya que

$$\mathrm{ann}_{K[X]}(v_3) = \langle X^3 - X^2 - 2X + 4 \rangle.$$

Deducimos que $\{v_3, T(v_3), T^2(v_3)\}$ es una K–base de V con respecto de la cual la matriz de T es

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -4 & 2 & 1 \end{pmatrix}$$

En cuanto a la descomposición cíclica primaria de V como K[X]–módulo respecta, esto depende de quién sea K. En efecto, si $K = \mathbb{Q}$, resulta que $\mu(X)$ no tiene raíces racionales por lo que, al ser cúbico, resulta irreducible en $\mathbb{Q}[X]$ y ${}_{\mathbb{Q}[X]}V$ no puede descomponerse más.

Puesto que $\mu'(X) = 3X^2-2X-2$ tiene como raíces $(1\pm\sqrt{7})/3$ y $\mu((1+\sqrt{7}))/3) > 0$, deducimos que la cúbica $\mu(X)$ tiene una única raíz real α, así que tenemos la descomposición

$$\mu(X) = (X-\alpha)(X-z)(X-\overline{z}),$$

para cierto número complejo no real z. La descomposición primaria de $V = \mathbb{R}[X]v_3$ viene a ser, pues,

$$V = \mathbb{R}[X]u_1 \dotplus \mathbb{R}[X]u_2,$$

para

$$u_1 = (T^2 - 2\mathrm{Re}(z)T + |z|^2)v_3, u_2 = (T-\alpha)v_3,$$

vectores que satisfacen

$$\mathrm{ann}_{\mathbb{R}[X]}(u_1) = \langle X-\alpha \rangle, \mathrm{ann}_{\mathbb{R}[X]}(u_2) = \langle X^2 - 2\mathrm{Re}(z)X + |z|^2 \rangle.$$

En la base

$$\{u_1, u_2, T(u_2)\},$$

la matriz del endomorfismo T adopta la forma

$$\begin{pmatrix} \alpha & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -|z|^2 & 2Re(z) \end{pmatrix}.$$

Los valores de α y z han de ser aproximados numéricamente.

La descomposición primaria de ${}_{\mathbb{C}[X]}V$ viene dada por

$$V = \mathbb{C}[x]u_1 \dot{+} \mathbb{C}[x]y_2 \dot{+} \mathbb{C}[x]y_3,$$

donde

$$y_2 = (T - z)u_2, y_3 = (T - \overline{z})u_2,$$

con lo que

$$\mathrm{ann}_{\mathbb{K}[X]}(y_2) = \langle X - \overline{z} \rangle, \mathrm{ann}_{\mathbb{C}[X]}(y_3) = \langle X - z \rangle.$$

Con respecto de la $\mathbb{C}$–base

$$\{u_1, y_2, y_3\},$$

la matriz de T resulta

$$\begin{pmatrix} \alpha & 0 & 0 \\ 0 & \overline{z} & 0 \\ 0 & 0 & z \end{pmatrix}.$$

Discutamos seguidamente el caso en que la característica de K es 2. La matriz característica de B es, en este caso,

$$A = \begin{pmatrix} X+1 & 1 & 1 \\ 1 & X+1 & 1 \\ 1 & 1 & X+1 \end{pmatrix}.$$

Una sucesión de operaciones elementales sobre filas y columnas para diagonalizar A puede ser

$$\begin{pmatrix} X+1 & 1 & 1 \\ 1 & X+1 & 1 \\ 1 & 1 & X+1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & X+1 \\ 1 & X+1 & 1 \\ X+1 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & X+1 \\ 0 & X & X \\ 0 & X & X^2 \end{pmatrix}$$

$$\sim \begin{pmatrix} 1 & 1 & X+1 \\ 0 & X & X \\ 0 & 0 & X^2+X \end{pmatrix} \sim_{c_2+c_1} \begin{pmatrix} 1 & 0 & X+1 \\ 0 & X & X \\ 0 & 0 & X^2+X \end{pmatrix} \sim_{c_3+(X+1)c_1} \begin{pmatrix} 1 & 0 & 0 \\ 0 & X & X \\ 0 & 0 & X^2+X \end{pmatrix}$$

$$\sim_{c_3+c_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & X & 0 \\ 0 & 0 & X^2+X \end{pmatrix}$$

La matriz de paso es ahora

$$Q = \begin{pmatrix} 1 & 1 & X+1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

De modo que $x_1 = 0, x_2 = v_2 + v_3, x_3 = v_3$ y

$$V = K[X]x_2 \dotplus K[X]v_3,$$

con $\mathrm{ann}_{K[X]}(x_2) = \langle X \rangle, \mathrm{ann}_{K[X]}(v_3) = \langle X^2 + X \rangle$.

La descomposición cíclica primaria se obtiene como

$$V = K[X]x_2 \dotplus K[X]y_1 \dotplus K[X]y_2,$$

con $y_1 = (T+1)v_3, y_2 = Tv_3$. Así, en la base

$$\{x_2, y_1, y_2\},$$

la matriz del endomorfismo T es

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

El procedimiento usado en el Ejemplo 3.3 puede sistematizarse para que funcione sobre cualquier dominio euclídeo (DE) R con función euclídea $\nu : R \setminus \{0\} \to \mathbb{N}$.

Proposición 3.3.5. *Dada cualquier matriz $A \in R^{s\times t}$ sobre un dominio euclídeo R, existe una matriz cuasi-diagonal $D \in R^{s\times t}$ y matrices $P \in \mathrm{GL}_s(R), Q \in \mathrm{GL}_t(R)$ tales que $PA = DQ$.*

Demostración. Supongamos que $A \neq 0$. Usaremos operaciones elementales sobre sus filas y columnas con objeto de demostrar que PAQ^{-1} es cuasi-diagonal para P, Q^{-1} invertibles obtenidas como producto de matrices elementales. Hacemos inducción sobre $\nu(A)$, el mínimo entre los valores de la función euclídea evaluada en las entradas no nulas de A para demostrar que se puede reducir a una matriz por bloques de la forma

$$\begin{pmatrix} d_1 & 0 \\ 0 & A_1 \end{pmatrix}, \tag{3.11}$$

para $A_1 \in R^{(s-1)\times(t-1)}$. Es resultado se deduce fácilmente reiterando el argumento sobre A_1.

Escogemos una entrada no nula a_{kl} de A con $\nu(a_{kl})$ mínima. Un intercambio entre las filas 1 y k, y un intercambio entre las columnas 1 y l colocan dicha

entrada en la posición $(1,1)$. Podemos, pues, suponer que a_{11} es no nulo y de función euclídea $\nu(a_{11})$ mínima entre los valores de la misma en las entradas no nulas de A.

Si a_{11} es un divisor de todas las entradas de la primera fila y la primera columna de A, entonces es claro que se puede reducir A a una matriz de la forma (3.11).

Si a_{i1} no es un múltiplo de a_{11}, para algún i, entonces, puesto que disponemos de la división euclídea, podemos escribir $a_{i1} = qa_{11} + r$ para ciertos $q, r \in R$ con $\nu(r) < \nu(a_{11})$. Sumando a la fila i–ésima la primera multiplicada por $-q$ nos ponemos en disposición de aplicar inducción, ya que, para la matriz A' que obtenemos, $\nu(A') \leq \nu(r)$. Un argumento análogo se usa si a_{1i} no es un múltiplo de a_{11} para algún i.

□

Ejercicio 52. Cada una de las siguientes matrices tiene coeficientes en un cuerpo K y dotan, por tanto, a un K–espacio vectorial V de dimensión 4, una vez fijada una base $\{v_1, v_2, v_3, v_4\}$ de estructura de $K[X]$–módulo. Calcular la descomposición cíclica primaria de dicho módulo, como suma directa interna, en los siguientes casos: $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_2, \mathbb{Z}_3$.

$$\begin{pmatrix} -3 & 2 & -2 & 2 \\ 0 & 0 & 1 & 0 \\ 1 & -1 & 1 & 0 \\ -1 & 1 & -1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} -2 & 1 & -1 & 2 \\ 0 & 0 & 1 & 0 \\ 1 & -1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 3 & 0 & 1 & -2 \\ 0 & 0 & 1 & 0 \\ 1 & -1 & 1 & 0 \\ 5 & -1 & 2 & -3 \end{pmatrix}$$

Ejercicio 53. Sean E, F módulos libres sobre $\mathbb{Z}_8$ con bases respectivas $\{e_1, e_2\}, \{f_1, f_2, f_3\}$ y $\psi : E \to F$ el homomorfismo de $\mathbb{Z}_8$–módulos cuya matriz con respecto de dichas bases es

$$A_\psi = \begin{pmatrix} 7 & 1 & 2 \\ 2 & 4 & 1 \end{pmatrix}.$$

Calcular una serie de composición del $\mathbb{Z}_8$–módulo $F/\mathrm{Im}\,(\psi)$.

Capítulo 4

Módulos y anillos semisimples

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

Proposición 4.0.1. *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,* $N \cap (\dot{+}_{i\in J} M_i) = \{0\}$*, y* $M' = N \dot{+} (\dot{+}_{i\in J} M_i)$*.*

Demostración. Sea Γ el conjunto de los subconjuntos J de I tales que la familia $\{M_j \mid j \in J\}$ es independiente y $(\dot{+}_{j\in J} M_j) \cap N = \{0\}$. Razonemos primero que Γ es no vacío. 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.

Queremos aplicar el Lema de Zorn a Γ, ordenado por inclusión, así que tomemos una cadena χ en Γ, y sea $J = \bigcup_{C\in\chi} C$. Para demostrar que el conjunto $\{M_i \mid i \in J\}$ es independiente podemos, en virtud de la Proposición 3.1.3, considerar cualquier subconjunto finito $F \subseteq J$. 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 $m \in N \cap (\dot{+}_{i\in J} M_i)$, entonces $m \in N \cap (\dot{+}_{i\in C} M_i)$ para algún $C \in \chi$, luego $m = 0$. Así que $J \in \Gamma$ es una cota superior para χ.

Por el Lema de Zorn, existe un elemento maximal J en Γ. Para todo índice $i \notin J$ ocurre que $M_i \cap (N + \dot{+}_{j\in J} M_j) \neq \{0\}$. Como M_i es simple, esto implica que $M_i \subseteq N + \dot{+}_{j\in J} M_j$, lo que concluye la prueba. □

Los módulos sobre un anillo de división D se suelen llamar D*–espacios vectoriales*

Corolario 4.0.2. *Sea* ${}_DV$ *un espacio vectorial sobre un anillo de división* D*. Para todo sistema de generadores no nulos* $\{v_i \mid i \in I\}$ *de* V *existe un subconjunto* $J \subseteq I$

tal que $V = \dot{+}_{j\in J} Dv_j$. *Como consecuencia, todo espacio vectorial sobre* D *tiene una base.*

Demostración. Observemos que $V = \sum_{i\in I} Dv_i$. Ahora bien, por ser D un anillo de división, ${}_DD \cong Dv_i$ para todo $i \in I$. Como ${}_DD$ es simple, se sigue que Dv_i es simple para todo $i \in I$. Ahora aplicamos la Proposición 4.0.1 para obtener J. Así, deducimos que todo espacio vectorial tiene una base, ya que tiene un sistema de generadores, por ejemplo, $\{v \mid 0 \neq v \in V\}$. □

Hay algunas observaciones aquí pertinentes en relación con la nomenclatura. En la demostración del corolario, hemos visto que $Dv_i \cong {}_DD$ para todo $i \in I$, con lo que Dv_i resulta ser libre de rango 1. Por tanto, hemos demostrado asímismo 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 de todos los D–espacios vectoriales por la izquierda.

4.1. Módulos semisimples de cualquier longitud

Dados homomorfismos

$$N \xrightarrow{g} M \xrightarrow{f} N$$

tales que $fg = id_N$, diremos que g es un *monomorfismo escindido* y que f un *epimorfismo escindido*. De hecho, es fácil ver que g es realmente un monomorfismo y que f es un epimorfismo.

Lema 4.1.1. *Todo módulo no nulo y finitamente generado tiene un submódulo maximal.*

Demostración. Sea $M = Rm_1 + \cdots + Rm_n$ un R–módulo generado por $m_1, \ldots, m_n$. Sea Γ el conjunto de los submódulos estrictamente contenidos en M. Dada una cadena $\mathcal{C}$ de Γ, ponemos $M' = \bigcup_{L\in\mathcal{C}} L$. Es rutinario comprobar que M' es un submódulo de M. Si $M' = M$, entonces $m_1, \ldots, m_n \in M'$. Ha de existir, pues, $L \in \mathcal{C}$ tal que $m_1, \ldots, m_n \in L$, lo que implica que $L = M$, en contradicción con el hecho de que $L \in \Gamma$. Por tanto, $M' \subsetneq M$. Aplicando el Lema de Zorn, concluimos que Γ tiene al menos un elemento maximal, que es, por definición, un submódulo maximal de M. □

Teorema 4.1.2. *Las siguientes condiciones son equivalentes para un módulo* M.

1. *Todo submódulo de* M *es un sumando directo;*
2. *todo monomorfismo* $L \to M$ *es escindido;*
3. *todo epimorfismo* $M \to N$ *es escindido;*
4. $\mathrm{Soc}(M) = M$*;*

5. *M es suma de una familia de submódulos simples;*

6. *M es suma directa interna de una familia de submódulos simples.*

Demostración. (1) $\Rightarrow$ (3). Sea $\phi : M \to N$ el epimorfismo y pongamos $L = \operatorname{Ker}\phi$. Entonces $M = L \dotplus X$ para cierto submódulo X de M. Pero se tienen los isomorfismos canónicos

$$N \cong \frac{M}{L} = \frac{L \dotplus X}{L} \cong X$$

De hecho, el isomorfismo $X \to N$ viene dado, precisamente, por la restricción de ϕ a X. El inverso, pues, escinde a ϕ.
(3) $\Rightarrow$ (2). Sea $\phi : L \to M$ un monomorfismo. Consideremos la sucesión exacta corta

$$0 \longrightarrow L \xrightarrow{\varphi} M \xrightarrow{\kappa} C \longrightarrow 0$$

donde $C = M/\operatorname{Im}\varphi$, y κ es la proyección canónica. Como este último morfismo escinde, existe $g : C \to M$ tal que $\kappa g = \mathrm{id}_C$. Consideremos el morfismo $h = \mathrm{id}_M - g\kappa$. Es fácil comprobar que $\kappa h = 0$, de donde h factoriza a través del núcleo de κ, que es L. Es decir, existe un morfismo $f : M \to L$ tal que $\varphi f = h$. De manera que

$$\varphi(f\varphi) = h\varphi = \varphi - g\kappa\varphi = \varphi$$

Como φ es inyectiva, deducimos que $f\varphi = 1_L$, luego φ escinde.
(2) $\Rightarrow$ (1). Dado un submódulo X de M, existe una escisión de la inclusión, esto es, un homomorfismo $p : M \to X$ que, restringido a X, es la identidad. Se deduce sin dificultad que $M = X \dotplus \operatorname{Ker} p$.
(4) $\Rightarrow$ (5). Por definición, $\operatorname{Soc}(M)$ es el menor submódulo de M que contiene a todos sus submódulos simples, equivalentemente, la suma de todos los submódulos simples de M.
(5) $\Rightarrow$ (6). Esto es consecuencia directa de la Proposición 4.0.1, tomando $N = \{0\}$.
(6) $\Rightarrow$ (1). Consecuencia de la Proposición 4.0.1.
(1) $\Rightarrow$ (4). Por hipótesis, $M = \operatorname{Soc}(M) \dotplus X$ para cierto submódulo X de M. Basta con demostrar que $X = \{0\}$. Supongamos que existe $0 \neq m \in X$. Por el Lema 4.1.1, existe un epimorfismo $p : Rm \to S$, para un módulo simple S. Por otra parte, como Rm es un sumando directo de M, tenemos un epimorfismo $\pi : M \to Rm$. Componiendo ambos, obtenemos el epimorfismo $p\pi : M \to S$. Ahora bien, hemos demostrado antes que (1) es equivalente a (3), por lo que existe un homomorfismo $\iota : S \to M$ tal que $p\pi\iota = \mathrm{id}_S$. Por tanto, $S \cong \operatorname{Im}(\pi\iota) \subseteq Rm$, lo que prueba que X contiene un módulo simple. Esto es una contradicción. □

Extendemos seguidamente la noción de módulo semisimple a módulos cuya longitud no es necesariamente finita.

Definición 32. Un módulo M se dice *semisimple* si $\operatorname{Soc}(M) = M$.

Corolario 4.1.3. *Todo cociente y todo submódulo de un módulo semisimple es semisimple.*

Demostración. Si N es una imagen epimórfica de un módulo semisimple M entonces, al ser éste suma de simples, así lo es N. Por otro lado, cada sumódulo de M es un sumando directo, luego isomorfo a un cociente de M. □

Corolario 4.1.4. *Un módulo semisimple es finitamente generado si, y sólo si, es de longitud finita.*

Demostración. Sea M semisimple, entonces, por el Teorema 4.1.2, $M = \dot{+}_{i\in I} S_i$ para un conjunto $\{S_i : i \in I\}$ de submódulos simples. Si M es finitamente generado, entonces $M = Rm_1 + \cdots + Rm_n$, para ciertos $m_1, \ldots, m_n \in M$. Existe un subconjunto finito $J \subseteq I$ tal que $m_1, \ldots, m_n \in \dot{+}_{j\in J} S_j$. Por tanto, $M = \dot{+}_{j\in J} S_j$, de donde M es de longitud finita. □

Definición 33. Un anillo R se dice *semisimple* si todo R–módulo es semisimple.

Ejemplo. Todo anillo de división es semisimple.

Teorema 4.1.5. *Un anillo R es semisimple si, y sólo si, el módulo regular ${}_RR$ es semisimple.*

Demostración. Supongamos que ${}_RR$ es semisimple y consideremos un R–módulo M. Para cada $m \in M$ tenemos un epimorfismo $R \to Rm$. Por el Corolario 4.1.3, Rm es semisimple, así que es suma de módulos simples. Como $M = \sum_{m\in M} Rm$, deducimos que M es suma de módulos simples, luego es semisimple. □

Observación 6. Si el anillo R es semisimple, entonces el módulo regular ${}_RR$ es de longitud finita, en virtud del Corolario 4.1.4.

4.2. Anillos de endomorfismos y Teorema de Densidad

Para investigar la estructura de los anillos semisimples es muy útil considerar anillos de endomorfismos de módulos, de acuerdo con la siguiente definición.

Definición 34. Sea M un módulo sobre cualquier anillo R. El conjunto

$$\mathrm{End}_R(M) = \{f : M \to M \mid f \text{ homomorfismo de } R-\text{módulos }\}$$

es un subanillo de $\mathrm{End}(M)$ llamado *anillo de endomorfismos del R–módulo M.*

Escribamos $S = \mathrm{End}_R(M)$. Como S es un subanillo de $\mathrm{End}(M)$, tenemos que M es un S–módulo y podemos considerar el anillo $\mathrm{End}_S(M)$. Dado $g \in \mathrm{End}(M)$, observemos que $g \in \mathrm{End}_S(M)$ si, y sólo si, para todo $m \in M, f \in \mathrm{End}_R(M)$ se tiene que $g(fm) = f(gm)$. Esto es,

$$\mathrm{End}_S(M) = \{g \in \mathrm{End}(M) \mid gf = fg \text{ para todo } f \in \mathrm{End}_R(M)\}.$$

Lema 4.2.1. *La aplicación $\lambda : R \to \mathrm{End}_S(M)$ definida para cada $r \in R$ por $\lambda(r)(m) = rm$ para $m \in M$ es un homomorfismo de anillos.*

Demostración. De hecho, la definición original de módulo fue dada como un homomorfismo de anillos $\lambda : R \to \mathrm{End}(M)$. Sólo tenemos que comprobar, pues, que $\mathrm{Im}\,(\lambda) \subseteq \mathrm{End}_S(M)$. Dados $r \in R, f \in S, m \in M$, tenemos

$$\lambda(r)(f(m)) = rf(m) = f(rm) = f(\lambda(r)(m)).$$

Por tanto, $\lambda(r) \in \mathrm{End}_S(M)$. □

Por R–*sumando directo* de ${}_RM$ entenderemos un R–submódulo X de M tal que $M = X \dotplus Y$ para otro R–submódulo Y de M.

Proposición 4.2.2. *Sea ${}_RM$ un módulo, $S = \mathrm{End}_R(M)$ y $T = \mathrm{End}_S(M)$. Consideremos el módulo ${}_TM$ dado por el subanillo T de $\mathrm{End}(M)$. Los R–sumandos directos de M son los mismos que los T–sumandos directos de M. Como consecuencia, si ${}_RM$ es semisimple, entonces ${}_TM$ es semisimple.*

Demostración. Tenemos el homomorfismo de anillos $\lambda : R \to T$. Así, si ${}_TM = X \dotplus Y$ entonces, por restricción de escalares, ${}_RM = X \dotplus Y$.

Recíprocamente, supongamos que ${}_RM = X \dotplus Y$. Vamos a demostrar que X e Y son T–submódulos de M. Consideremos la aplicación $p : M \to M$ definida por $p(m) = x$ para $m = x + y$ la única descomposición con $x \in X, y \in Y$ de $m \in M$. Tenemos que $p \in S$ e $\mathrm{Im}\,(p) = X$. Ahora, si $g \in T$, entonces $gp = pg$, con lo que, para $x \in X$, $g(x) = gp(x) = pg(x) \in X$. Por tanto, X es un T–submódulo de M. Análogamente para Y.

La segunda afirmación es ahora consecuencia del Teorema 4.1.2. □

Corolario 4.2.3. *Si ${}_RM$ es semisimple de longitud finita, entonces ${}_TM$ es semisimple de longitud finita. En tal caso $\ell({}_RM) = \ell({}_TM)$.*

Demostración. Consecuencia de la Proposición 4.2.2 y de que los módulos semisimples de longitud finita son, precisamente, los que se descomponen como suma directa finita de submódulos simples. □

Dado un módulo ${}_RM$, consideremos una suma directa externa finita M^n de copias de M. Pongamos $S = \mathrm{End}_R(M)$ y $S' = \mathrm{End}_R(M^n)$. Para cada $i = 1, \ldots, n$, sea $\iota_i : M \to M^n$ la aplicación que lleva $m \in M$ a la n–tupla todas cuyas componentes son 0 salvo la i–ésima, que vale m. Por $\pi_i : M \to M_i$ denotamos la

aplicación que lleva cada n–tupla en su componente i–ésima. Tanto ι_i como π_i son homomorfismos de R–módulos. Se tiene que

$$\mathrm{id}_{M^n} = \sum_{i=1}^{n} \iota_i \pi_i$$

Si ahora nos dan $f \in \mathrm{End}_S(M)$, definimos $\overline{f} = \sum_{i=1}^{n} \iota_i f \pi_i \in \mathrm{End}(M^n)$, esto es

$$\overline{f}(m_1, \ldots, m_n) = (f(m_1), \ldots, f(m_n)), \qquad (m_1, \ldots, m_n) \in M^n. \tag{4.1}$$

Afirmamos que $\overline{f} \in \mathrm{End}_{S'}(M^n)$. En efecto, si $g \in S'$, entonces

$$g\overline{f} = \sum_{i,j=1}^{n} \iota_i \pi_i g \iota_j f \pi_j = \sum_{i,j=1}^{n} \iota_i f \pi_i g \iota_j \pi_j = \overline{f} g,$$

donde la segunda igualdad se da porque $\pi_i g \iota_j \in S$ y $f \in \mathrm{End}_S(M)$.

Teorema 4.2.4. *(Densidad) Sea* ${}_RM$ *un módulo semisimple, y* $m_1, \ldots, m_n \in M$. *Pongamos* $S = \mathrm{End}_R(M)$. *Para cada* $f \in \mathrm{End}_S(M)$, *existe* $r \in R$ *tal que* $f(m_i) = rm_i$ *para todo* $i = 1, \ldots, n$.

Demostración. Tomemos $m = (m_1, \ldots, m_n) \in M^n$. Como M^n es un R–módulo semisimple, Rm es un R–sumando directo de M^n. La Proposición 4.2.2 garantiza que Rm es un $\mathrm{End}_{S'}(M^n)$–submódulo de M^n, para $S' = \mathrm{End}_R(M^n)$. Como $\overline{f} \in \mathrm{End}_{S'}(M^n)$, deducimos que $\overline{f}(m) \in Rm$. Esto es, existe $r \in R$ tal que $\overline{f}(m) = rm$, lo que concluye la demostración en vista de (4.1). □

Lema 4.2.5 (Schur)**.** *Sea* M *un módulo simple sobre un anillo* R. *Si* ${}_RN$ *es otro módulo simple y* $f : M \to N$ *es un homomorfismo no nulo de* R*–módulos, entonces* f *es un isomorfismo. Como consecuencia,* $\mathrm{End}_R(M)$ *es un anillo de división.*

Demostración. Como $f \neq 0$, $\mathrm{Im}\, f$ es un submódulo no nulo de N, luego $\mathrm{Im}\, f = N$ y f es sobreyectivo. Pero $\ker f \neq M$, así que $\ker f = \{0\}$. Luego f es un isomorfismo. □

Proposición 4.2.6. *Sea* R *un anillo cuyo módulo regular* ${}_RR$ *es artiniano. Supongamos que* ${}_RM$ *es un módulo simple y pongamos* $D = \mathrm{End}_R(M)$. *Entonces* M *es un* D*–espacio vectorial de dimensión finita y*

$$\lambda : R \to \mathrm{End}_D(M)$$

es un homomorfismo sobreyectivo de anillos.

Demostración. Supongamos que ${}_DM$ fuese de dimensión infinita. Podemos, así, seleccionar, de una base B de ${}_DM$, cuya existencia está garantizada por el Corolario 4.0.2, un conjunto $\{x_i : i \in \mathbb{N}\} \subseteq B$ linealmente independiente. Para cada

$i \in \mathbb{N}$, tomamos la aplicación D–lineal $f_i : M \to M$ que vale 0 en todos los elementos de B salvo en x_i, donde asignamos $f_i(x_i) = x_i$. Por el Teorema 4.2.4, existe $r_i \in R$ tal que $f_i(x_j) = r_i x_j$ para todo $j = 0, \ldots, i$. Así, para $i \geq 1$,

$$r_i \in \operatorname{ann}_R(x_0) \cap \cdots \cap \operatorname{ann}_R(x_{i-1})$$

pero

$$r_i \notin \operatorname{ann}_R(x_0) \cap \cdots \cap \operatorname{ann}_R(x_i).$$

Obtenemos así una cadena estrictamente descendente de ideales a izquierda de R, con lo que ${}_RR$ no es artiniano.

Hemos demostrado, pues, que si ${}_RR$ es artiniano, entonces ${}_DM$ es finito-dimensional. Tomemos $\{m_1, \ldots, m_n\}$ una D–base de M. Si $f \in \operatorname{End}_D(M)$, el Teorema 4.2.4 nos da $r \in R$ tal que $f(m_i) = rm_i$ para $i = 1, \ldots, n$. De aquí, $f = \lambda(r)$ y deducimos que λ es sobreyectiva. □

Observación 7. En las hipótesis de la Proposición 4.2.6, deducimos del teorema del isomorfismo que $R/\operatorname{Ann}_R(M)$ es isomorfo a $\operatorname{End}_D(M)$.

Observación 8. El enunciado de la Proposición 4.2.6 se puede refinar como sigue: Dado un simple ${}_RM$, se tiene que $R/\operatorname{Ann}_R(M)$ es artiniano a izquierda si, y sólo si, ${}_DM$ es de dimensión finita, en cuyo caso, el anillo $R/\operatorname{Ann}_R(M)$ es isomorfo a $\operatorname{End}_D(M)$.

Ahora vamos a usar una herramienta sencilla que necesitamos para terminar de desentrañar la estructura de un anillo semisimple. Un elemento e de un anillo se dice *idempotente* si $e^2 = e$.

Definición 35. Un conjunto de idempotentes $e_1, \ldots, e_n \in R$ tales que

$$1 = e_1 + \cdots + e_n$$

y $e_i e_j = 0$ cuando $i \neq j$ se llamará un *conjunto completo de idempotentes ortogonales* (brevemente, CCIO).

Si $\{e_1, \ldots, e_n\}$ es un CCIO de R, entonces

$$R = Re_1 \dotplus \cdots \dotplus Re_n.$$

En efecto, si $r \in R$, entonces $r = \sum_{i=1}^{n} re_i$, luego $R = Re_1 + \cdots + Re_n$. Además, si $0 = \sum_{i=1}^{n} r_i e_i$ para ciertos $r_i \in R$, entonces, multiplicando por la derecha por e_j para cada $j = 1, \ldots, n$, obtenemos $0 = r_j e_j$. Así que la suma es directa.

Teorema 4.2.7. *Las siguientes condiciones son equivalentes para un anillo no nulo* R.

1. ${}_RR$ *es semisimple y todos los* R*–módulos simples son isomorfos entre sí;*

2. R *es isomorfo, como anillo, a* $\mathrm{End}_D(M)$ *para cierto anillo de división* D *y un* D*–espacio vectorial de dimensión finita* M*;*

3. ${}_RR$ *es artiniano y existe un* R*–módulo simple fiel;*

4. ${}_RR$ *es artiniano y los únicos ideales de* R *son* $\{0\}, R$*.*

Además, el anillo de división D *y la dimensión del* D*–espacio vectorial* M *mencionados en 4.5.5 están determinados por* R *en el sentido de que* D *es isomorfo como anillo a* $\mathrm{End}_R(\Sigma)$*, para* Σ *cualquier* R*–módulo simple, y* $\dim_D(M) = \ell({}_RR)$*.*

Demostración. (1) $\Rightarrow$ (4). Como ${}_RR$ es suma directa interna de un número finito de simples, resulta ser de longitud finita y, así, artiniano. Si ahora I es un ideal de R e $I \neq R$, entonces el R–módulo no nulo R/I es semisimple. Como es finitamente generado y todos los módulos simples son isomorfos entre sí, deducimos que $R/I \cong \Sigma^m$, para un módulo simple Σ. Así,

$$I = \mathrm{Ann}_R(R/I) = \mathrm{Ann}_R(\Sigma^m) = \mathrm{Ann}_R(\Sigma).$$

Pero $R \cong \Sigma^n$ para $n = \ell(R)$, así que

$$I = \mathrm{Ann}_R(\Sigma) = \mathrm{Ann}_R(\Sigma^n) = \mathrm{Ann}_R(R) = \{0\}.$$

(4) $\Rightarrow$ (3). Si Σ es cualquier módulo simple, entonces $\mathrm{Ann}_R(\Sigma) \neq R$. Luego $\mathrm{Ann}_R(\Sigma) = \{0\}$, por lo que Σ es fiel.

(3) $\Rightarrow$ (4.5.5). Consecuencia de la Proposición 4.2.6.

(4.5.5) $\Rightarrow$ (1). Pongamos $U = \mathrm{End}_D(M)$. Puesto que, para cada par de elementos $m, m' \in M$ con $m \neq 0$, existe un homomorfismo de D–espacios vectoriales $f \in U$ tal que $f(m) = m'$, deducimos que ${}_UM$ es simple.

Sea $\{m_1, \ldots, m_n\}$ una D–base de M. Para cada $i = 1, \ldots, n$, sea $e_i \in U$ el homomorfismo determinado por las condiciones $e_i(m_j) = 0$ si $j \neq i$ pero $e_i(m_i) = m_i$. Es claro que $\{e_1, \ldots, e_n\}$ es un CCIO para U, de modo que tenemos una descomposición

$$U = Ue_1 \dotplus \cdots \dotplus Ue_n. \tag{4.2}$$

Demostremos que cada Ue_i es simple. Basta con que demostremos que si $0 \neq fe_i$ para cierto $f \in U$, entonces $Ufe_i = Ue_i$. Tenemos que $0 \neq fe_i(m_i) = \sum_{j=1}^n a_j m_j$, para $a_j \in D$. Tomemos un índice k tal que $a_k \neq 0$, y definamos $s : M \to M$ por $s(m_j) = 0$ si $j \neq k$, mientras que $s(m_k) = a_k^{-1} m_i$.

Tenemos

$$sfe_i(m_i) = s(\sum_j a_j m_j) = a_k^{-1} a_k m_i = m_i,$$

de donde $sfe_i = e_i$ y, por tanto, $Ue_i \subseteq Ufe_i$.

Veamos que cada Ue_i es isomorfo a ${}_UM$. Tomemos el homomorfismo de U–módulos $\varphi : U \to M$ dado por $\varphi(f) = f(m_i)$. Como $\varphi(e_i) = m_i \neq 0$, deducimos

que la restricción de φ a Ue_i es no nula, luego, por el Lema de Schur, da un isomorfismo de U–módulos $Ue_i \cong M$. Por último, si ${}_U\Sigma$ es simple, entonces es isomorfo a un cociente de ${}_UU$, por lo que existe un epimorfismo $p : U \to \Sigma$. Así, la restricción de p a Ue_i ha de ser no nula para algún i, lo que da, por el Lema de Schur, un isomorfismo entre Ue_i y Σ.

Ahora, denotemos por $\phi : U \to R$ un isomorfismo de anillos. La descomposición como suma de simples (4.2) da una descomposición análoga

$$R = R\phi(e_1) \dotplus \cdots \dotplus R\phi(e_n).$$

Por tanto, R es semisimple y $\ell({}_RR) = \ell({}_UU)$.

Si Σ es un R–módulo simple, entonces, por la restricción de escalares proporcionada por el isomorfismo ϕ, tenemos que ${}_U\Sigma$ es simple y, como ya hemos demostrado, ha de ser isomorfo a ${}_UM$. Pero tal isomorfismo ha de ser también de R–módulos, por restricción de escalares asociada a ϕ^{-1}. Así que R es semisimple y todos sus módulos simples son isomorfos a ${}_RM$ y, por ende, isomorfos entre sí.

Para dar cuenta de la unicidad enunciada tras las afirmaciones equivalentes, observemos primero que $\mathrm{End}_U(M) = \mathrm{End}_R(M)$. Por otra parte, el homomorfismo de anillos

$$\lambda : D \to \mathrm{End}_U(M)$$

es un isomorfismo por el Teorema 4.2.4. Por último,

$$\dim_D(M) = n = \ell({}_UU) = \ell({}_RR).$$

□

Ejercicio 54. Supongamos que, para R un anillo, se tiene una descomposición ${}_RR = I_1 \dotplus \cdots \dotplus I_t$, para I_i ideales a izquierda. Demostrar que existe un CCIO $\{e_1, \ldots, e_t\}$ en R tal que $I_i = Re_i$, para $i = 1, \ldots, t$.

Ejercicio 55. Supongamos D y E anillos de división y sean ${}_DM$ y ${}_EN$ espacios vectoriales de dimensión finita. Demostrar que $\mathrm{End}_D(M)$ y $\mathrm{End}_E(N)$ son anillos isomorfos si, y sólo si, D y E son isomorfos y $\dim_D(M) = \dim_E(N)$.

Ejercicio 56. Sea M un módulo sobre un anillo R, $S = \mathrm{End}_R(M)$ y $T = \mathrm{End}_S(M)$. Demostrar que $S = \mathrm{End}_T(M)$. Deducir que, si Q es el cuerpo de fracciones de un dominio de integridad A, entonces Q es indescomponible como A–módulo.

Ejercicio 57. Sea K un cuerpo y

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

Demostrar que R es un anillo artiniano que no es semisimple. Calcular $\mathrm{Soc}({}_RR)$.

4.3. Componentes homogéneas

Nuestro próximo objetivo es descubrir la estructura de un anillo semisimple cualquiera.

Lema 4.3.1. *Dado cualquier anillo* R*, existe un conjunto* Ω_R *de* R*–módulos simples no isomorfos entre sí tal que cada* R*–módulo simple es isomorfo a un módulo en el conjunto* Ω_R*.*

Demostración. Sea ${}_RS$ cualquier módulo simple. Tomado $0 \neq s \in S$, tenemos que $S = Rs$. Como $Rs \cong R/\mathrm{ann}_R(s)$, vemos que cada R–módulo simple es isomorfo a un módulo de la forma R/I para I un ideal a izquierda maximal de R. Podemos tomar entonces en el conjunto de los ideales a izquierda maximales de R la relación de equivalencia $I \sim J$ si $R/I \cong R/J$ como R–módulos. Si tomamos un conjunto de representantes de las correspondientes clases de equivalencia de ideales maximales a izquierda bajo esta relación, obtenemos, realizando los respectivos módulos cocientes, un conjunto Ω_R de R–módulos simples como el descrito en el enunciado. □

Definición 36. El conjunto Ω_R descrito en el Lema 4.3.1 se llama *conjunto de tipos de isomorfía de* R*–módulos simples.*

Proposición 4.3.2. *Sea* ${}_RM$ *un módulo y definamos, para cada* $\Sigma \in \Omega_R$*, el submódulo* $\mathrm{Soc}_\Sigma(M)$ *como la suma de todos los submódulos de* M *isomorfos a* Σ *(si no hay ninguno de éstos,* $\mathrm{Soc}_\Sigma(M)$ *se define entonces como el submódulo* $\{0\}$*). Entonces*

$$\mathrm{Soc}(M) = \dotplus_{\Sigma\in\Omega_R}\mathrm{Soc}_\Sigma(M).$$

Además, si $f : M \to M$ *es un endomorfismo de* R*–módulos, entonces* $f(\mathrm{Soc}_\Sigma(M)) \subseteq \mathrm{Soc}_\Sigma(M)$ *para todo* $\Sigma \in \Omega_R$*.*

Demostración. Obviamente, por definición, $\mathrm{Soc}(M) = \sum_{\Sigma\in\Omega_R}\mathrm{Soc}_\Sigma(M)$. Tenemos, pues, que demostrar que si $\Sigma' \in \Omega_R$, entonces

$$N = \mathrm{Soc}_{\Sigma'}(M) \cap \sum_{\Sigma\neq\Sigma'}\mathrm{Soc}_\Sigma(M) = \{0\}.$$

Si $N \neq \{0\}$, entonces tomamos $0 \neq m \in N$. Tenemos que Rm es un módulo semisimple finitamente generado. Por tanto, es artiniano y ha de contener un sumódulo simple S. Como $S \subseteq \mathrm{Soc}_\Sigma(M)$, y esta inclusión ha de ser escindida, existe un epimorfismo $g : \mathrm{Soc}_\Sigma(M) \to S$. Al ser $S \neq \{0\}$, tenemos que $g \neq 0$, lo que implica que $g(S') \neq 0$ para algún $S' \subseteq M$ con $S' \cong \Sigma$. Pero, por el Lema de Schur, la restricción de g a S' da un isomorfismo $S' \cong S$. Luego $S \cong \Sigma$. Un argumento idéntico demuestra que $S \cong \Sigma'$ para algún $\Sigma' \neq \Sigma$. Como en Ω_R módulos distintos son no isomorfos, tenemos la contradicción $\Sigma \cong S \cong \Sigma'$. Por tanto, $N = \{0\}$.

Para la segunda parte, consideremos que

$$f(\mathrm{Soc}_\Sigma(M)) = f\left(\sum_{S\cong\Sigma} S\right) = \sum_{S\cong\Sigma} f(S) \subseteq \mathrm{Soc}_\Sigma(M),$$

donde la última inclusión viene del hecho de que, para $S \cong \Sigma$, se tiene que, o bien $f(S) = \{0\}$, o bien $f(S) \cong S$. □

Corolario 4.3.3. *Para cada $\Sigma \in \Omega_R$, $\mathrm{Soc}_\Sigma(R)$ es un ideal de R.*

Demostración. En efecto, si $r \in R$, entonces $\rho_r : R \to R$, definido por $\rho_r(s) = sr$, es un homomorfismo de R–módulos. Por la Proposición 4.3.2, $\rho_r(\mathrm{Soc}_\Sigma(R)) \subseteq \mathrm{Soc}_\Sigma(R)$. Deducimos fácilmente que $\mathrm{Soc}_\Sigma(R)$ es un ideal. □

Teorema 4.3.4. *Sea R un anillo semisimple. Entonces Ω_R es finito. Si ponemos $\Omega_R = \{\Sigma_1, \ldots, \Sigma_t\}$ y $D_i = \mathrm{End}_R(\Sigma_i)$, entonces $\dim_{D_i}(\Sigma_i)$ es finita para para $i = 1, \ldots, t$ y existe un isomorfismo de anillos*

$$R \cong \mathrm{End}_{D_1}(\Sigma_1) \times \cdots \times \mathrm{End}_{D_t}(\Sigma_t). \tag{4.3}$$

Demostración. Sabemos que $R = S_1 \dotplus \cdots \dotplus S_n$, para ciertos ideales a izquierda simples $S_1, \ldots, S_n$. Por otra parte, si $\Sigma \in \Omega_R$, entonces existe un epimorfismo $R \to \Sigma$ cuya restricción a algún S_i será no nula. El Lema de Schur nos dice ahora que $\Sigma \cong S_i$. Esto muestra la finitud de Ω_R.

Para obtener el isomorfismo (4.3), observemos primero que, para $i \neq j$, se tiene

$$\mathrm{Soc}_{\Sigma_j}(R) \subseteq \mathrm{Ann}_R(\Sigma_i). \tag{4.4}$$

Esto es consecuencia de que

$$\mathrm{Soc}_{\Sigma_j}(R) \cdot \mathrm{Soc}_{\Sigma_i}(R) \subseteq \mathrm{Soc}_{\Sigma_j}(R) \cap \mathrm{Soc}_{\Sigma_i}(R) = \{0\},$$

puesto que ambos son ideales por el Corolario 4.3.3.

Por otra parte, si ponemos $I_i = \sum_{j\neq i} \mathrm{Soc}_{\Sigma_j}(R)$, tenemos que $I_i + I_j = R$ si $i \neq j$. Esto, junto con (4.4), dar que los ideales $\mathrm{Ann}_R(\Sigma_i)$ son coprimos. Por el Teorema Chino del Resto, tenemos un isomorfismo de anillos

$$R \to R/\mathrm{Ann}_R(\Sigma_1) \times \cdots \times R/\mathrm{Ann}_R(\Sigma_t), \quad (r \mapsto (r + \mathrm{Ann}_R(\Sigma_1), \ldots, r + \mathrm{Ann}_R(\Sigma_t))),$$

ya que $\mathrm{Ann}_R(\Sigma_1) \cap \cdots \cap \mathrm{Ann}_R(\Sigma_t) = \{0\}$.

Deducimos del Teorema 4.2.7 que

$$R/\mathrm{Ann}_R(\Sigma_i) \cong \mathrm{End}_{D_i}(\Sigma_i),$$

para

$$D_i = \mathrm{End}_R(\Sigma_i).$$

□

Ejercicio 58. Sean R, S anillos y $T = R \times S$, el anillo producto. Tomamos $e = (1, 0) \in T$. Por $\pi : T \to R$ denotamos la proyección canónica dada por $\pi(r, s) = r$. Demostrar que la aplicación $\mathcal{L}({}_T Te) \to \mathcal{L}({}_R R)$ que envía un T–submódulo I de Te en $\pi(I)$ está bien definida y es una biyección que preserva la inclusión. Deducir que T es semisimple si, y sólo si, R y S son semisimples.

Para completar la clasificación de los anillos semisimples, hemos de discutir la unicidad de la descomposición proporcionada por el Teorema 4.3.4. Para ello, es útil discutir los idempotentes centrales de un anillo, es decir, los idempotentes del centro del anillo.

Ejercicio 59. Demostrar que, si e es un idempotente central de un anillo R, entonces Re es un anillo con el producto y la suma heredados de los de R y con e como uno.

Ejercicio 60. Demostrar que si $R = I \dotplus J$ para I, J ideales de R, entonces existe un idempotente central e tal que $I = Re$ y $J = R(1 - e)$.

Definición 37. Un ideal I no nulo de un anillo se dice *indescomponible* si no admite descomposiciones $I = I' \dotplus I''$ para ideales no nulos I', I'' de R. El anillo R se dice indescomponible si lo es como ideal.

Definición 38. Un idempotente central e de un anillo R se dice *indescomponible* si $e \neq 0$ si Re es un ideal indescomponible. Equivalentemente, si $e \neq 0$ y cada descomposición $e = e' + e''$, para e', e'' idempotentes centrales ortogonales implica que $e' = e$ o bien $e'' = e$. Observemos que el anillo R es indescomponible si 1 es un idempotente indescomponible.

Ejercicio 61. Demostrar que el anillo $\mathbb{Z}[\sqrt{3}]/\langle 3 \rangle$ es indescomponible.

Ejercicio 62. Demostrar que un anillo no nulo R es indescomponible si, y sólo si, R no es isomorfo a ningún producto de anillos $R_1 \times R_2$ con R_1, R_2 no triviales.

Observación 9. Un anillo semisimple es indescomponible si, y sólo si, satisface las condiciones equivalentes del Teorema 4.2.7.

Proposición 4.3.5. *Si un anillo contiene un CCIO centrales indescomponibles, entonces éste es único. Todo anillo R tal que $\ell({}_R R)$ es finita contiene un único CCIO centrales indescomponibles.*

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

Por otra parte, dado e_i, tenemos que

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

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

Para ver que el anillo ${}_RR$ tiene un CCIO centrales indescomponibles, razonaremos que cada ideal I de R admite una descomposición $I = I_1 \dotplus \cdots \dotplus I_n$ para ideales indescomponibles $I_1, \ldots, I_n$. Aplicando esto a $I = R$, obtenemos lo deseado. Pero la afirmación se sigue fácilmente por inducción sobre $\ell({}_RI)$.

□

Teorema 4.3.6. *Supongamos que* R *es un anillo semisimple con*

$$\Omega = \{\Sigma_1, \ldots, \Sigma_t\}$$

y que se tiene un isomorfismo de anillos

$$R \cong R_1 \times \cdots \times R_s,$$

donde $R_1, \ldots, R_s$ *son anillos indescomponibles. Entonces* $s = t$ *y, salvo eventual reordenación,* $R_i \cong \mathrm{End}_{D_i}(\Sigma_i)$ *con* $D_i = \mathrm{End}_R(\Sigma_i)$ *para* $i = 1, \ldots, t$*. Además, los anillos de división* $D_1, \ldots, D_t$ *son únicos salvo isomorfismos y los números* $\dim_{D_1}(\Sigma_1), \ldots, \dim_{D_t}(\Sigma_t)$ *son únicos.*

Demostración. Una primera observación, que vamos a usar, es que los CCIO centrales indescomponibles se preservan por isomorfismos de anillos. A partir de aquí, el enunciado es claro, ya que $R = \mathrm{Soc}_{\Sigma_1}(R) \dotplus \cdots \dotplus \mathrm{Soc}_{\Sigma_t}(R)$ es la descomposición de R como suma directa de ideales indescomponibles.

□

Definición 39. Un anillo semisimple R se dirá de tipo $(D_1, \ldots D_t, n_1, \ldots, n_t)$ si es isomorfo a $\mathrm{End}_{D_1}(\Sigma_1) \times \cdots \times \mathrm{End}_{D_t}(\Sigma_t))$ con $n_i = \dim_{D_i}(\Sigma_i)$.

Corolario 4.3.7. *Sea* R *un anillo semisimple, mantenemos la notación anterior. Si* M *es un* R*–módulo, entonces, para cada* $i = 1, \ldots, t$*, se tiene*

$$\mathrm{Soc}_{\Sigma_i}(M) = e_i M = \{e_i m : m \in M\}.$$

Demostración. Observemos que $\mathrm{Ann}_R(\Sigma_i) = \mathrm{Ann}(Re_i)$, así que si $r \in \mathrm{Ann}(Re_i)$, entonces $re_i = 0$. Pero $r = re_1 + \cdots + re_t$, luego $r \in \sum_{j \neq i} Re_j$. Tenemos, pues, que $\mathrm{Ann}_R(\Sigma_i) \subseteq \sum_{j \neq i} Re_j$. Puesto que la inclusión recíproca se demostró en la prueba del Teorema 4.3.4, deducimos que

$$\mathrm{Ann}_R(\Sigma_i) = \sum_{j \neq i} Re_j \tag{4.5}$$

Si N es cualquier submódulo simple de M isomorfo a Σ_i, entonces, según (4.5),

$$\mathrm{Ann}_R(N) = \mathrm{Ann}_R(\Sigma_i) = \sum_{j \neq i} Re_i.$$

De aquí, para $m \in N$, tenemos que $m = e_i m$. Deducimos, pues, que $\mathrm{Soc}_{\Sigma_i}(M) \subseteq e_i M$. Para la inclusión recíproca, observemos que si $m \in M$, entonces $\mathrm{ann}_R(e_i m) \supseteq \sum_{j \neq i} Re_j$. Por tanto, tenemos un epimorfismo de módulos

$$Re_i \cong R/\sum_{j \neq i} Re_j \to R/\mathrm{ann}_R(e_i m) \cong Re_i m.$$

Como $Re_i = \mathrm{Soc}_{\Sigma_i}(R)$, deducimos que $Re_i m$ es suma de módulos simples isomorfos a Σ_i, esto es, $Re_i m \subseteq \mathrm{Soc}_{\Sigma_i}(M)$. □

4.4. Anillo opuesto y módulos a derecha.

Para un anillo R, tenemos el llamado anillo opuesto R^{op}. Como grupo aditivo, $R^{op} = R$, pero el producto se modifica definiendo $r * s = sr$, para $r, s \in R^{op}$. Algunos R^{op}–módulos aparecen de forma natural a partir de los R–módulos, como indica la siguiente construcción.

Sea M un R–módulo. Sobre el grupo aditivo

$$^*M = \{f : M \to R \mid f \text{ es homomorfismo de } R-\text{módulos}\}$$

se tiene una estructura de R^{op}–módulo dada, para $r \in R^{op}$, $\varphi \in {}^*M$, por

$$(r \cdot \varphi)(m) = \varphi(m)r, \qquad m \in M. \tag{4.6}$$

Ejercicio 63. Comprobar que, con la acción dada en (4.6), $^*M$ es ciertamente un R^{op}–módulo.

Tenemos un homomorfismo de anillos

$$\theta : \mathrm{End}_R(M)^{op} \to \mathrm{End}_{R^{op}}({}^*M) \tag{4.7}$$

definido por

$$\theta(f)(\varphi) = \varphi \circ f, \qquad f \in \mathrm{End}_R(M)^{op}, \varphi \in \mathrm{End}_{R^{op}}({}^*M). \tag{4.8}$$

Ejercicio 64. Comprobar que θ, definido según (4.8), es un homomorfismo de anillos.

Proposición 4.4.1. *Supongamos que ${}_R M$ es libre con base $\{v_1, \ldots, v_n\}$. Para $i = 1, \ldots, n$, tomamos ${}^*v_i \in {}^*M$ definidos por ${}^*v_i(v_j) = \delta_{ij}$, ("delta de Kronecker"). Entonces $\{{}^*v_1, \ldots, {}^*v_n\}$ es una base para el R^{op}–módulo $^*M$ y el homomorfismo de anillos* (4.7) *es un isomorfismo.*

Demostración. Para cada $m \in M$, se tiene que

$$m = \sum_{i=1}^{n} {}^*v_i(m)v_i.$$

Así, si $\varphi \in {}^*M$, tenemos

$$\varphi(m) = \sum_{i=1}^{n} {}^*v_i(m)\varphi(v_i) = (\sum_{i=1}^{n} \varphi(v_i) \cdot {}^*v_i)(m).$$

Por tanto,

$$\varphi = \sum_{i=1}^{n} \varphi(v_i)\, {}^*v_i,$$

de donde $\{{}^*v_1, \ldots, {}^*v_n\}$ es un conjunto de generadores del R^{op}–módulo ${}^*M$. Ahora, si $0 = \sum_{i=1}^{n} r_i {}^*v_i$ para $r_i \in R^{op}$, entonces, evaluando en v_j, obtenemos que $r_j = 0$, por lo que se trata de una base.

Bien, probemos que θ es un isomorfismo. Si $f \in \mathrm{End}_R(M)$ es tal que $\theta(f) = 0$ entonces, dado $m \in M$, tenemos

$$f(m) = \sum_i {}^*v_i(f(m))v_i = \sum_i \theta(f)({}^*v_i)(m)v_i = 0.$$

Por tanto, $f = 0$ y θ es inyectivo.

Para ver que es sobreyectivo, dado $\psi \in \mathrm{End}_{R^{op}}({}^*M)$ definamos la aplicación $f : M \to M$ como

$$f(m) = \sum_i \psi({}^*v_i)(m)v_i, \qquad (m \in M).$$

Es fácil ver que $f \in \mathrm{End}_R(M)$. Por otra parte, para $\varphi \in {}^*M$ y $m \in M$, tenemos

$$\begin{array}{rcl} \theta(f)(\varphi)(m) & = & \varphi(f(m)) \\ & = & \sum_i \varphi(\psi({}^*v_i)(m)v_i) \\ & = & \sum_i \psi({}^*v_i)(m)\varphi(v_i) \\ & = & (\sum_i \varphi(v_i)\psi({}^*(v_i))(m) \\ & = & \psi(\sum_i \varphi(v_i){}^*v_i)(m) \\ & = & \psi(\varphi)(m). \end{array}$$

De donde $\theta(f) = \psi$. □

Teorema 4.4.2. *Si* R *es semisimple de tipo* $(D_1, \ldots, D_t, n_1, \ldots, n_t)$*, entonces* R^{op} *es semisimple de tipo* $(D_1^{op}, \ldots, D_t^{op}, n_1, \ldots, n_t)$*.*

Demostración. Tenemos que R es isomorfo al anillo $\mathrm{End}_{D_1}(\Sigma_1) \times \cdots \times \mathrm{End}_{D_t}(\Sigma_t)$. Por tanto, R^{op} es isomorfo a $\mathrm{End}_{D_1}(\Sigma_1)^{op} \times \cdots \times \mathrm{End}_{D_t}(\Sigma_t)^{op}$. Para cada i, tenemos un isomorfismo de anillos $\mathrm{End}_{D_i}(\Sigma_i)^{op} \cong \mathrm{End}_{D_i^{op}}({}^*\Sigma_i)$ y $\dim_{D_i}(\Sigma_i) = \dim_{D_i^{op}}({}^*\Sigma_i)$. □

Ejercicio 65. Un anillo R puede dotarse de estructura de R^{op}–módulo mediante el homomorfismo de anillos $\rho : R^{op} \to \mathrm{End}(R)$ dado por $\rho(r)(s) = sr$ para $r, s \in R$ (si se quiere, R es un R–módulo a derecha). Para el subanillo

$$R = \{\begin{pmatrix} r & z \\ 0 & w \end{pmatrix} : r \in \mathbb{R}, z, w \in \mathbb{C}\}$$

de $M_2(\mathbb{C})$, calcular $\ell({}_R R)$ y $\ell({}_{R^{op}} R)$.

4.5. Funciones sobre un grupo finito

Sea G un grupo con elemento neutro e y denotemos por $\mathbb{C}G$ el espacio vectorial complejo con base G. Consideremos la aplicación bilineal $\mu : \mathbb{C}G \times \mathbb{C}G \to \mathbb{C}G$ determinada, sobre los elementos de la base G por la multiplicación de G, esto es, $\mu(g, h) = gh$, para $g, h \in G$. Para cada elemento $r \in \mathbb{C}G$, usaremos la expresión $r = \sum_{g \in G} r_g g$, con $r_g \in \mathbb{C}$. De esta manera, la expresión de la multiplicación μ será

$$rs := \mu(r, s) = \sum_{g,h \in G} r_g s_h gh, \qquad (r, s \in \mathbb{C}G).$$

Como la multiplicación en G es asociativa, deducimos que así lo es la multiplicación que hemos definido en $\mathbb{C}G$. Además, e resulta ser obviamente el elemento neutro para esta multiplicación. Obtenemos así un anillo, que seguimos denotando por $\mathbb{C}G$.

Observemos que la aplicación $\eta : \mathbb{C} \to \mathbb{C}G$ definida por $\eta(z) = ze$, para $z \in \mathbb{C}$, es un homomorfismo de anillos. Así, podemos identificar $\mathbb{C}$ con el subanillo

$$\mathrm{Im}\,(\eta) = \{ze : z \in \mathbb{C}\}$$

de $\mathbb{C}G$. De hecho, se trata de un subanillo del centro de $\mathbb{C}G$, ya que, para $z \in \mathbb{C}$ y $r \in \mathbb{C}G$, tenemos

$$rze = (\sum_{g \in G} r_g g)ze = \sum_{g \in G} r_g zge = \sum_{g \in G} zr_g eg = zer.$$

Así, a partir de ahora, consideraremos que $\mathbb{C}$ es un subanillo del centro de $\mathbb{C}G$, lo que hace de éste último un álgebra asociativa compleja con uno. Por cierto, consecuentemente, escribiremos $e = 1e = 1$, cuando sea conveniente. Este álgebra se llama *álgebra compleja del grupo* G.

Consideremos ahora el $\mathbb{C}$–espacio vectorial de las aplicaciones de G en $\mathbb{C}$:

$$\mathcal{M}(G) = \{\varphi : G \to \mathbb{C}\}.$$

Dados $g \in G$, $\varphi \in \mathcal{M}(G)$, definimos $\rho(g)(\varphi) \in \mathcal{M}(G)$ por

$$\rho(g)(\varphi)(x) = \varphi(xg), \qquad (x \in G).$$

Obtenemos, así, una aplicación $\rho(g) : \mathcal{M}(G) \to \mathcal{M}(G)$, que resulta ser lineal. Así que tenemos una aplicación

$$\rho : G \to \mathrm{End}_{\mathbb{C}}(\mathcal{M}(G)).$$

El siguiente cálculo muestra que $\rho(gh) = \rho(g) \circ \rho(h)$ para todo $g, h \in G$:

$$\rho(gh)(\varphi)(x) = \varphi(xgh) = \rho(h)(\varphi)(xg) = \rho(g)(\rho(h)(\varphi))(x), \qquad (x \in G, \varphi \in \mathcal{M}(G)).$$

De esta forma, ρ deviene en lo que se llama una representación lineal de G con espacio de representación $\mathcal{M}(G)$.

Ahora, ρ define una aplicación lineal

$$\widetilde{\rho} : \mathbb{C}G \to \mathrm{End}_{\mathbb{C}}(\mathcal{M}(G))$$

que, al preservar ρ productos, es un homomorfismo de anillos. Por tanto, $\mathcal{M}(G)$ es un $\mathbb{C}G$–módulo, con la acción

$$(r\varphi)(x) = \widetilde{\rho}(r)(\varphi)(x) = \sum_{g \in G} r_g \rho(g)(\varphi)(x) = \sum_{g \in G} r_g \varphi(xg).$$

Dado un $\mathbb{C}G$–módulo V de dimensión finita y una $\mathbb{C}$–base $\{v_1, \ldots, v_n\}$ de V tenemos, para cada $x \in G$,

$$xv_i = \sum_{j=1}^{n} t_{ij}(x) v_j,$$

para ciertas $t_{ij} \in \mathcal{M}(G)$. Estas son las llamadas *funciones matriciales* del módulo V asociadas a la base $\{v_1, \ldots, v_n\}$. Supongamos ahora un homomorfismo de $\mathbb{C}G$–módulos $f : V \to V'$, con V' de dimensión finita y base $\{v'_1, \ldots, v'_m\}$. Denotamos por t'_{ij} a las funciones matriciales de V' con respecto de esta base. Sea $A = (a_{ij})$ la matriz de f con respecto de las bases mencionadas, esto es,

$$f(v_i) = \sum_j a_{ij} v'_j.$$

Dado $x \in G$, tenemos

$$xf(v_i) = x \sum_j a_{ij} x v'_j = \sum_j a_{ij} \sum_k t'_{jk}(x) v'_k,$$

y

$$f(xv_i) = f(\sum_j t_{ij}(x) v_j) = \sum_j t_{ij}(x) f(v_j) = \sum_j t_{ij}(x) \sum_k a_{jk} v'_k.$$

Como $xf(v_i) = f(xv_i)$ para todo $x \in G$, obtenemos la igualdad matricial

$$(t_{ij})A = A(t'_{ij}). \tag{4.9}$$

Lema 4.5.1. *El subespacio vectorial* $C(V)$ *de* $\mathcal{M}(G)$ *generado por las funciones matriciales* $\{t_{ij} : 1 \leq i, j \leq n\}$ *es independiente de la base escogida, y es un* $\mathbb{C}G$*–submódulo de* $\mathcal{M}(G)$*. Además, si* V' *es un* $\mathbb{C}G$*–módulo isomorfo a* V*, entonces* $C(V) = C(V')$*.*

Demostración. Si f es un isomorfismo, la matriz A es inversible, así que la ecuación (4.9) implica que cada t'_{kl} es combinación lineal de las funciones t_{ij}, y recíprocamente. Por tanto, ambos conjuntos de funciones matriciales generan el mismo subespacio vectorial. Esto da cuenta de que $C(V)$ no depende de la base escogida y que, de hecho, es el mismo para cualquier módulo isomorfo a V.

Observemos ahora que, para $x, y \in G$ cualesquiera,

$$t_{ij}(xy) = \sum_k t_{ik}(y)t_{kj}(x)$$

Ahora, si $x, y \in G$, tenemos

$$yt_{ij}(x) = t_{ij}(xy) = \sum_k t_{ik}(y)t_{kj}(x) = (\sum_k t_{ik}(y)t_{kj})(x),$$

por lo que

$$yt_{ij} = \sum_k t_{ik}(y)t_{kj}.$$

Así que $C(V)$ es un $\mathbb{C}G$–submódulo de $\mathcal{M}(G)$. □

Enunciemos este hecho junto con otra propiedad que es útil.

Proposición 4.5.2. *Para cada* $\mathbb{C}G$*–módulo* V *de dimensión finita, se tiene que* $C(V)$ *es un* $\mathbb{C}G$*–submódulo de* $\mathcal{G}$*. Si* $f : V \to \mathcal{M}(G)$ *es un homomorfismo de* $\mathbb{C}G$*–módulos, entonces* $\operatorname{Im} f \subseteq C(V)$*.*

Demostración. Basta con comprobar que $f(v_i) \in C(V)$ para los elementos v_i de una base de V. En efecto, dado $x \in G$, tenemos que

$$f(v_i)(x) = xf(v_i)(e) = f(xv_i)(e) = f(\sum_j t_{ij}(x)v_j)(e) = \sum_j t_{ij}(x)f(v_j)(e).$$

De donde

$$f(v_i) = \sum_j f(v_j)(e)t_{ij} \in C(V).$$

□

Definición 40. Definimos el $\mathbb{C}G$–submódulo $\mathcal{R}(G)$ de las funciones representativas sobre G como la suma de todos los submódulos $C(V)$ para V $\mathbb{C}G$–módulo de dimensión finita.

4.5.1. Grupos finitos

Vamos a tratar ahora el caso en que G es un grupo finito.

Usaremos alguna terminología proveniente de la teoría de representaciones. Así, por ejemplo, si tomamos un $\mathbb{C}G$–módulo V, tenemos un homomorfismo de grupos $\rho : G \to GL(V)$ dado por $\rho(g)(v) = gv$ para $g \in G, v \in V$. Esto es lo que se llama una representación compleja de G con espacio de representación V. De hecho, la estructura de $\mathbb{C}G$–módulo queda completamente determinada por esta representación y resulta equivalente, dado un espacio vectorial complejo V, dar una representación compleja de G cuyo espacio de representación es V y dar una estructura de $\mathbb{C}G$–módulo sobre V.

Cuando el espacio de representación V es de dimensión finita y viene dotado de un producto interno $\langle -, - \rangle$, la representación ρ se llama unitaria si todos los operadores $\rho(g)$ para $g \in G$ son unitarios.

Proposición 4.5.3. *Si la representación dada por un $\mathbb{C}G$–módulo V de dimensión finita es unitaria y W es un $\mathbb{C}G$–submódulo de V, entonces $W^\perp$ es un $\mathbb{C}G$–submódulo de V. Por tanto, toda representación unitaria de dimensión finita da un $\mathbb{C}G$–módulo semisimple.*

Demostración. Sean $u \in W^\perp$, $g \in G$. Dado $w \in W$, tenemos que

$$\langle gu, w \rangle = \langle gu, gg^{-1}w \rangle = \langle u, g^{-1}w \rangle = 0,$$

ya que $g^{-1}w \in W$. Por tanto, $gu \in W^\perp$.

Para la segunda afirmación, si V no es simple, entonces tomo un $\mathbb{C}G$–submódulo no nulo propio W de V. Sabemos que $W^\perp$ es también un $\mathbb{C}G$–submódulo y que $V = W \dot{+} W^\perp$. Una sencilla inducción sobre la longitud (o sobre la dimensión compleja, como se prefiera) muestra que V es semisimple. □

Proposición 4.5.4. *Sea V un $\mathbb{C}G$–módulo de dimensión finita como espacio vectorial. Existe un producto interno sobre V tal que la representación de G dada por V es unitaria. Por tanto, V es semisimple.*

Demostración. Tomamos un producto interno cualquiera $\langle -, - \rangle$ en V y, a partir de él, definimos

$$\langle u, v \rangle_G = \sum_{g \in G} \langle gu, gv \rangle,$$

para $u, v \in V$. Es rutinario comprobar que $\langle , \rangle_G$ es también un producto interno en V. Además, tenemos, para cada $g \in G$, $u, v \in V$, que

$$\langle gu, gv \rangle_G = \sum_{x \in G} \langle xgu, xgv \rangle = \sum_{y \in G} \langle yu, yv \rangle = \langle u, v \rangle_G,$$

donde hicimos el cambio de variable $y = xg$ en G. Así, la representación dada por el módulo V resulta unitaria con respecto de $\langle -, - \rangle_G$. Por la Proposición 4.5.3, deducimos que V es semisimple. □

Teorema 4.5.5. *El álgebra de grupo* $\mathbb{C}G$ *es semi-simple.*

Demostración. Como G es finito, el módulo regular $\mathbb{C}G$ es semisimple por la Proposición 4.5.4. □

Lema 4.5.6. *Si* Σ *es un* $\mathbb{C}G$*–módulo simple, entonces*

$$\mathrm{End}_{\mathbb{C}G}(\Sigma) = \{\lambda\, \mathrm{id}_\Sigma : \lambda \in \mathbb{C}\}.$$

Demostración. Tenemos que, por el Lema de Schur, $D = \mathrm{End}_{\mathbb{C}G}(\Sigma)$ es un anillo de división. De hecho, es un álgebra compleja. Además, puesto que Σ es isomorfo a un cociente de $\mathbb{C}G$, resulta ser de dimensión finita como $\mathbb{C}$–espacio vectorial. Por tanto, D es un anillo de división que, como $\mathbb{C}$, es de dimensión finita. De aquí, es de dimensión compleja 1. □

Teorema 4.5.7. *Sea* $\Omega_{\mathbb{C}G} = \{\Sigma_1, \ldots, \Sigma_t\}$*. Entonces existe un isomorfismo de* $\mathbb{C}$*–álgebras*

$$\mathbb{C}G \cong \mathrm{End}_{\mathbb{C}}(\Sigma_1) \times \cdots \times \mathrm{End}_{\mathbb{C}}(\Sigma_t).$$

Por tanto,

$$|G| = \dim_{\mathbb{C}}(\Sigma_1)^2 + \cdots + \dim_{\mathbb{C}}(\Sigma_t)^2.$$

Demostración. □

Lema 4.5.8. *Si* $f : V \to W$ *es una aplicación* $\mathbb{C}$*–lineal entre dos* $\mathbb{C}G$*–módulos, entonces la aplicación* $\widetilde{f} : V \to W$ *definida por*

$$\widetilde{f}(v) = \sum_{x \in G} x^{-1} f(xv)$$

es un homomorfismo de $\mathbb{C}G$*–módulos.*

Demostración. Para $y \in G$, $v \in V$, tenemos

$$\widetilde{f}(yv) = \sum_{x \in G} x^{-1} f(xyv) = \sum_{z \in G} yz^{-1} f(zv) = y\widetilde{f}(v).$$

□

Dado un módulo de dimensión finita V sobre $\mathcal{M}(G)$, y fijada una base suya, a las funciones matriciales calculadas con respecto de ésta las denotaremos por t_{ij}^V.

Teorema 4.5.9. *Sea* G *un grupo finito. Sobre* $\mathcal{M}(G)$ *definimos el producto interno*

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

Si $\Omega_{\mathbb{C}G} = \{\Sigma_1, \ldots, \Sigma_t\}$, *entonces*

$$\mathcal{M}(G) = C(\Sigma_1) \dot{+} \cdots \dot{+} C(\Sigma_t). \tag{4.10}$$

Además, si dotamos a cada Σ_a *de un producto interno de manera que la representación de* G *asociada sea unitaria, tomamos funciones matriciales con respecto de bases ortonormales y ponemos* $d_a = \dim_{\mathbb{C}} \Sigma_a$, *entonces*

$$\{\sqrt{d_a}\, t_{jk}^{\Sigma_a} : a = 1, \ldots, t, 1 \leq j, k \leq d_i\}, \tag{4.11}$$

es una base ortonormal de $\mathcal{M}(G)$.

Demostración. Como $\mathcal{M}(G)$ is semisimple, podemos tomar su descomposición en componentes homogéneas

$$\mathcal{M}(G) = \mathrm{Soc}_{\Sigma_1}(\mathcal{M}(G)) \dot{+} \cdots \dot{+} \mathrm{Soc}_{\Sigma_t}(\mathcal{M}(G)).$$

Por el Lema 4.5.2, $\mathrm{Soc}_{\Sigma_i}(\mathcal{M}(G)) \subseteq C(\Sigma_i)$, así que

$$\mathcal{M}(G) = C(\Sigma_1) + \cdots + C(\Sigma_t). \tag{4.12}$$

Supongamos ahora $\mathbb{C}G$–módulos de dimensión finita V y W, dotados con sendos productos internos para los cuales las representaciones correspondientes de G son unitarias. Tomamos bases ortonormales $\{v_1, \ldots, v_n\}$ de V y $\{w_1, \ldots, w_m\}$ de W.

Para $i = 1, \ldots, n, j = 1, \ldots, m$, definimos la aplicación lineal $p_{ij} : V \to W$ por

$$p_{ij}(v_k) = \begin{cases} w_j & \text{si } k = i \\ 0 & \text{si } k \neq i. \end{cases}$$

Tenemos, de acuerdo con el Lema 4.5.8, el homomorfismo de $\mathbb{C}G$–módulos $\widetilde{p}_{ij} : V \to W$ dado por

$$\widetilde{p}_{ij}(v) = \sum_{x \in G} x^{-1} p_{ij}(xv), \qquad v \in V.$$

Bien, la cosa es que

$$\widetilde{p}_{ij}(v_k) = \sum_{x \in G} x^{-1} p_{ij}(xv_k) = \sum_{x \in G} x^{-1} p_{ij}\Big(\sum_l t_{kl}^V(x) v_l\Big)$$
$$= \sum_{x \in G} x^{-1} t_{ki}^V(x) w_j = \sum_l \sum_{x \in G} t_{ki}^V(x) t_{jl}^W(x^{-1}) w_l.$$

Por otra parte, como cada matriz $(t_{ij}^W(x))$ es unitaria, obtenemos

$$(t_{jl}^W(x^{-1})) = (t_{jl}^W(x))^{-1} = (\overline{t_{lj}^W(x)}).$$

Así,

$$\widetilde{p}_{ij}(v_k) = \sum_l \left(\sum_{x \in G} t^V_{ki}(x) \overline{t^W_{lj}(x)} \right) w_l. \tag{4.13}$$

Si tomamos V y W simples no isomorfos, entonces $\widetilde{p}_{ij} = 0$ para todo i, j y, en virtud de (4.13),

$$0 = \sum_{x \in G} t^V_{ki}(x) \overline{t^W_{lj}(x)},$$

para todo i, j, k, l. Esto muestra que, para $a \neq b$, toda función $t^{\Sigma_a}_{ij}$ es ortogonal a toda función $t^{\Sigma_b}_{kl}$. En particular, la suma (4.12) ha de ser directa, luego obtenemos (4.10).

Tomemos ahora $V = W = \Sigma_a$ para cierto $a = 1, \ldots, t$. Por el Lema 4.5.6, $\widetilde{p}_{ij} = \alpha_{ij} id_{\Sigma_a}$ para cierto escalar $\alpha_{ij} \in \mathbb{C}$. Por (4.13), tenemos que

$$\alpha_{ij} v_k = \sum_l \left(\sum_{x \in G} t^{\Sigma_a}_{ki}(x) \overline{t^{\Sigma_a}_{lj}(x)} \right) v_l, \tag{4.14}$$

para todo $k = 1, \ldots, d_a$.

Para $k \neq l$, deducimos de (4.14) que

$$0 = \sum_{x \in G} t^{\Sigma_a}_{ki}(x) \overline{t^{\Sigma_a}_{lj}(x)}.$$

Pero si $l = k$ con $i \neq j$, tenemos que

$$0 = \sum_{x \in G} t^{\Sigma_a}_{ik}(x^{-1}) \overline{t^{\Sigma_a}_{jk}(x^{-1})} = \sum_{x \in G} \overline{t^{\Sigma_a}_{ki}(x)} t^{\Sigma_a}_{kj}(x).$$

Conjugando,

$$0 = \sum_{x \in G} t^{\Sigma_a}_{ki}(x) \overline{t^{\Sigma_a}_{kj}(x)}.$$

Tenemos, por tanto, que cada par de funciones matriciales distintas asociadas a Σ_a son ortogonales. Finalmente,

$$\sum_{x \in G} t^{\Sigma_a}_{ki}(x) \overline{t^{\Sigma_a}_{ki}(x)} = \alpha_{ii}.$$

Por otra parte, si hacemos explícita la representación $\rho : G \to GL(\Sigma_a)$, tenemos que

$$\widetilde{p_{ii}} = \sum_{x \in G} \rho(x^{-1}) p_{ii} \rho(x) = \sum_{x \in G} \rho(x)^{-1} p_{ii} \rho(x).$$

Tomando trazas, $\alpha_{ii} d_a = |G|$. Por tanto,

$$\langle t_{ik}, t_{ik} \rangle = 1/d_a.$$

□

Seguidamente, vamos a dar algunos ejemplos de descomposición de funciones sobre grupos finitos. Comenzaremos por algunos conmutativos, para cuya discusión será útil el siguiente hecho.

Proposición 4.5.10. *Si* G *es un grupo abeliano, entonces todo* $\mathbb{C}G$*–módulo simple de dimensión finita tiene dimensión* 1 *como espacio vectorial complejo. Como consecuencia, si* G *es abeliano finito, entonces* $\Omega_{\mathbb{C}G}$ *tiene cardinal* $|G|$*.*

Demostración. Sea Σ simple de dimensión finita. Dado $x \in G$, la aplicación lineal $f_x : \Sigma \to \Sigma$ dada por $f_x(v) = xv$ es un homomorfismso de $\mathbb{C}G$–módulos, ya que, para $y \in G$, tenemos

$$f_x(yv) = xyv = yxv = yf_x(v).$$

Por el Lema 4.5.6, $f_x(v) = \alpha_x v$ para cierto $\alpha_x \in \mathbb{C}$. Ahora, tomo $0 \neq v \in \Sigma$. Si $w \in \Sigma$, entonces existe $\sum_{x\in G} \lambda_x x \in \mathbb{C}G$ tal que

$$w = \sum_{x\in G} \lambda_x xv = \sum_{x\in G} \lambda_x \alpha_x v$$

Por tanto, v genera Σ como espacio vectorial.

Si ahora G es finito, y $\Omega_{\mathbb{C}G} = \{\Sigma_1, \ldots, \Sigma_n\}$, entonces, por el Teorema de Wedderburn-Artin,

$$\mathbb{C}G \cong \mathrm{End}_{\mathbb{C}}(\Sigma_1) \times \cdots \times \mathrm{End}_{\mathbb{C}}(\Sigma_n).$$

Comparando dimensiones, deducimos que $|G| = n$. □

Ejemplo. Tomemos $G = \mathbb{Z}_n$. Por la Proposición 4.5.10,

$$\Omega_{\mathbb{C}G} = \{\Sigma_0, \ldots, \Sigma_{n-1}\},$$

y cada Σ_j es de dimensión compleja 1. Podemos dar directamente una tal colección de simples no isomorfos como sigue. Sea $\omega = e^{\mathbf{i}2\pi/n} \in \mathbb{C}$. Para $j = 0, \ldots, n-1 \in \mathbb{Z}_n$, defino, para un espacio vectorial complejo Σ_j de dimensión 1 con base u_j,

$$k \cdot u_j = \omega^{jk} u_j \qquad (k = 0, \ldots, n-1).$$

Dicha acción, extendida por linealidad, da una estructura de $\mathbb{C}\mathbb{Z}_n$–módulo, a fortiori simple, sobre Σ_j. Un homomorfismo de módulos $f : \Sigma_j \to \Sigma_{j'}$ estaría determinado por $\alpha \in \mathbb{C}$ tal que $f(u_j) = \alpha u_{j'}$. Ahora, para $1 \in \mathbb{Z}_n$, tendríamos

$$\omega^j \alpha u_{j'} = f(\omega^j u_j) = f(1 \cdot u_j) = 1 \cdot \alpha u_{j'} = \alpha \omega^{j'} u_{j'}.$$

De donde, si $\alpha \neq 0$, entonces $j = j'$. Por tanto, los módulos Σ_j no son isomorfos entre sí.

La base ortonormal correspondiente a estas representaciones unitarias es $\{t^{\Sigma_0}, \ldots, t^{\Sigma_{n-1}}\}$, donde $t^{\Sigma_j}(k) = \omega^{jk}$, para $k = 0, \ldots, n-1$. Así, cualquier función $\varphi \in \mathbb{Z}_n$ se expresa como

$$\varphi = \sum_{j=0}^{n-1} \langle \varphi, t^{\Sigma_j} \rangle t^{\Sigma_j},$$

donde

$$\langle \varphi, t^{\Sigma_j} \rangle = \frac{1}{n} \sum_{k \in \mathbb{Z}_n} \varphi(k) \overline{t^{\Sigma_j}(k)} = \frac{1}{n} \sum_{k \in \mathbb{Z}_n} \varphi(k) \omega^{-jk}.$$

Ejemplo. Consideramos ahora el grupo $\mathbb{Z}_n \times \mathbb{Z}_m$. Vamos a calcular

$$\Omega_{\mathbb{Z}_n \times \mathbb{Z}_m} = \{\Sigma_{(j,j')} : 0 \leq j \leq n-1, 0 \leq j' \leq m-1\}.$$

Tomamos $\omega = e^{\mathbf{i}2\pi/n}$, $\mu = e^{\mathbf{i}2\pi/m} \in \mathbb{C}$. Tomo un vector $u_{j,j'}$ de $\Sigma_{(j,j')}$, que considero como base ortonormal. Sobre $\Sigma_{(j,j')}$ definimos una representación declarando

$$(k, k') \cdot u_{(j,j')} = \omega^{kj} \mu^{k'j'} u_{(j,j')}.$$

Razonando como en el ejemplo anterior, obtenemos que estas representaciones dan módulos simples no isomorfos y que una base ortonormal de $\mathcal{M}(\mathbb{Z}_n \times \mathbb{Z}_m)$ es

$$\{t^{\Sigma_{(j,j')}} : 0 \leq j \leq n-1, 0 \leq j' \leq m-1\},$$

para $t^{\Sigma_{(j,j')}}(k, k') = \omega^{kj} \mu^{k'j'}$.

Ejemplo. Tomemos el grupo diédrico D_n dado por generadores r, s sujetos a las relaciones $r^n = s^2 = 1, sr = r^{-1}s$. Así,

$$D_n = \{s^a r^k : a = 0, 1; k = 0, \ldots, n-1\}.$$

Vamos a calcular algunas representaciones complejas unitarias de dimensión 2 de D_n. Para ello, tomo $\alpha \in \mathbb{C}$ tal que $\alpha^n = 1$ y un espacio vectorial hermitiano V_α de dimensión 2 con base ortonormal $\{v_1, v_2\}$, para el que defino el homomorfismo de grupos[1] $D_n \to U(V)$ dado, en coordenadas con respecto de esa base, por

$$r \mapsto \begin{pmatrix} \alpha & 0 \\ 0 & \overline{\alpha} \end{pmatrix}, \qquad s \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Vamos a calcular las funciones matriciales correspondientes $\{t_{11}, t_{12}, t_{21}, t_{22}\}$. Para ello, consideremos que

$$s^a r^k \mapsto \begin{pmatrix} \alpha^k & 0 \\ 0 & \overline{\alpha}^k \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^a = \begin{cases} \begin{pmatrix} \alpha^k & 0 \\ 0 & \overline{\alpha}^k \end{pmatrix} & \text{si } a = 0 \\ \begin{pmatrix} 0 & \alpha^k \\ \overline{\alpha}^k & 0 \end{pmatrix} & \text{si } a = 1 \end{cases}$$

Analicemos ahora cuándo es V_α simple. Supongamos que no lo es: entonces existe $0 \neq v \in V_\alpha$ tal que $rv, sv \in \mathbb{C}v$. Si v tiene coordenadas (x, y), tenemos que

$$(x, y) \begin{pmatrix} \alpha & 0 \\ 0 & \overline{\alpha} \end{pmatrix} = \beta(x, y), \quad (x, y) \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \gamma(x, y),$$

[1] $U(V)$ denota el grupo unitario de V

para ciertos $\beta, \gamma \in \mathbb{C}$. Es fácil ver que esto implica que $\alpha^2 = 1$. Por tanto, para $\alpha^2 \neq 1$, obtenemos que el módulo V_α es simple.

Por otra parte, si V_α y $V_{\alpha'}$ son módulos isomorfos, entonces, tomando trazas, obtenemos que $\alpha+\overline{\alpha} = \alpha'+\overline{\alpha'}$. Así, obtenemos condiciones para obtener módulos simples no isomorfos.

Ahora consideremos $\omega = e^{i2\pi/n}$, que es una raíz n–ésima primitiva de la unidad, y tomemos $\Sigma_j = V_{\omega^j}$. La condición $(\omega^j)^2 = 1$ implica que $4\pi j/n$ ha de ser un múltiplo de 2π o, lo que es lo mismo, $2j$ un múltiplo de n. Vamos a discutir el caso en que n es impar. Escribimos entonces $n = 2\nu + 1$, lo que implica que, tomando $j = 1, \ldots, \nu$, según la discusión anterior, Σ_j es simple. Además, la igualdad $\omega^j + \omega^{-j} = \omega^{j'} + \omega^{-j'}$ implica que $\cos 2\pi j/n = \cos 2\pi j'/n$. Esto, para $1 \leq j, j' \leq \nu$ fuerza que $j = j'$. Así, obtenemos que Σ_j, $j = 1, \ldots, \nu$ son módulos simples no isomorfos entre sí.

Para estimar cuántos $\mathbb{C}D_n$–módulos simples faltan para completar la lista, observemos que $2n - 4\nu = 4\nu + 2 - 4\nu = 2$ que, para ser expresado como suma de cuadrados, sólo admite la forma $2 = 1 + 1$. Así que han de existir dos módulos simples de dimensión 1, que completarán, junto con $\Sigma_1, \ldots, \Sigma_\nu$ la "lista" de todos los módulos simples. Llamémoslos Σ_0, Σ_{-1}, donde Σ_0 es la representación trivial, que lleva todo elemento de D_n en $1 \in \mathbb{C}$, en tanto que Σ_{-1} lleva s en -1 y r en 1.

Hemos demostrado, pues, que

$$\Omega_{D_n} = \{\Sigma_{-1}, \Sigma_0, \Sigma_1, \ldots, \Sigma_\nu\}.$$

La base ortonormal de $\mathcal{M}(D_n)$ que obtenemos es

$$\{t^{\Sigma_{-1}}, t^{\Sigma_0}, \sqrt{2}t^{\Sigma_j}_{bc} : l = 1, \ldots, \nu, b, c = 1, 2\},$$

donde

$$t^{\Sigma_0}(s^a r^k) = 1, \qquad (a = 0, 1, k = 0, \cdots, n-1),$$

$$t^{\Sigma_{-1}}(s^a r^k) = \begin{cases} 1 & \text{si } a = 0, k = 0, \ldots, n-1 \\ -1 & \text{si } a = 1, k = 0, \ldots, n-1 \end{cases}$$

$$t^{\Sigma_j}_{11}(s^a r^k) = \begin{cases} e^{\mathbf{i}2\pi jk/n} & \text{si } a = 0, k = 0, \ldots, n-1 \\ 0 & \text{si } a = 1, k = 0, \ldots, n-1 \end{cases}$$

$$t^{\Sigma_j}_{12}(s^a r^k) = \begin{cases} 0 & \text{si } a = 0, k = 0, \ldots, n-1 \\ e^{\mathbf{i}2\pi jk/n} & \text{si } a = 1, k = 0, \ldots, n-1 \end{cases}$$

$$t^{\Sigma_j}_{21}(s^a r^k) = \begin{cases} 0 & \text{si } a = 0, k = 0, \ldots, n-1 \\ e^{-\mathbf{i}2\pi jk/n} & \text{si } a = 1, k = 0, \ldots, n-1 \end{cases}$$

$$t^{\Sigma_j}_{22}(s^a r^k) = \begin{cases} e^{-\mathbf{i}2\pi jk/n} & \text{si } a = 0, k = 0, \ldots, n-1 \\ 0 & \text{si } a = 1, k = 0, \ldots, n-1 \end{cases}$$

El caso n par admite una discusión similar.

4.6. Apéndice: S^1

.

Proposición 4.6.1. *Para cada función $f \in \mathcal{M}(G)$ consideremos $y \in G$, consideremos $y \cdot f \in \mathcal{M}(G)$ definida por $(y \cdot f)(x) = f(xy)$ para $x \in G$. Las siguientes condiciones son equivalentes sobre f:*

1. *f es una función representativa;*
2. *$\mathbb{C}G \cdot f$ es un espacio vectorial de dimensión finita.*

Demostración. $(1 \Rightarrow 2)$. Sea (Π, V) tal que f es una combinación lineal de funciones matriciales z_{ij} con respecto de Π y una base $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$. Podemos reducirnos al caso $f = z_{ij}$ para ciertos $i, j \in \{1, \ldots, n\}$. Para $x, y \in G$, tenemos

$$(y \cdot z_{ij})(x) = z_{ij}(xy) = \sum_k z_{ik}(x) z_{kj}(y).$$

De aquí,

$$y \cdot f = y \cdot z_{ij} = \sum_k z_{kj}(y) z_{ik}.$$

Por tanto, $\mathbb{C}G \cdot f$ es un espacio vectorial de dimensión finita por estar contenido en el subespacio de $\mathcal{M}(G)$ generado por $\{z_{ik} : k = 1, \ldots, n\}$.

$(2 \Rightarrow 1)$. Si $f \in \mathcal{M}(G)$ es una función tal que $\mathbb{C}G \cdot f$ es de dimensión finita, puesto que se trata de un subespacio invariante para la representación regular R', tenemos la restricción de esta última a $\mathbb{C}G \cdot f$ da una representación finito-dimensional de G. Obviamente, podemos suponer que $f \neq 0$ y, así, elegir una base $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ de $\mathbb{C}G \cdot f$ tal que $\mathbf{e}_1 = f$. Así, para $x \in G$,

$$x \cdot f = \sum_i z_{i1}(x) \mathbf{e}_i,$$

para ciertas funciones matriciales $\{z_{i1} : i = 1, \ldots, n\}$. Evaluando en el elemento neutro $e \in G$,

$$f(x) = (x \cdot f)(e) = \sum_i z_{i1}(x) \mathbf{e}_i(e).$$

Por tanto,

$$f = \sum_i \mathbf{e}_i(e) z_{i1}.$$

□

Ejemplo. Cualquier homomorfismo de grupos $\chi : G \to \mathbb{C}^\times$ es una función representativa, ya que $\mathbb{C}G\chi = \mathbb{C}\chi$.

Lema 4.6.2. *Si* G *es un grupo topológico, el conjunto* $\mathrm{Cont}(G,\mathbb{C})$ *de todas las funciones continuas es un* $\mathbb{C}G$*–submódulo de* $\mathcal{M}(G)$*.*

Demostración. Dada $f : G \to \mathbb{C}$ continua y $x \in G$, entonces la función xf es continua ya que

$$xf(y) = f(yx), \quad (y \in G),$$

y el producto en G es continuo. □

Proposición 4.6.3. *Si* G *es un grupo topológico, entonces el conjunto* $\mathcal{R}_c(G)$ *de todas las funciones representativas continuas es un* $\mathbb{C}G$*–submódulo de* $\mathcal{M}(G)$*.*

Ejemplo. Toda representación compleja continua del grupo aditivo $\mathbb{R}$ es, de acuerdo con el Lema de Schur, de dimensión 1. Esto es, se trata, salvo equivalencias, de un homomorfismo continuo de grupos $\chi : \mathbb{R} \to \mathbb{C}^\times$. Vamos a describir todos ellos.

Para ello, observemos primero que el conjunto de los números de la forma $n/2^m$, para $n \in \mathbb{Z}, m \in \mathbb{N}$ es denso en $\mathbb{R}$. Supuesto conocido que $\mathbb{Q}$ lo es, basta el siguiente argumento: dado $p/q \in \mathbb{Q}$ con $q > 0$ y $m \in \mathbb{N}$, existen $n \in \mathbb{Z}, r \in \mathbb{N}$ tales que

$$2^m p = nq + r, \qquad r < q.$$

Así,

$$\left|\frac{p}{q} - \frac{n}{2^m}\right| = \frac{r}{2^m q} < \frac{1}{2^m}.$$

En segundo lugar, dado un homomorfismo de grupos continuo $\chi : \mathbb{R} \to \mathbb{C}^\times$, tenemos que $\rho(t) = \chi(t)/|\chi(t)|$ es otro homomorfismo continuo de grupos. Existe $c > 0$ tal que, para todo $t \in [-c, c]$, el número complejo $\rho(t)$ pertenece al conjunto $\{e^{i\theta} : \theta \in (-\pi/2, \pi/2)\}$. Si escribo $\rho(c) = e^{i\theta_0}$, entonces $\rho(c) = \rho(c/2)^2$, de donde $\rho(c/2) = e^{i\theta_0/2}$. Reiterando el argumento, tenemos que $\rho(c/2^m) = e^{i\theta_0/2^m}$ para todo $m \in \mathbb{N}$. De aquí, $\rho(cn/2^m) = e^{i\theta_0 n/2^m}$ para todo $n \in \mathbb{Z}, m \in \mathbb{N}$. Por tanto, las funciones continuas $\rho(ct)$ y $e^{i\theta_0 t}$ coinciden en un subconjunto denso de $\mathbb{R}$, así que son iguales. Tomando $b = \theta_0/c$ obtenemos que $\rho(t) = e^{ibt}$ para todo $t \in \mathbb{R}$. Por otra parte, $r(t) = |\chi(t)|$ da una función continua de $\mathbb{R}$ en $\mathbb{R}$ tal que $r(t + t') = r(t)r(t')$ para todo $t, t' \in \mathbb{R}$. Se supone conocido que, en tal caso, $r(t) = e^{at}$, para cierto $a \in \mathbb{R}$.

En conclusión, $\chi(t) = e^{wt}$, para $w = a + bi \in \mathbb{C}$.

Vamos ahora a dar todas las representaciones continuas complejas irreducibles de $U(1) = S^1$. Para ello, observemos que tenemos un homomorfismo de grupos $p : \mathbb{R} \to U(1)$ dado por $p(t) = e^{it}$. Dada una representación continua $\chi : U(1) \to \mathbb{C}^\times$, tenemos, según la discusión anterior, que existe $w \in \mathbb{C}$ tal que $\chi p(t) = e^{wt}$. Esto es, $\chi(e^{it}) = e^{wt}$. En particular, $1 = \chi(1) = \chi(e^{i2\pi}) = e^{w2\pi}$. Si escribo $w = a + ib$, tengo la igualdad $1 = e^{a2\pi}e^{ib2\pi}$. De donde $a = 0, b \in \mathbb{Z}$. Por tanto,

$\chi(e^{it}) = e^{ibt}$, con $b \in \mathbb{Z}$. En resumen, las representaciones complejas continuas irreducibles de $U(1)$ son

$$\mathrm{Irr}(U(1)) = \{\chi_k : k \in \mathbb{Z}\},$$

donde $\chi_k(z) = z^k$ para $z \in U(1)$.

Bibliografía

[1] E. Abe, *Hopf Algebras*, Cambridge University Press, 1980.

[2] M. Braun, *Differential equations and their applications*, Springer, 1993.

[3] J. Gómez-Torrecillas, *Basic module theory over non-commutative rings with computa- tional aspects of operator algebras.* Lecture Notes in Comput. Sci. 8372, Algebraic and algorithmic aspects of differential and integral operators, 23–82, Springer, Heidelberg, 2014.

[4] J. Gómez-Torrecillas, *Álgebras, Grupos y Representaciones*, Universidad de Granada, 2020. http://hdl.handle.net/10481/62890

[5] N. Jacobson, *Algebra II*, W. H. Freeman & co, 1980.

[6] L. Rowen, *Algebra*, AK Peters, 1994.

[7] B. L. Van der Waerden, *Algebra 2*, Frederic Ungar Publishing Co., 1970.

[8] N. Zierler, *Linear Recurring Sequences*, Journal of the Society for Industrial and Applied Mathematics 7 (1959), pp. 31-48.