

---

# ÁLGEBRA MODERNA

JOSÉ ANTONIO DE LA ROSA CUBERO

# Índice

<b>1. Introducción</b>	<b>2</b>
1.1. Generalidades sobre anillos . . . . .	2
1.1.1. Interpolación . . . . .	5
1.1.2. Transformada discreta de Fourier . . . . .	6
<b>2. Introducción al concepto de módulo</b>	<b>7</b>
2.1. $K[x]$ -módulos con $K$ cuerpo . . . . .	10
2.2. Módulos abstractos . . . . .	11
2.2.1. Suma directa interna . . . . .	12
2.2.2. Módulos acotados sobre un DIP . . . . .	13
2.3. Homomorfismos de módulos . . . . .	14
2.3.1. Suma directa externa . . . . .	16
<b>3. Módulos noetherianos, artinianos y de longitud finita</b>	<b>17</b>
3.1. Módulos noetherianos . . . . .	17
3.2. Módulos artinianos . . . . .	21
3.3. Módulos de longitud finita . . . . .	22
3.3.1. Módulos de longitud finita sobre un DIP . . . . .	26
<b>4. Teoría de módulos</b>	<b>35</b>
4.1. Presentaciones de módulos . . . . .	39
4.2. Módulos semisimples . . . . .	51
4.2.1. Anillos semisimples . . . . .	56
4.3. Descomposición de anillos en ideales indescomponibles . . . . .	63
4.4. Módulos a derecha . . . . .	65
<b>5. Algunas aplicaciones</b>	<b>67</b>
5.1. $\mathbb{C}$ -álgebras de grupos finitos . . . . .	67

# 1. Introducción

## 1.1. Generalidades sobre anillos

**Definición 1** (Anillo). Sea  $A$  un conjunto en el que existen dos operaciones  $+, \cdot : A \times A \longrightarrow A$  tales que:

1.  $(A, +, 0)$  es un grupo aditivo (conmutativo):
  - $(a + b) + c = a + (b + c)$  para todos  $a, b, c \in A$ .
  - $a + b = b + a$  para todos  $a, b \in A$ .
  - $a + 0 = a$  para todo  $a \in A$ .
  - Para todo  $a \in A$  existe un  $-a \in A$  tal que  $-a + a = 0$ .
2.  $(A, \cdot, 1)$  es un monoide:
  - $(ab)c = a(bc)$  para todos  $a, b, c \in A$ .
  - $a \cdot 1 = 1 \cdot a = a$  para todo  $a \in A$ .
3. Se cumplen las siguientes propiedades distributivas:
  - $(a + b)c = ac + bc$  para todos  $a, b, c \in A$ .
  - $a(b + c) = ab + ac$  para todos  $a, b, c \in A$ .

**Definición 2** (Ideal). Sea  $A$  un anillo.  $I \subset A$  se dice ideal si cumple las siguientes propiedades:

- $I$  es un subgrupo aditivo de  $A$  (es decir,  $I$  es un conjunto no vacío que cumple  $b - a \in I$  para todo  $a, b \in I$ ).
- $ax, xa \in I$  para todo  $a \in I$  y  $x \in A$ .

**Teorema 1** (Teorema de Isomorfía). Sea  $f : A \longrightarrow B$  un homomorfismo de anillos. Entonces:

- $\ker f$  es un ideal de  $A$ ,
- $\text{Im } f$  es un subanillo de  $B$ ,
- Si  $I \subset \ker f$  es un ideal de  $A$ , entonces existe un único homomorfismo de anillos tal que  $\tilde{f} : A/I \longrightarrow B$  tal que  $\tilde{f}(a + I) = f(a)$ .
- El homomorfismo anterior es inyectivo si y solo si  $I = \ker f$ .
- El homomorfismo anterior es sobreyectivo si y solo si lo era  $f$ .

**Definición 3** (Homomorfismo de anillos).  $A, B$  anillos. Se dice que  $f : A \longrightarrow B$  se dice un (homo)morfismo de anillos si para todos  $a, a' \in A$  se tiene:

1.  $f(a + a') = f(a) + f(a')$
2.  $f(aa') = f(a)f(a')$
3.  $f(1) = 1$

**Definición 4** (Producto de ideales). Sean  $I, J$  ideales. Definimos su producto por:

$$IJ = \left\{ \sum_i x_i y_i : x_i \in I, y_i \in J \right\} \subseteq I \cap J$$

La suma de ideales es un ideal.

**Definición 5** (Ideales coprimos). Dos ideales  $I, J \subset A$  se dirán primos entre sí o coprimos si  $I + J = A$ .

Equivalentemente, existen  $x \in I, y \in J$  tales que  $1 = x + y$ .

La motivación de la definición anterior reside en la identidad de Bezout, que estamos generalizando.

**Lema 1.** Sean  $I, J, K$  ideales de  $A$ ,  $I + J = I + K = A$  si y solo si  $I + (J \cap K) = I + J \cap K = A$ .

*Es decir, son coprimos entre sí si y solo si uno es coprimo con la intersección de los otros dos.*

*Demostración.*

$$1 = x + y = x' + z$$

con  $x, x' \in I, y \in J, z \in K$ .

$$1 = x + y = x + y1 = x + y(x' + z) = x + yx' + yz$$

$x + yx' \in I$ , y  $yz \in J \cap K$ .

Para el recíproco,  $A \supseteq I + J \supseteq I + J \cap K = A$ , luego  $A = I + J$ . □

**Lema 2.** Sean  $I_1, \dots, I_t$  ideales de  $A$ .  $I_1 \cap I_i = A$  si y solo si  $I_1 + \bigcap_{i=2}^t I_i = A$ .

*Demostración.* Para  $t = 2$  es trivial.

Supongamos cierto  $I_1 \cap I_i = A \implies I_1 + \bigcap_{i=2}^t I_i = A$  para  $t$ , veamos para  $t + 1$ .

Llamo  $I = I_1, J = \bigcap_{i=2}^t I_i, K = I_{t+1}$ . Por hipótesis de inducción  $I + J = A$  y  $I + K = A$  por ser coprimos (hipótesis del lema). Por el lema anterior tenemos:

$$I + J \cap K = I_1 + I_{t+1} \cap \bigcap_{i=2}^t I_i = I_1 + \bigcap_{i=2}^{t+1} I_i$$

La otra implicación es muy sencilla. □

Hipótesis de trabajo para el teorema chino del resto:

1.  $A$  un anillo.
2.  $A_1, \dots, A_t$  anillos.
3.  $f_i : A \longrightarrow A_i$  un homomorfismo de anillos para cada  $i \in \{1, \dots, t\}$ .
4.  $\text{Im } f_i \subseteq A_i$  es un subanillo.
5. A  $\text{Im } f_1 \times \dots \times \text{Im } f_t$  se le llama el anillo producto.
6. Definimos  $f : A \longrightarrow \text{Im } f_1 \times \dots \times \text{Im } f_t$ ,  $f(x) = (f_1(x), \dots, f_t(x))$  para cada  $x \in A$ .
7. Tenemos que  $f$  es un homomorfismo de anillos, cuyo núcleo es la intersección de todos los núcleos. Llamaremos  $I = \ker f$ .  $x \in A$ ,  $x \in \ker f$  si y solo si  $f_i(x) = 0$  para todo  $i$ , es decir,  $x \in \bigcap_{i=1}^t \ker f_i$ .
8. Además, existe  $\tilde{f} : A/I \longrightarrow \text{Im } f_1 \times \dots \times \text{Im } f_t$ , con  $x + I \mapsto f(x)$ .
9. Cada  $\ker f_i$  es coprimo con cualquier  $\ker f_j$  para  $j \neq i$ .
10. Llamamos  $I_i = \ker f_i$ .

**Teorema 2** (Teorema Chino del Resto).  $\tilde{f}$  es isomorfismo si y solo si  $I_i + I_j = A$  para todo  $i \neq j$ .

*Demostración.* Veamos primero la implicación a la derecha.

Vamos a suponer  $\tilde{f}$  sobreyectiva, es decir, que  $f$  lo es. Veamos que todos los  $I_i$  son coprimos entre sí.

Dado  $i$  tomamos  $x \in A$  tal que  $f_i(x) = 1$  y  $f_j(x) = 0$  para todo  $j \neq i$ .

Observemos que  $x - 1 \in I_i$ ,  $x \in \bigcap_{j \neq i} I_j$

$$1 = 1 - x + x \in I_i + \bigcap_{j \neq i} I_j$$

Por tanto,  $I_i + \bigcap_{j \neq i} I_j = A$  y entonces por el lema anterior  $I_i + I_j = A$ .

Veamos el recíproco. Suponemos que  $I_i + I_j = A$  para cualquier  $i \neq j$ .

Tomamos  $(f(b_1), \dots, f(b_t)) \in I_1 \times \dots \times I_t$ .

Para cada  $i$ , tomamos  $1 = a_i + p_i$  con  $a_i \in I_i$  y  $p_i \in \bigcap_{j \neq i} I_j$ .

Tomamos  $x = \sum_{i=1}^t b_i p_i$ .

$$f_j(x) = \sum_{k=1}^t f_j(b_k) f_j(p_k) = f_j(b_j) f_j(p_j) = f_j(b_j(1 - a_j)) = f_j(b_j) - f_j(b_j) f_j(a_j) = f_j(b_j)$$

porque  $f_j(p_k) = 0$  si  $k \neq j$  y  $a_j \in \ker f_j$ .

□

*Observación 1.* Para anillos conmutativos denotamos

$$\langle a \rangle = \{ba : b \in A\}$$

el ideal generado por  $a$ .

Vamos a hacer un ejemplo, aplicando el teorema anterior.

### 1.1.1. Interpolación

Tomamos  $A = K[x]$ , un anillo de polinomios con coeficientes en un cuerpo  $K$ .

Sea  $A_i = K$  con  $i \in \{1, \dots, t\}$ . Tomamos  $\alpha_i \in K$  para cada  $i$  y definimos  $\xi_i : K[x] \rightarrow K$ ,  $\xi_i(g) = g(\alpha_i)$ , para cada  $g \in K[x]$  y es un homeomorfismo de anillos.

$\text{Im } X_i = K$  y  $\xi : K[x] \rightarrow K \times \dots \times K = K^t$ .

$\ker \xi_i = \langle x - \alpha_i \rangle$  que es ideal de un anillo de polinomios, luego principal. Está generado por el polinomio de grado menor, como las constantes no pueden anular a  $\xi_i$ , tiene que estar generado por ese, que es de grado uno.

$$I = \bigcap_{i=1}^t \langle x - \alpha_i \rangle = \langle p(x) \rangle$$

donde  $p(x) = \text{mcm}\{x - \alpha_i : i \in \{1, \dots, t\}\}$ .

El teorema chino del resto nos asegura que  $\tilde{\xi} : K[x]/\langle p(x) \rangle \rightarrow K^t$  es un isomorfismo si y solo si  $\text{mcd}\{x - \alpha_i, x - \alpha_j\}$  para todo  $j \neq i$ , es decir, si  $\alpha_i \neq \alpha_j$ .

Lo que estamos viendo es que para cualquier tupla  $(y_1, \dots, y_t) \in K^t$ , existe un  $g \in K[x]$  tal que  $g(\alpha_i) = y_i$ , si y solo si  $\alpha_i \neq \alpha_j$ . En tal caso,  $p(x) = \prod_{i=1}^t (x - \alpha_i)$ .

Existe un único representante  $g \in K[x]$  tal que  $g(\alpha_i) = y_i$  de grado menor que  $t$ , siempre que  $p(x) = \prod_{i=1}^t (x - \alpha_i)$ .

$\alpha_1, \dots, \alpha_t \in K$  distintos dos a dos

$$\tilde{\xi} : K[x]/\langle p(x) \rangle \rightarrow K^t$$

es un isomorfismo de anillos.

$K[x]/\langle p(x) \rangle$  es un espacio vectorial cociente.

$\tilde{\xi}$  es también un isomorfismo entre espacios vectoriales.

$$\tilde{\xi}(\alpha(g + p)) = \tilde{\xi}(\alpha g + p) = \tilde{\xi}((\alpha + p)(g + p)) =$$

$$\tilde{\xi}(\alpha + p)\tilde{\xi}(g + p) = (\alpha, \dots, \alpha)(g(\alpha_1), \dots, g(\alpha_t)) = \alpha\tilde{\xi}(g + p)$$

Sea  $\{1 + p, x + p, x^2 + p, \dots, x^{t-1} + p\}$   $K$ -base de  $K[x]/\langle p(x) \rangle$ . Notamos:

$$1 = 1 + p$$

$$x = x + p$$

Sea  $\{e_1, \dots, e_n\}$  es la base canónica de  $K^t$ . Nuestro objetivo es calcular sus preimágenes por  $\xi$ , en concreto un polinomio de grado menor que  $t$ .

$$g_i(x) = \prod_{j \neq i} (x - \alpha_j)$$

$$L_i(x) = \frac{g_i(x)}{g(\alpha_i)} = \prod_{j \neq i} \frac{x - x_j}{x_i - x_j}$$

que vale 0 en  $\alpha_j$  para cualquier  $j$  salvo en  $\alpha_i$  que vale 1.

Tenemos que

$$g(x) = \sum_{i=1}^t y_i L_i(x)$$

satisface que  $g(\alpha_i) = y_i$ .

Finalmente vamos a ver que la matriz de  $\tilde{\xi}$  en las bases consideradas es:

$$\begin{pmatrix} 1 & \dots & 1 \\ \alpha_1 & \dots & \alpha_t \\ \dots & \dots & \dots \\ \alpha_1^t & \dots & \alpha_t^t \end{pmatrix}$$

### 1.1.2. Transformada discreta de Fourier

Ahora vamos a reindexar. En lugar de usar  $1, \dots, t$  vamos a tomar los índices  $1, \dots, n-1$ .

Vamos a suponer que el cuerpo  $K$  contiene una raíz primitiva de 1, o sea, existe un  $\omega \in K$  tal que  $\omega^n = 1$  y  $1, \omega, \omega^2, \dots, \omega^{n-1}$  son distintos.

Seguro que  $\text{car } K \nmid n$  ya que  $1, \omega, \omega^2, \dots, \omega^{n-1}$  son las raíces de  $x^n - 1$  y son distintas.

Vamos a interpolar las raíces de la unidad.

Tomo  $\alpha_j = \omega^j$ ,  $j \in \{0, \dots, n\}$  y

$$M = A_\omega = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \omega^0 & \omega^1 & \dots & \omega^{n-1} \\ (\omega^0)^2 & (\omega^1)^2 & \dots & (\omega^{n-1})^2 \\ \dots & \dots & \dots & \dots \end{pmatrix} = (\omega^{ij})$$

Tenemos que  $x^n - 1 = (x - 1)(x^{n-1} + \dots + x + 1)$  y evaluando en  $\omega^j$  obtenemos

$$\omega^{(n-1)j} + \dots + \omega^j + 1 = 0$$

Entonces  $\sum_{k=0}^{n-1} \omega^{ik} = 0$  para  $0 < i < n$ .

$$\begin{pmatrix} \omega^i & \omega^{2i} & \dots & \omega^{(n-1)i} \end{pmatrix} \begin{pmatrix} \omega^{-j} \\ \omega^{-2j} \\ \dots \\ \omega^{-(n-1)j} \end{pmatrix} = \sum_{k=0}^{n-1} \omega^{k(i-j)} = 0$$

Tenemos entonces que  $A_\omega A_{\omega^{-1}}^T = nI$ , es decir,  $A_\omega^{-1} = \frac{1}{n} A_{\omega^{-1}}^T$ .

$\tilde{\xi} : K[x]/\langle x^n - 1 \rangle \longrightarrow K^n$ , con  $\xi^{-1}(y)$  es el polinomio interpolador.

Tenemos unos datos  $(y_0, \dots, y_{n-1}) \in K^n$ . El polinomio interpolador de esos datos en los nodos  $1, \omega, \dots, \omega^{n-1}$  viene dado por

$$\hat{y} = \sum_{j=0}^{n-1} \hat{y}_j x^j$$

donde  $\hat{y} = y_n^{\frac{1}{n}} A_{\omega^{-1}}^T$ .

Explicitamente, se calcula que los coeficientes quedan:

$$y_j = \frac{1}{n} \sum_{k=0}^{n-1} y_k \omega^{-jk}$$

Tomamos  $K = \mathbb{C}$ .  $\omega = e^{i2\pi/n}$ :

$$y_j = \frac{1}{n} \sum_{k=0}^{n-1} y_k \omega^{-i2\pi jk/n}$$

que es la transformada de Fourier de  $y$ .

¿Qué interpretación le damos? Supongamos una función periódica de periodo  $2\pi$ ,  $f : [0, 2\pi] \longrightarrow \mathbb{C}$  con  $f(0) = f(2\pi)$ . Dividimos el intervalo en  $n$  partes iguales, una muestra:  $y_j = f(\frac{2\pi j}{n})$  con  $j = 0, \dots, n-1$ .

Tomamos  $g : [0, 2\pi] \longrightarrow \mathbb{C}$  con  $g(t) = \sum_{j=0}^{n-1} \hat{y}_j e^{ijt}$ .

Tenemos entonces que  $g(\frac{2\pi l}{n}) = \sum_{j=0}^{n-1} \hat{y}_j e^{i2\pi lj/n} = y_l = f(\frac{2\pi j}{n})$

A los  $\hat{y}$  también se le llama el espectro de  $y$ .

## 2. Introducción al concepto de módulo

**Definición 6.** Sean  $M, N$  grupos aditivos:

$$\text{Ad}(M, N) = \{f : M \longrightarrow N \mid f \text{ homomorfismo de grupos}\}$$



El conjunto anterior es no vacío porque  $0 \in \text{Ad}(M, N)$ .  $\text{Ad}(M, N)$  es un grupo aditivo con la suma:

$$(f + g)(m) := f(m) + g(m) \quad \forall m \in M$$

**Definición 7** (Anillo de endomorfismo de  $M$ ). Definimos directamente  $\text{End}(M) := \text{Ad}(M, M)$ .

**Proposición 1.**  $(\text{End}(M), +, 0, \circ, \text{id})$  es un anillo.

*Demostración.* Se comprueba que es cerrado para composición. Es obvio que la composición es asociativa y tiene como elemento neutro la identidad.

Finalmente se ve que se cumplen las propiedades distributivas, que se siguen de que son homomorfismos.  $\square$

*Observación 2.* Consideramos el grupo  $\{0\}$ , es el anillo  $\{0\}$  (anillo cero o trivial).

Si  $M \neq \{0\}$ , entonces  $\text{End}(M)$  no es trivial.

**Definición 8** (Módulo). Sea  $M$  un grupo aditivo y  $A$  un anillo. Una estructura de  $A$ -módulo sobre  $M$  es un homomorfismo de anillos  $\rho : A \rightarrow \text{End}(M)$ .

Ejemplo: los números enteros.  $M$  grupo aditivo,  $A = \mathbb{Z}$ . Existe un único  $\chi : \mathbb{Z} \rightarrow \text{End}(M)$  determinado por  $\chi(1) = \text{id}_M$ , es decir, una única estructura de  $\mathbb{Z}$ -módulo sobre  $M$  (y su núcleo te da la característica del anillo).

Ejemplo: cuerpos. Sea  $K$  un cuerpo. Si  $V$  es un  $K$ -espacio vectorial, definimos  $\rho : K \rightarrow \text{End}(V)$ , tomamos  $\rho(\alpha) : V \rightarrow V$  cumpliendo  $\rho(\alpha)(v) = \alpha v$ . Trivialmente se cumple que  $\rho$  es un homomorfismo por la estructura de espacio vectorial de  $V$ . Con lo cual tenemos una estructura de  $K$ -módulo sobre  $V$ . Se puede demostrar el recíproco trivialmente.

*Observación 3.* Sean  $X, Y, Z$  conjuntos.  $\text{Map}(X, Y)$  es el conjunto de aplicaciones de  $X$  en  $Y$ .

Entonces:

$$\psi : \text{Map}(X \times Y, Z) \rightarrow \text{Map}(X, \text{Map}(Y, Z))$$

es una biyección dada por  $\psi(f)(x)(y) := f(x, y)$  y  $\psi^{-1}(g)(x, y) := g(x)(y)$ .

Ejercicio: comprobar que  $\psi^{-1}$  es realmente la inversa de  $\psi$ .

*Observación 4.* Sean  $M, N, L$  grupos aditivos.

$$\psi : \text{Biad}(M \times N, L) \rightarrow \text{Ad}(M, \text{Ad}(N, L))$$

donde  $b \in \text{Biad}(M \times N, L)$  si  $b$  es biaditiva:

$$b(m + m', n) = b(m, n) + b(m', n)$$

$$b(m, n + n') = b(m, n) + b(m, n')$$

Ejercicio, demostrar que la aplicación  $\psi$  es una biyección.

**Teorema 3** (Caracterización de módulos). *Sea  $A$  anillo,  $M$  un grupo aditivo. Sea  $\text{Ring}(A, \text{End}(M))$ , llamamos  $A$ -módulo a la imagen por  $\psi$  de ese conjunto.*

**Definición 9.**

$$\text{Ring}(R, S) = \{\phi : R \longrightarrow S, \phi \text{ es homomorfismo de anillos}\}$$

**Proposición 2.** *Dados un grupo aditivo  $M$  y un anillo  $A$ , se tiene una correspondencia biyectiva entre:*

1. *Homomorfismos de anillos  $\rho : A \longrightarrow \text{End}(M)$*
2. *Las aplicaciones  $A \times M \longrightarrow M$  que satisfacen:*

- $(a + a')m = am + a'm$
- $a(m + m') = am + am'$
- $(aa')m = a(a'm)$
- $1 \cdot m = m$

*Demostración.* Tomamos la biyección  $\psi^{-1} : \text{Map}(A, \text{Map}(M, M)) \longrightarrow \text{Map}(A \times M, M)$ . Tomamos  $\rho \in \text{Ring}(A, \text{End}(M))$ , su imagen por la biyección,  $\psi^{-1}(\rho)$  son las aplicaciones que satisfacen justo las propiedades anteriores.

Llamamos a  $\psi^{-1}(\rho)(a, m) = a \cdot m$ . Tenemos que  $\psi^{-1}(\rho)(a, m) = \rho(a)(m)$ . Entonces  $a \cdot m = \rho(a)(m)$ .

Comprobamos la tercera propiedad como ejemplo:

Dados  $a, a' \in A$  y  $m \in M$ :

$$(aa')m = \rho(aa')(m) = (\rho(a) \circ \rho(a'))(m) = \rho(a)(\rho(a')(m)) = \rho(a)(a'm) = a(a'm)$$

De forma análoga se demuestran el resto de propiedades.

Esta correspondencia responde a la fórmula  $am = \rho(a)(m)$ . □

Un  $A$ -módulo lo veré de cualquiera de las maneras anteriores, que ya hemos visto que son equivalentes, según su conveniencia.

Ejemplo, si  $K$  es un cuerpo, un  $K$ -módulo es esencialmente un  $K$  espacio vectorial.

Otro ejemplo, el  $A$ -módulo regular.  $A$  es un  $A$ -módulo, vía  $\lambda : A \longrightarrow (A)$  que lleva cada  $a$  a  $\lambda(a)(a') := aa'$ . La demostración es sencilla usando la segunda definición.

**Proposición 3** (Restricción de escalares). Sea  $\phi : R \longrightarrow S$  homomorfismo de anillos. Si  $M$  es un  $S$ -módulo, vía un homomorfismo de anillos  $\rho : S \longrightarrow \text{End}(M)$ , tenemos que  $M$  es un  $R$ -módulo vía  $\rho \circ \phi$ .

Equivalentemente, si  $r \in R$  y  $m \in M$ , definimos

$$rm = (\rho \circ \phi)(r)(m) = \rho(\phi(r))(m) = \phi(r)m$$

## 2.1. $K[x]$ -módulos con $K$ cuerpo

Tenemos  $K[x]$ -módulo  $M$ . O sea,  $M$  es un grupo aditivo y  $\rho : K[x] \longrightarrow \text{End}(M)$  es un homomorfismo de anillos.

$K$  se puede ver como subanillo de  $K[x]$ , aplicando la restricción de escalares aplicada a la aplicación inclusión,  $M$  es un  $K$ -espacio vectorial.

Veamos que ocurre con la indeterminada.  $\rho(x) \in \text{End}(M)$ .

Veamos que es un endomorfismo de espacios vectoriales:

$$\rho(x)(km) = x \cdot (km) = x \cdot (k \cdot m) = (xk) \cdot m = kx \cdot m = k(xm) = k\rho(x)(m)$$

Así que  $\rho(x)$  es  $K$ -lineal.

Si  $p = \sum_i p_i x^i \in K[x]$ , tenemos que

$$pm = \rho(p)(m) = \sum_i p_i \rho(x)^i(m)$$

**Proposición 4.** Si tengo un  $K$ -espacio vectorial  $V$  y una aplicación lineal  $T : V \longrightarrow V$ , podemos definir para  $p \in K[x]$  y  $v \in V$  el operador

$$pv := p(T)(v) = \sum_i p_i T^i(v)$$

resulta que  $V$  es un  $K[x]$ -módulo.

Ejemplo,  $\mathcal{C}^\infty(\mathbb{R})$  con  $T = \frac{d}{dt}$  es un  $\mathbb{R}[x]$ -módulo.

*Observación 5.*  $\mathcal{C}^\infty(\mathbb{R})$  dotado de estructura de  $\mathbb{R}[x]$ -módulo a través del endomorfismo lineal  $T = \frac{d}{dt}$  es un ejemplo ilustrativo en el siguiente sentido.

Tomemos sin,  $x \sin t = T(\sin t) = \cos t$   $x^2 \sin t = -\sin t$  con lo que

$$(x^2 + 1) \sin t = 0$$

es decir, en un  $A$ -módulo  $M$  puede pasar que  $am = 0$   $a \neq 0$ ,  $m \neq 0$ .

Ejemplo en el  $\mathbb{Z}$ -módulo  $\mathbb{Z}_4$  tenemos que  $2 \cdot \bar{2} = \bar{0}$ .

## 2.2. Módulos abstractos

Sea  $A$  un anillo,  ${}_A M$  un  $A$ -módulo, entonces si tenemos un homomorfismo de anillos  $\varphi : A \longrightarrow \text{End}(M)$  cuyo núcleo es un ideal de  $A$ .

Aplicando el primer teorema de isomorfía, tenemos:

$$A/\ker \varphi \longrightarrow \text{Im } \varphi \subseteq \text{End}(M)$$

y entonces  $M$  es un  $A/\ker \varphi$ -módulo. De hecho  $(a + \ker \varphi)m = \varphi(m)$ .

$$\ker \varphi = \{a \in A : am = 0\} = \text{Ann}_A(M)$$

se le llama el anulador de  $M$ .

Tenemos que  ${}_A M$  entonces  $M_{A/\text{Ann}_A(M)}$

Ejercicio: si tenemos una aplicación lineal entre espacios vectoriales de dimensión finita, entonces el anulador está generado por un único polinomio, el polinomio mínimo de  $T$ .

**Definición 10.** Un submódulo de un módulo  ${}_A M$  es un subgrupo aditivo  $N \subseteq M$  tal que  $am \in N$  para cualquier  $a \in A$  y  $m \in N$ . Los submódulos del módulo regular  $A$  se llaman ideales por la izquierda de  $A$ .

*Observación 6.* Todo ideal es un ideal a izquierda. Si  $A$  es conmutativo, los ideales a izquierda coinciden con los ideales.

Ejemplo: tomando  $A = \mathcal{M}_2(K)$  con  $K$  un cuerpo.

$$\mathcal{M}_2(K) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in K \right\}$$

Tenemos que el conjunto:

$$\left\{ \begin{pmatrix} 0 & b \\ 0 & d \end{pmatrix} : b, d \in K \right\}$$

es un ideal a izquierda de  $A$ .

Ejemplo:  $T : V \longrightarrow V$ ,  $K$ -lineal. ¿Qué es un  $K[x]$ -submódulo de  $V_{K[x]}$ ? Sea  $W$  un tal submódulo.  $W$  es un subespacio vectorial y además  $T(w) = xw \in W$ , es decir, un subespacio  $T$ -invariante (un ejemplo de subespacio  $T$  invariante es un subespacio propio). El recíproco es también cierto.

**Definición 11** (Submódulo cíclico). Dado  ${}_A M$ , y un  $m \in M$ . Es claro que  $Am = \{am : a \in A\}$  es un submódulo de  ${}_A M$  que se llama submódulo cíclico generado por  $m$ .

Ejemplo:  $\mathbb{R}[x] \sin t = \mathbb{R} \sin t + \mathbb{R} \cos t$ .

**Definición 12** (Submódulo finitamente generado). Dados  $m_1, \dots, m_n \in M$ , el conjunto

$$Am_1 + \dots + Am_n = \{a_1m_1 + \dots + a_nm_n : a_i \in A\}$$

es un submódulo de  ${}_A M$  llamado el submódulo generado por  $m_1, \dots, m_n$ . Si  $M = Am_1 + \dots + Am_n$ , diremos que  $M$  es finitamente generado con generadores  $m_1, \dots, m_n$ .

### 2.2.1. Suma directa interna

**Definición 13** (Módulo suma). Dados  $N_1, \dots, N_n$  submódulos de  ${}_A M$ , definio:

$$N_1 + \dots + N_n = \{m_1 + \dots + m_n : m_i \in N_i\}$$

es un submódulo de  $M$  que se llama suma de  $N_1 + \dots + N_n$ .

**Notación.** Se puede expresar  $N_1 + \dots + N_n$  como  $\sum_{i=1}^n N_i$ .

**Proposición 5.** Sean  $N_1, \dots, N_t$  submódulos de  $A$ . Son equivalentes:

1.  $N_i \cap \sum_{j \neq i} N_j = \{0\}$  para todo  $i$ .
2. Si  $0 = n_1 + \dots + n_t$ ,  $n_i \in N_i$  entonces  $n_i = 0$  para todo  $i$ .
3. Cada  $n \in N_1 + \dots + N_t$  admite una representación única como  $n = n_1 + \dots + n_t$  con  $n_i \in N_i$ .

*Demostración.* Veamos que 1 implica 2. Tenemos que  $0 = n_1 + \dots + n_t$ , si despejamos,  $n_i = -\sum_{j \neq i} n_j \in N_i \cap \left(\sum_{j \neq i} N_j\right) = \{0\}$ .

Veamos que 2 implica 3. Si  $n = \sum n_i = \sum n'_i$ , entonces  $0 = \sum (n_i - n'_i)$  lo que implica que  $n_i = n'_i$ .

Finalmente, tomando  $n \in N_i \cap \left(\sum_{j \neq i} N_j\right)$ , es decir,  $n = \sum_{j \neq i} n_j$  con lo que  $0 = n - \sum_{j \neq i} n_j$  y como las descomposiciones son únicas,  $n = 0$ .  $\square$

**Definición 14** (Suma interna). Si  $M = N_1 + \dots + N_t$  tales que satisfacen una de las condiciones equivalentes anteriores, diremos que  $M$  es la suma directa interna y usaremos la notación  $M = N_1 \dot{+} \dots \dot{+} N_t$ .

**Definición 15.** Si  $\{N_1, \dots, N_t\}$  verifican las condiciones equivalentes anteriores y  $N_i \neq \{0\}$ , se dice que el conjunto  $\{N_1, \dots, N_t\}$  es una familia independiente.

Ejemplo:  $\mathbb{Z}_6$  es un  $\mathbb{Z}$  módulo.

$$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5, 6\}$$

Tomamos

$$N_1 = \{0, 3\}$$

y

$$N_2 = \{0, 2, 4\}$$

Tenemos que  $N_1, N_2$  es una familia independiente. Además es obvio que:

$$N_1 \dot{+} N_2 = \mathbb{Z}_6$$

ya que tienen como intersección  $\{0\}$  y su suma es el total.

### 2.2.2. Módulos acotados sobre un DIP

**Definición 16** (Módulo acotado sobre un DIP). Sea  $A$  un dominio de ideales principales,  ${}_A M$  un módulo,  $\text{Ann}_A(M) = \langle \mu \rangle$  para cierto  $\mu \in A$ .

Si  $\mu \neq 0$ , diré que  $M$  es acotado.

Supongamos que  ${}_A M$  es acotado y  $\mu \notin \mathcal{U}(A)$ , ya que si  $\mu \in (A)$  entonces  $M = \{0\}$ .

Si  $\mu = p_1^{e_1} \cdots p_t^{e_t}$ , posible porque todo DIP es un dominio de factorización única (DFU), con  $p_i \in A$  irreducible y  $e_i > 0$ .

**Proposición 6** (Descomposición primaria del módulo). *Tomamos  $q_i = \frac{\mu}{p_i^{e_i}} \in A$ .*

*Llamamos  $M_i = \{q_i m : m \in M\} \subseteq M$ . Veamos que  $M_i \in \mathcal{L}({}_A M) = \{\text{submódulos de } {}_A M\}$ .*

*Queremos que  $M = M_1 \dot{+} \cdots \dot{+} M_t$ , con  $t > 1$  para evitar trivialidades. En ese caso,  $\text{mcd}\{q_1, \dots, q_t\} = 1$ , donde se ha usado que estamos en un DFU.*

*Por la identidad de Bezout (válida porque estamos en un DIP), tenemos que  $1 = \sum_{i=1}^t q_i a_i$ , para ciertos  $q_i \in A$ . Para en  $m \in M$ ,  $M = 1 \cdot m = \sum_i q_i a_i m$ , luego  $M = M_1 + \cdots + M_t$ .*

*Vamos a ver que la suma es directa.  $q_i q_j \in \langle \mu \rangle$  si  $i \neq j$ . Eso significa que si  $m \in M_i$  y entonces  $q_j m = 0$  si  $i \neq j$ . Por tanto  $M_i = \{m \in M : m = q_i a_i m\}$ .*

*Si  $0 = \sum_{i=1}^t m_i$  con  $m_i \in M_i$ , entonces*

$$0 = q_j a_j 0 = m_j$$

*y por tanto  $M = M_1 \dot{+} \cdots \dot{+} M_t$ .*

**Definición 17** (Componentes primarias). Tenemos que los  $M_i$  se llaman componentes primarias.

**Proposición 7.**

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

$$\text{Así, } \langle \mu \rangle = \text{Ann}_A(M) = \bigcap_{i=1}^t \text{Ann}_A(M_i) \supseteq \bigcap_{i=1}^t \langle p_i^{e_i} \rangle = \langle \mu \rangle$$

Ejercicio: Obtener la descomposición primaria usando  $\dot{+}$  de  $\mathbb{Z}_{8000}$ . Ejemplo:  $T$  endomorfismo  $K$ -lineal.  $V = {}_{K[x]}V$ .

Un  $W$  es un submódulo de  $V$  es un subespacio vectorial tal que  $T(W) \subseteq W$ , es decir,  $W$  es  $T$  invariante.

Si  $\text{Ann}_{K[x]}(V) \neq \{0\}$ , tomo  $\mu(x) \in K[x]$ , el polinomio mínimo de  $T$ . Es decir,  $\text{Ann}_{K[x]}(V) = \langle \mu(x) \rangle$ .

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

Entonces la descomposición primaria de  $V$  es  $V = V_1 \dot{+} \cdots \dot{+} V_t$  con

$$V_i = \{v \in V : p_i(x)v = 0\}$$

Caso particular:  $\dim(V) < \infty$  y que  $\mu(x) = (x - \alpha_1) \cdots (x - \alpha_t)$  con  $\alpha_i \neq \alpha_j$ .

$$V_i = \{v \in V : (x - \alpha_i)v = 0\} = \{v \in V : T(v) = \alpha_i v\}$$

es decir, el subespacio propio asociado al valor propio  $\alpha_i$ .

Si el polinomio factoriza como producto de polinomios de grado 1 distintos,  $T$  es diagonalizable. Veremos en el futuro que el polinomio mínimo divide siempre al polinomio característico.

¿Cómo se calcula el polinomio mínimo de un endomorfismo lineal?

Ejercicio: Sea  $V$  un espacio vectorial real euclídeo (con producto escalar). Sea  $T : V \rightarrow V$  una isometría. Se pide demostrar que si  $W$  es un subespacio  $T$  invariante de  $V$ , entonces su ortogonal  $W^\perp$  es también  $T$  invariante. Entonces  $V = W \dot{+} W^\perp$ . Se usa inducción. Como consecuencia, usando el teorema fundamental del álgebra, deducir que  $V$  admite una base ortonormal con respecto de la cual la matriz de  $T$  es diagonal por bloques, con bloques de dimensión 1 o 2. ¿Qué aspecto tienen dichos bloques? Hay que ver que uno de los dos subespacios invariantes tienen dimensión 1 o 2.

## 2.3. Homomorfismos de módulos

**Definición 18** (Módulo cociente o factor). Sea  ${}_A M$  y  $L \in \mathcal{L}(M)$ . Consideramos  $M/L$  grupo aditivo y se define la acción:

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

$M/L$  es un módulo.

**Definición 19** (Homomorfismo de módulos). Se dice que  $f : {}_A M \longrightarrow {}_A N$  es un homomorfismo de módulos si respeta sumas y productos.

**Definición 20** (Proyección canónica). Es la aplicación  $\pi : M \longrightarrow M/L$  dada por  $\pi(m) = m + L$  es un homomorfismo de módulos.

**Teorema 4** (Teorema de isomorfía para módulos).  $f : M \longrightarrow N$  un homomorfismo de  $A$ -módulos. Entonces el núcleo  $\ker f \in \mathcal{L}({}_A M)$  y  $\operatorname{Im} f \in \mathcal{L}(N)$ . Para cada  $L \in \mathcal{L}({}_A M)$  tal que  $L \subseteq \ker f$  existe un único homomorfismo de módulos  $\tilde{f} : M/L \longrightarrow N$  tal que  $\tilde{f} \circ \pi = f$ . Finalmente,  $\tilde{f}$  es inyectiva si y solo si  $L = \ker f$ , en cuyo caso,  $\tilde{f}$  da un isomorfismo de  $A$ -módulos  $M/\ker f \cong \operatorname{Im} f$ .

Ejemplo  ${}_A M$ , definimos  $f : A \longrightarrow M$  dada por:

$$f(a) = am \quad \forall a \in A$$

es un homomorfismo de  $A$ -módulos.

Tenemos  $\operatorname{Im} f = Am$  y  $\operatorname{ann}(a) = \ker f = \{a \in A : am = 0\}$  es un ideal izquierda y se tiene

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

$$a + \operatorname{ann}_A(m) \mapsto am$$

Ejemplo:  $S = \operatorname{Map}(\mathbb{N}, K)$ , el conjunto de las sucesiones (que forman un  $K$ -espacio vectorial). Tomamos  $T : S \longrightarrow S$  tal que  $T(s)(n) = s(n+1)$ . Es lineal. Entonces  ${}_{K[x]} S$ , donde  $xs = T(s)$ .

Para cualquier  $f \in K[x]$ , es decir  $f = \sum_i f_i x^i$ , se tiene:

$$(fs)(n) = \sum_i f_i s(n+i)$$

Imaginémonos que  $s$  verifica que  $\operatorname{ann}_{K[x]}(s) \neq \langle 0 \rangle$ . Podemos tomar entonces un polinomio tal que  $fs = 0$  y que sea mónico. Tenemos entonces que  $s(n+m) = -\sum_{i=0}^{m-1} f_i s(n+i)$  para todo  $n \in \mathbb{N}$ . Es decir, la sucesión es linealmente recursiva.

Caso particular,  $s(0) = s(1) = 1$ , tenemos que

$$s(n+2) = s(n) + s(n+1)$$

$$x^2 - x - 1 \in \operatorname{ann}_{K[x]}(s)$$



Volviendo al caso general, tenemos que

$$K[x]/\text{ann}_{K[x]}(s) \cong K[x]s$$

Tenemos que  $\dim_K(K[x]s) < \infty$  si y solo si  $\text{ann}_{K[x]}(s) \neq \langle 0 \rangle$  si y solo si  $s$  es una sucesión linealmente recursiva.

El generador  $p(x)$  de  $\text{ann}_{K[x]}(s)$  se le llama el polinomio mínimo de  $s$ . El grado de dicho polinomio, coincide con  $\dim_K(K[x]s)$  y se le llama complejidad lineal de  $s$ .

$s, t$  dos sucesiones linealmente recursivas.  $K[x](s+t) \subseteq K[x]s + K[x]t$ , luego la primera tiene dimensión finita. Luego  $s+t$  es una sucesión linealmente recursiva, de complejidad menor o igual a la suma de las complejidades lineales. Puede argumentarse lo mismo para combinaciones lineales.

Las sucesiones linealmente recursivas forman un subespacio vectorial del espacio de sucesiones. De hecho forman un submódulo. Sea  $S^l$  el conjunto de las sucesiones linealmente recursivas, forma un  $S^l$  es un  $K[x]$ -submódulo de  $S$ , ya que es invariante por la acción de  $x$  (es  $T$ -invariante).

Otro ejemplo:  $T$  endomorfismo de  $\mathcal{C}^\infty(\mathbb{R})$  tal que  $T(\varphi) = \varphi'$ . Tenemos que  ${}_{R[x]}\mathcal{C}^\infty(\mathbb{R})$ . Dada  $\varphi$ , tenemos que

$$\text{ann}_{\mathbb{R}[x]}(\varphi) = \{f \in \mathbb{R}[x] : f(x)\varphi = 0\} = \{f = \sum_i f_i \frac{d^i}{dt^i} : f\varphi = 0\}$$

$\text{ann}(\varphi) \neq \langle 0 \rangle$  si  $\varphi$  satisface una ecuación diferencial lineal homogénea con coeficientes constantes. Bla bla.

$\mathbb{R}[x]/\text{ann}_{\mathbb{R}[x]}(\varphi) \cong \mathbb{R}[x]\varphi$ , donde  $\varphi$  satisface bla bla.

Tenemos que  $\varphi'' - \varphi' - \varphi = 0$ , cuya solución  $\varphi(t) = e^{\phi t}$ , donde  $\phi$  es la razón áurea.

### 2.3.1. Suma directa externa

**Definición 21.** Tomando el producto cartesiano de  $t$  módulos sobre el mismo anillo y tomando la suma usual de tuplas y definiendo el siguiente producto:

$$a(m_1, \dots, m_t) = (am_1, \dots, am_t)$$

Es un módulo que se llama suma directa externa de  $M_1, \dots, M_t$  con  $M^t$  si son todos iguales.

Se denota  $M_1 \oplus \dots \oplus M_t$ .

Ejercicio: Sea  ${}_A M, N_1, \dots, N_t \in \mathcal{L}({}_A M)$ . Se pide demostrar que existe un homomorfismo  $f : N_1 \oplus \dots \oplus N_t \longrightarrow N_1 + \dots + N_t$  sobreyectivo de  $A$ -módulos

tal que entre la suma directa externa y la suma interna, tal que  $f$  es un isomorfismo si y solo si la suma interna es directa. Podría ser interesante usar coordenadas.

**Definición 22** (Base de un módulo libre). Consideramos  $A^n = A \oplus \cdots \oplus A$ , donde la suma se repite  $n$  veces. Para cada  $i = 1, \dots, n$ , tenemos que  $\{e_i : e_i = (0, \dots, 0, 1, 0, \dots, 0)\}$  forman un sistema de generadores de  $A^n$ . Por tanto  $a = \sum_i a_i e_i \in A^n$  es una expresión única.

Dicha base puede no existir.

**Proposición 8.** Dado un módulo cualquiera  ${}_A M$  y  $m_1, m_n \in M$ , existe un único homomorfismo de módulos  $f : A^n \longrightarrow M$  tal que  $f(e_i) = m_i$ .

**Corolario 1.** Si  $M$  es finitamente generado con generadores  $\{m_i\}$ , entonces  $M \cong A^n/L$  para  $L$  un cierto submódulo.

*Demostración.* Unicidad: si existe una tal aplicación  $f$ , entonces para cualquier  $a \in A^n$ ,

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

Veamos la existencia, Definiendo  $f(a) = \sum_i a_i m_i$  obtenemos un homomorfismo de módulos que cumple lo exigido en el enunciado.

Si  $M = Am_1 + \cdots + Am_n$  tenemos que  $L = \ker f$  cumple lo que se pide por el teorema de isomorfía para módulos.  $\square$

### 3. Módulos noetherianos, artinianos y de longitud finita

#### 3.1. Módulos noetherianos

**Definición 23** (Sucesiones exactas). Una sucesión de homomorfismos de módulos  $f_i : M_i \longrightarrow M_{i+1}$  se dice exacta en  $M_{i+1}$  si  $\ker f_{i+1} = \operatorname{Im} f_i$ .

Ejemplo: Dada una sucesión  $\{0\} \longrightarrow L \xrightarrow{\alpha} M \xrightarrow{\beta} N \longrightarrow \{0\}$  es exacta en  $L$  si y solo si  $\ker \alpha = \{0\}$ , es decir,  $\alpha$  es inyectiva, en  $N$  si y solo si  $\operatorname{Im} \beta = N$ , es decir,  $\beta$  sobreyectiva y en  $M$  si y solo si  $\ker \beta = \operatorname{Im} \alpha$ .

A  $\alpha$  se le llama monomorfismos de módulos y a  $\beta$  epimorfismos de módulos.

A esta sucesión se le llama sucesión exacta corta.

Caso particular: Por ejemplo, si  $f : M \longrightarrow N$  es un homomorfismo de módulos, obtenemos:

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

**Proposición 9.** Sea  $0 \longrightarrow L \xrightarrow{\psi} M \xrightarrow{\varphi} N \longrightarrow 0$  una sucesión exacta de  $A$ -módulos. Entonces:

1. Si  $M$  es finitamente generado, lo es también  $N$ .
2. Si  $L$  y  $N$  son finitamente generados, lo es también  $M$ .

*Demostración.* Veamos primero la primera afirmación. Sea  $\{m_i\}$  generadores de  $M$ . Es claro que  $\{\varphi(m_i)\}$  generan  $N$ .

Para la segunda,  $\{n_i\}$  generadores de  $N$ , y tomamos  $\{m_i\} \subseteq M$  tales que  $\varphi(m_i) = n_i$ .

Tomamos  $\{e_i\}$  generadores de  $L$ . Tomamos  $m \in M$ .

$$\varphi(m) = \sum_{i=1}^s r_i n_i = \sum_{i=1}^s r_i \varphi(m_i) = \varphi\left(\sum r_i m_i\right)$$

con lo que  $m - \varphi(\sum r_i m_i) \in \ker \varphi = \text{Im } \psi$ . Luego existen  $b_1, \dots, b_t$  tales que

$$m - \varphi\left(\sum r_i m_i\right) = \psi\left(\sum_j b_j e_j\right)$$

y finalmente:

$$m = \varphi\left(\sum r_i m_i\right) + \sum r_j \varphi(e_j)$$

con lo que  $\{m_i\} \cup \{\psi(e_j)\}$ . □

Ejemplo de que no se puede mejorar la proposición anterior: Sea  $I$  un conjunto infinito,  $K$  un cuerpo.

$$K^I = \{(\alpha_i)_i \in I : \alpha_i \in K\}$$

$K^I$  es un anillo finitamente generado por  $(\dots, 1, 1, 1, \dots)$ . Definimos:

$$K^{(I)} = \{(\alpha_i)_i \in I : \alpha_i \in K \text{ y } \alpha_i = 0 \text{ salvo un número finito de } i \in I\}$$

Tenemos que  $K^{(I)}$  es un ideal de  $K^I$ , y por tanto ideal a izquierda, pero no es finitamente generado como ideal a izquierda.

Es decir,  $M$  finitamente generado no implica que un submódulo suyo sea finitamente generado.

**Definición 24** (Módulos Noetherianos). Un módulo finitamente generado  $M$  se dice Noetheriano si todo submódulo de  $M$  es finitamente generado.

El ejemplo anterior no era un módulo Noetheriano.

**Proposición 10.** *Equivalen:*

1.  $M$  es noetheriano.
2. Cualquier cadena ascendente  $L_1 \subseteq L_2 \subseteq \dots \subseteq L_n \subseteq \dots$  se estabiliza, es decir, a partir de un cierto  $m$  las inclusiones se vuelven igualdades.
3. Cada subconjunto no vacío de  $\mathcal{L}(M)$  tiene un elemento maximal con respecto de la inclusión.

*Demostración.* Veamos que la primera implica la segunda. Tomamos:

$$L = \bigcup_{n \geq 1} L_n \in \mathcal{L}(M)$$

es un submódulo porque están encajados. Por hipótesis, es finitamente generado. Si tomamos un conjunto finito de generadores  $F$  tenemos que  $F \subset L$  y como es finito, debe existir un  $m$  suficientemente grande tal que  $F \subseteq L_m$  y como genera a  $F$  se tiene que  $L \subseteq L_m \subseteq L$  con lo que  $L_n = L_m = L$  para todo  $n \geq m$ .

Veamos que la segunda implica la primera. Sea  $\Gamma \subseteq \mathcal{L}(M)$  no vacío. Si  $\Gamma$  no tiene elemento maximal y tomamos  $L_1 \in \Gamma$ , entonces existe  $L_2 \in \Gamma$  tal que  $L_1 \subsetneq L_2$ .

Reiterando el proceso, tenemos que  $L_1 \subsetneq L_2 \subsetneq \dots \subsetneq L_n \subsetneq \dots$  no se estabiliza.

Veamos que la tercera afirmación implica la primera. Sea  $N \in \mathcal{L}(M)$ . Tomamos el conjunto  $\Gamma$  el conjunto de todos los submódulos finitamente generados de  $N$ . Tenemos que el módulo trivial es finitamente generado, luego  $\Gamma$  es no vacío.

Sea  $L$  un elemento maximal de  $\Gamma$ . Veamos que  $L = N$ .

En caso contrario, tomamos  $x \in N$  tal que  $x \notin L$ . Resulta que  $L + Ax$  es un submódulo de  $N$  y es finitamente generado.  $L + Ax \in \Gamma$  y  $L \neq L + Ax$ , con lo que  $L$  no sería maximal.  $\square$

**Notación.**  $N \in \mathcal{L}(M)$ , escribimos  $N \leq M$ .

**Proposición 11** (Sucesiones exactas cortas en módulos noetherianos). *Sea  $0 \longrightarrow L \xrightarrow{\varphi} M \xrightarrow{\psi} N \longrightarrow 0$ .*

*Entonces  $M$  es noetheriano si y solo si  $L$  y  $N$  son noetherianos.*

*Demostración.* Supongamos  $M$  noetheriano.

$L \cong \text{Im } \psi \leq M$  y entonces  $L$  es noetheriano trivialmente.

Tomamos  $N_1 \subseteq N_2 \subseteq \dots \subseteq N_n \subseteq \dots$  una cadena ascendente en  $\mathcal{L}(N)$ .

Tenemos  $\varphi^{-1}(N_1) \subseteq \varphi^{-1}(N_2) \subseteq \varphi^{-1}(N_n) \subseteq \dots$  cadena en  $\mathcal{L}(M)$ . Existe un  $m$  a partir del cual se estabiliza. Entonces, para todo  $n \geq m$ :

$$N_n = \varphi(\varphi^{-1}(N_n)) = \varphi(\varphi^{-1}(N_m)) = N_m$$

con lo cual  $N$  es noetheriano.

Supongamos ahora que  $N$  y  $L$  son noetherianos. Tomamos una cadena ascendente  $M_n$  de submódulos de  $M$ .

Por otro lado,  $M_n \cap \text{Im } \psi$  es una cadena de submódulos de  $M$ , que se estabiliza por ser noetheriano  $\text{Im } \psi \cong L$ .

Tenemos  $\varphi(M_n)$  es una cadena de submódulos de  $N$ , que también se estabiliza.

Tomemos el menor natural tal que ambas cadenas se hayan estabilizado. Sea  $n$  mayor,  $x \in M_n$ ,  $\varphi(x) \in \varphi(M_n) = \varphi(M_m)$ , debe existir  $y \in M_m$ . Luego  $x - y \in \ker \varphi = \text{Im } \psi$ , con lo que  $x - y \in M_n \cap \text{Im } \psi = M_m \cap \text{Im } \psi \subseteq M_m$  y  $x \in M_m$  ya que  $y \in M_m$ .

Por tanto  $M$  es noetheriano.  $\square$

**Corolario 2.** Dados dos módulos  $M_1$  y  $M_2$ . Entonces:

$$M_1 \oplus M_2$$

es noetheriano si y solo si  $M_1$  y  $M_2$  lo son.

*Demostración.* Sea la sucesión exacta corta

$$0 \longrightarrow M_1 \longrightarrow M_1 \oplus M_2 \longrightarrow M_2 \longrightarrow 0$$

donde la primera aplicación es  $m_1 \mapsto (m_1, 0)$  y  $(m_1, m_2) \mapsto m_2$  y el núcleo de la segunda es la imagen de la primera. Trivialmente se sigue el corolario.  $\square$

**Teorema 5.** Sea  $A$  un anillo. Cada módulo sobre  $A$  finitamente generado es noetheriano si y solo si  ${}_A A$  es noetheriano.

*Demostración.* Una de las implicaciones es obvia.

Veamos que si el módulo regular es noetheriano, veamos que cualquier otro lo es.

Sea  $M$  finitamente generado, existe un homomorfismo sobreyectivo  $\phi$  tal que  $A^n \longrightarrow M$ .

Usando inductivamente el corolario, tenemos que  $A^n$  es noetheriano. La proposición nos dice que  $M$  es noetheriano, aplicándolo a la sucesión

$$0 \longrightarrow \ker \phi \longrightarrow A^n \longrightarrow M \longrightarrow 0$$

$\square$

**Definición 25** (Anillo noetheriano).  $A$  se dice noetheriano a izquierda si el módulo regular es noetheriano. Si  $A$  es conmutativo diremos simplemente noetheriano.

**Corolario 3.** Si  $A$  es noetheriano, equivalen para cualquier sucesión exacta corta:

1.  $M$  es finitamente generado.
2.  $L$  y  $N$  son finitamente generados.

**Corolario 4.** Todo dominio de ideales principales es noetheriano.

### 3.2. Módulos artinianos

**Definición 26** (Módulo artiniano). Para un  ${}_A M$ , son equivalentes:

1. Cada cadena descendente  $L_1 \supseteq L_2 \supseteq \dots \supseteq L_n \supseteq \dots$  de submódulos de  $M$  se estabiliza, esto es, a partir de cierto natural  $m$  se tiene  $L_n = L_m$  para todo  $n \geq m$ .
2. Cada subconjunto de  $\mathcal{L}(M)$  tiene un elemento minimal.

A un tal módulo lo llamaremos artiniano.

Ejercicio: Sea  $A$  un dominio de integridad conmutativo. Si el módulo regular es artiniano, entonces  $A$  es un cuerpo.

En particular  $\mathbb{Z}$  no es artiniano, aunque por ser un DIP, sí que es noetheriano.

Ejercicio:  $K$  un cuerpo de característica 0. Tomo  $K[x]$  anillo de polinomios. Veo  $K[x]$  como  $K$ -espacio vectorial. Tomamos  $T$  la aplicación lineal  $T(f) := f'$ , donde  $f'$  es el polinomio derivado. Esto nos da una estructura de  $K[x]$ -módulo sobre  $K[x]$  que no es la del módulo regular. Se pide demostrar que ese módulo es artiniano y no finitamente generado.

En consecuencia, la estructura que hemos definido no es la misma que la del módulo regular.

**Proposición 12.** Sea

$$0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0$$

Entonces  $M$  es artiniano si y solo si  $L$  y  $N$  son artinianos.

Ejercicio: sea  $p$  un número primo. Definimos:

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

Se pide comprobar que es un subgrupo  $\mathbb{S} = \{z \in \mathbb{C} : |z| = 1\}$  y demostrar que visto como  $\mathbb{Z}$ -módulo es artiniano pero no es finitamente generado.

### 3.3. Módulos de longitud finita

**Definición 27** (Serie de composición). Sea  $M$  un módulo. Una serie de composición de  $M$  es una cadena de submódulos

$$M = M_n \supsetneq M_{n-1} \supsetneq \dots \supsetneq M_1 \supsetneq M_0 = \{0\}$$

tal que si  $M_i \supseteq N \supseteq M_{i-1}$  para  $N$  submódulo, entonces  $N = M_i$  o  $N = M_{i-1}$ . Es decir, cada submódulo es maximal en el anterior.

A  $n$  le llamamos la longitud de la serie.

Ejemplo: serie de composición de  $\mathbb{Z}_{12}$ . Tiene como subgrupos a  $\mathbb{Z}_m$  con  $m$  divisor de 12.

$$M_3 = \mathbb{Z}_{12}$$

tiene como subgrupo maximal (argumentando por Lagrange):

$$M_2 = \langle 2 \rangle$$

que a su vez tiene como subgrupo maximal

$$M_1 = \langle 4 \rangle$$

y ya solo tiene

$$M_0 = \{0\}$$

**Definición 28** (Módulo simple).  $M$  se dice simple si  $M \supset \{0\}$  es una serie de composición. Es decir, si no tiene submódulos propios y no es el módulo 0.

**Proposición 13.** *La condición de que cada submódulo sea maximal en el anterior es equivalente a que los factores  $M_i/M_{i-1}$  sean simples.*

**Teorema 6.** *Toda serie de composición del mismo módulo tiene la misma longitud y los mismos factores salvo isomorfismo y reordenación.*

$\mathbb{Z}_{12}$  tiene como factores  $\mathbb{Z}_2$ ,  $\mathbb{Z}_2$  y  $\mathbb{Z}_3$ .

**Proposición 14.** *Un módulo no nulo admite una serie de composición si y solo si es noetheriano y artinian.*

*Demostración.* Sea  $M_i$  una serie de composición. Inducción sobre  $n$ . Si  $n = 1$ , tenemos que  $M$  es simple y en particular noetheriano y artinian.

Si  $n > 1$ , entonces  $M_{n-1}$  admite una serie de composición de longitud  $n - 1$ , luego es noetheriano y artinian. Tomamos la sucesión exacta corta

$$0 \longrightarrow M_{n-1} \longrightarrow M_n \longrightarrow M_n/M_{n-1} \longrightarrow 0$$

El primer elemento es noetheriano y artinian, el último es simple (luego noetheriano y artinian), con lo que  $M_n$  es noetheriano y artinian.

Para el recíproco, como  $M$  es artinian, contiene un submódulo simple  $M_1$ . Entonces hay un  $M_2 \supsetneq M_1$  donde  $M_2/M_1$  es simple. Reiterando el proceso, tenemos  $0 \subsetneq M_1 \subsetneq M_2 \subsetneq \dots$  y como es noetheriano, habrá un  $M_n$  que termine la cadena.  $\square$

**Corolario 5.** Dada una sucesión exacta corta,  $0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0$ ,  $L$  y  $N$  admite serie de composición si y solo si  $M$  admite serie de composición.

**Corolario 6.**  $M_1, M_2$  admiten series de composición si y solo si  $M_1 \oplus M_2$  admite serie de composición.

**Teorema 7** (Jordan-Hölder). *Supongan que  $M$  admite series de composición:*

$$\begin{aligned}\{0\} &= M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \dots \subsetneq M_n = M \\ \{0\} &= N_0 \subsetneq N_1 \subsetneq N_2 \subsetneq \dots \subsetneq N_m = M\end{aligned}$$

*Entonces  $n = m$  y existe una permutación  $\sigma$  tal que*

$$M_i/M_{i-1} \cong N_{\sigma(i)}/N_{\sigma(i)-1}$$

*Demostración.* Si  $n = 1$ , entonces  $M$  es simple y  $m = 1$  y el único factor posible es el  $M/\{0\} = M$ .

Si  $n > 1$ , como  $M$  no es simple,  $m > 1$ .

Vamos a observar un caso particular. Supongamos que  $N_{m-1} = M_{n-1}$ . Por hipótesis de inducción aplicado a  $N_{m-1}$ , tenemos que  $n - 1 = m - 1$ , luego  $n = m$  y se da el enunciado (tomando la permutación  $\sigma$  para los  $n - 1$  primeros elementos y extendiéndola a una permutación de  $n$  elementos  $\sigma'$  tal que  $\sigma'(n) := n$ ,  $\sigma'(k) := \sigma(k)$ ).

Vamos ahora al caso general. Como hemos visto en el caso particular anterior, podemos suponer  $M_{n-1} \neq N_{m-1}$ , por lo que  $M_{n-1} + N_{m-1} = M$  (ya que  $M_{n-1} \subsetneq M_{n-1} + N_{m-1} \subseteq M$  y  $M_{n-1}$  es maximal).

Tomamos  $N_{m-1} \cap M_{n-1}$  que admite una serie de composición:

$$\{0\} = L_0 \subsetneq L_1 \subsetneq \dots \subsetneq L_k = N_{m-1} \cap M_{n-1}$$

y tenemos que, por el teorema de isomorfía:

$$N_m/N_{m-1} = M/N_{m-1} = (M_{n-1} + N_{m-1})/N_{m-1} \cong M_{n-1}/(M_{n-1} \cap N_{m-1})$$

que al ser un factor es simple.



Aplicando la inducción,  $n - 1 = k + 1$  y existe una permutación  $\tau$  de  $n - 1$  elementos tal que

$$L_i/L_{i-1} \cong M_{\tau(i)}/M_{\tau(i)-1}$$

donde  $i = 1, \dots, n - 2$  y

$$M_{n-1}/L_{n-2} = M_{n-1}/(M_{n-1} \cap N_{m-1}) \cong M_{\tau(n-1)}/M_{\tau(n-1)-1}$$

Tenemos que, por el teorema de isomorfía:

$$M_n/M_{n-1} = M/M_{n-1} = (N_{m-1} + M_{n-1})/M_{n-1} \cong N_{m-1}/(N_{m-1} \cap M_{n-1})$$

que al ser un factor es simple.

Aplicando la inducción,  $m - 1 = k + 1$  y existe una permutación  $\rho$  de  $m - 1$  elementos tal que

$$L_i/L_{i-1} \cong N_{\rho(i)}/N_{\rho(i)-1}$$

donde  $i = 1, \dots, n - 2$  y

$$N_{n-1}/L_{n-2} = N_{n-1}/(M_{n-1} \cap N_{m-1}) \cong N_{\rho(n-1)}/N_{\rho(n-1)-1}$$

Tenemos ya que  $n = k + 2 = m$ , y si definimos  $\sigma$  la permutación de  $n$  elementos:

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

□

**Definición 29** (Módulo de longitud finita). Un módulo se dice de longitud finita si tiene una serie de composición finita o es  $\{0\}$ . La longitud  $\ell(M)$  es la de cualquiera de sus series de composición, o cero si  $M = \{0\}$ .

Ejercicio: sea  $M$  un módulo de longitud finita. Se pide demostrar que si  $0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0$  es una sucesión exacta corta, entonces:

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

Si  $U, V \in \mathcal{L}(M)$ , entonces:

$$\ell(U + V) = \ell(U) + \ell(V) - \ell(U \cap V)$$

Ejemplo: si  $V$  es un  $K$ -espacio vectorial,  $\ell(V) = \dim(V)$ .

Ejemplo:  $\ell(\mathbb{Z}_{12}) = 3$ , ya que calculamos antes una serie de composición.

Otro ejemplo:  $\ell(\mathbb{Z}_p) = 1$  si  $p$  es primo.

Ejercicio:  $\ell(\mathbb{Z}_n)$  es la suma de los exponentes de su descomposición en primos.

Ejemplo: si  $n = \prod p_i^{e_i}$  entonces  $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{e_1}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{e_t}}$ . Sea  ${}_A M$  un módulo,  $\mathcal{L}(M)$  es el conjunto de todos los submódulos de  $M$ .

Dado  $\Gamma \subseteq \mathcal{L}(M)$  no vacío, tenemos  $\bigcap_{N \in \Gamma} N \in \mathcal{L}(M)$  (no tiene por qué ocurrir que estén en  $\Gamma$ ,  $\bigcap_{n \geq 1} n\mathbb{Z} = \{0\} \notin m\mathbb{Z}$  para ningún  $m \geq 1$ ).

**Definición 30** (Zócalo). El zócalo de  $M$  es el menor submódulo de  $M$  que contiene a todos los submódulos simples de  $M$ .

Si  $M$  no tiene ningún submódulo simple, definimos el zócalo como  $\{0\}$ .

En ambos casos usaremos la notación  $\text{Soc}(M)$ .

Ejemplo: si  $V$  es un  $K$ -espacio vectorial,  $\text{Soc}(V) = V$ .

Ejemplo:  $\text{Soc}(\mathbb{Z}) = \{0\}$ , puesto que cada  $n\mathbb{Z}$  contiene un  $2n\mathbb{Z}$ , luego no es simple.

De hecho, si  $A$  es un dominio de integridad que no es un cuerpo,  $\text{Soc}(A) = \{0\}$ . Tienes que sus submódulos son ideales. Para  $x \in I$ , el ideal generado por  $x^2$  está dentro de  $I$ , luego  $I$  no es simple.

**Proposición 15.** Sea  $M$  de longitud finita. Existen submódulos  $S_i$  simples de  $M$  tales que

$$\text{Soc}(M) = S_1 \dot{+} \cdots \dot{+} S_n$$

Además si  $T_i$  son simples tales que  $\text{Soc}(M) = T_1 \dot{+} \cdots \dot{+} T_m$ , entonces  $n = m$  y tras reordenación,  $S_i \cong T_i$ .

*Demostración.* Si  $\Gamma$  es el conjunto de todos los submódulos de la forma  $S_1 \dot{+} \cdots \dot{+} S_n$

Si  $M \neq \{0\}$ , entonces  $\Gamma \neq \emptyset$ , ya que  $M$  contiene algún submódulo simple.

Como  $M$  es Noetheriano, existe un  $S_1 \dot{+} \cdots \dot{+} S_n$  maximal.

$S_1 \dot{+} \cdots \dot{+} S_n \subseteq \text{Soc}(M)$ . Sea  $S \in \mathcal{L}(M)$  simple.

$$S \cap (S_1 \dot{+} \cdots \dot{+} S_n)$$

puesto que  $S$  es simple y la intersección es submódulo, se tiene que dicha intersección o es  $\{0\}$  o es  $S$ .

Consideramos

$$S \cap (S_1 \dot{+} \cdots \dot{+} S_n) = \{0\}$$

luego

$$S \dot{+} S_1 \dot{+} \cdots \dot{+} S_n \in \Gamma$$

con lo que no sería maximal.

Luego se tiene:

$$S \subseteq S_1 \dot{+} \cdots \dot{+} S_n \in \Gamma$$

luego, como  $S$  era un modulo simple arbitrario, tenemos que  $\text{Soc}(M) = S_1 \dot{+} \cdots \dot{+} S_n$ .

Resulta que

$$\{0\} \subsetneq S_1 \subsetneq S_1 \dot{+} S_2 \subsetneq \cdots \subsetneq S_1 \dot{+} \cdots \dot{+} S_n = \text{Soc}(M)$$

es una serie de composición, ya que:

$$(S_1 \dot{+} \cdots \dot{+} S_i) / (S_1 \dot{+} \cdots \dot{+} S_{i-1}) \cong S_i$$

Aplicando Jordan-Hölder se obtiene el resultado.  $\square$

**Definición 31** (Módulo semisimple). Sea  $M$  de longitud finita. Decimos que  $M$  es semisimple si es  $\text{Soc}(M) = M$ .

Ejercicio: Sea  $A$  un DIP que no sea un cuerpo,  $I$  ideal de  $A$ . Se pide demostrar que  $A/I$  es de longitud finita si y solo si  $I \neq \langle 0 \rangle$ .

¿Se puede deducir cuál es la longitud de  $A/I$  de un generador de  $I$ ?

### 3.3.1. Módulos de longitud finita sobre un DIP

Sea de ahora en adelante  $A$  un dominio de ideales principales que no sea un cuerpo.

**Lema 3.**  ${}_A M$  es de longitud finita si y solo si  ${}_A M$  finitamente generado y acotado.

*Demostración.*  $M$  distinto del 0, porque si no es trivial.

$M$  de longitud finita, por tanto noetheriano, por tanto finitamente generado:  $M = Am_1 + \cdots + Am_n$ , con  $m_i \in M$ .

$$\langle \mu \rangle = \text{Ann}_A(M) = \bigcap_{i=1}^n \text{ann}_A(m_i)$$

porque el anillo  $A$  es conmutativo, donde ademas cada anulador de cada elemento es un ideal (a izquierdas en un conmutativo, luego ideal).

Sea  $\langle f_i \rangle = \text{ann}_A(m_i)$ , entonces

$$\langle \mu \rangle = \bigcap_{i=1}^n \langle f_i \rangle$$

donde  $\mu = \text{mcm}\{f_i : 1 \leq i \leq n\}$ .

Veamos que  $f_i \neq 0$  para cada  $i$ .

$$M \subseteq Am_i \cong A/\langle f_i \rangle$$

luego  $\ell(Am_i) < \infty$ , como  $A$  no es un cuerpo y por tanto  $M$  no es artiniano, entonces  $\langle f_i \rangle \neq 0$ .

Luego  $\langle \mu \rangle \neq 0$  y por tanto  $M$  es acotado.

Veamos el recíproco:  $M$  acotado y finitamente generado.

$$M = Am_1 + \cdots + Am_n$$

Vemos que cada  $Am_i$  es de longitud finita ( $\mu \neq 0$  por ser acotado, luego cada  $\langle f_i \rangle \neq 0$ ). Tenemos que  $Am_i \cong A/\langle f_i \rangle$  es de longitud finita.

Existe un epimorfismo entre  $Am_1 \oplus \cdots \oplus Am_n$  (que es de longitud finita) y  $Am_1 \oplus \cdots \oplus Am_n$ , con lo que el segundo tiene longitud finita.  $\square$

$\ell_A(M) < \infty$ , entonces es acotado, o sea  $\langle \mu \rangle = \text{Ann}_A(M) = \langle 0 \rangle$ . Entonces

$$M = M_1 \dot{+} \cdots \dot{+} M_t$$

donde  $M_i$  es la componente  $p_i$  primaria que viene de  $\mu = p_1^{e_1} \cdots p_t^{e_t}$  ( $M_i = \{m \in M : m \cdot p_i^{e_i} = 0\}$ ). Además  $M_i$  es finitamente generado. ¿Se puede descomponer como suma directa de submódulos indescomponibles?

$$M = M_1 \dot{+} \cdots \dot{+} M_t$$

donde

$$M_i = \{q_i m : m \in M\} = \{m \in M : p_i^{e_i} m = 0\} = \{m \in M : a_i q_i m = m\}$$

con  $q_i = \frac{\mu}{p_i^{e_i}}$  y  $\sum_i a_i q_i = 1$  y  $\langle \mu \rangle = \text{Ann}_A(M)$ . Se tiene que  $\text{Ann}_A(M_i) = \langle p_i^{e_i} \rangle$ .

**Definición 32** (Módulo  $p$ -primario).  ${}_A M$  se dice  $p$ -primario si  $\text{Ann}_A(M) = \langle p^e \rangle$ ,  $p$  un irreducible.

Vamos a estudiar la estructura de módulos primarios de longitud finita.

*Observación 7.*  ${}_A M$   $p$ -primario,  $\ell(M) < \infty$ .

$$\text{Ann}_A(M) = \langle p^t \rangle$$

Si  $0 \neq m \in M$ ,  $\text{ann}_A(m) \supseteq \text{Ann}_A(M) = \langle p^t \rangle$ , tenemos que  $\text{ann}_A(m) = \langle p^r \rangle$  con  $r \leq t$ .

Si  $M = Am_1 + \cdots + Am_m$ , entonces  $\langle p^t \rangle = \text{ann}_A(m_1) \cap \cdots \cap \text{ann}_A(m_m)$ . Luego  $\langle p^t \rangle = \text{ann}_A(m_i)$  para algún  $i$ .

**Corolario 7.** Existe un  $x \in M$ ,  $\text{Ann}_A(M) = \text{ann}_A(x)$ .

**Lema 4.**  $\ell(M) < \infty$ ,  $M$   $p$ -primario. Para  $0 \neq m \in M$ , entonces:

$$Am \text{ es simple} \iff \text{ann}_A(m) = \langle p \rangle$$

y como consecuencia

$$\text{Soc}(M) = \{m \in M : pm = 0\}$$

*Demostración.* Dado  $m$ , tenemos  $Am \cong A/\text{ann}_A(m)$ . Si  $Am$  es simple, entonces  $\text{ann}_A(m)$  es ideal maximal (generado por irreducible o ideal primo) y  $\text{ann}_A(m) \supseteq \text{Ann}_A(M) = \langle p^t \rangle$ . Entonces  $\text{ann}_A(m) = \langle p \rangle$ .

Recíprocamente, si  $\text{ann}_A(m) = \langle p \rangle$  entonces  $Am \cong A/\langle p \rangle$  es simple.

$\text{Soc}(M) = S_1 \dot{+} \cdots \dot{+} S_n$  con  $S_i$  simple. Sea  $m$  en el zócalo,  $\text{ann}_A(m) \supseteq \text{Ann}_A(S_1 \dot{+} \cdots \dot{+} S_n) = \bigcap_{k=1}^n \text{Ann}_A(S_k)$ . Tomamos  $s_i$  tal que  $\text{Ann}_A(S_i) = \text{ann}_A(s_i)$ , tenemos que  $S_i = As_i$ , luego  $As_i \cong A/\text{ann}_A(s_i)$  y es simple, luego  $\text{ann}_A(s_i) = \langle p \rangle$ , tenemos que  $\text{ann}_A(m) \supseteq \langle p \rangle$  y finalmente  $pm = 0$ .

Tomamos ahora  $m \in M$  tal que  $pm = 0$ .  $\langle p \rangle \subseteq \text{ann}_A(m)$  pero es maximal, luego se da la igualdad.

$$Am \cong A/\text{ann}_A(m) = A/\langle p \rangle$$

luego es simple, y  $Am \subseteq \text{Soc}(M)$  y en particular  $m \in \text{Soc}(M)$ .

□

**Proposición 16.** Suponemos que tenemos  $M$   $p$ -primario y de longitud finita. Sea  $x \in M$  tal que  $\text{Ann}_A(M) = \text{ann}_A(x)$ . Entonces  $Ax$  es un sumando directo interno de  $M$ .

*Demostración.* Por inducción sobre la longitud  $\ell(M) < \infty$ .

Si la longitud es 1,  $M$  es simple, entonces  $M = Ax$ .

Si  $\ell(M) > 1$  y  $Ax = M$ , no hay nada que demostrar.

Veamos que pasa si  $Ax \neq M$ . Veamos que existe un  $y \in M$  tal que  $y \neq Ax$  y  $\text{ann}_A(y) = \langle p \rangle$ .  $\ell(M/Ax) < \infty$ , debe contener algún simple  $S \subseteq M/Ax$ . Tomamos  $s \in S$  tal que  $S = As$ .

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

Y por tanto  $\text{ann}_A(s) = \langle p \rangle$ .

Tomamos  $z \in M$  tal que  $s = z + Ax$ , es decir,  $pz \in Ax$ . Es decir,  $pz = ax$  para cierto  $a \in A$ . Afirmamos que  $p|a$  (no es obvio porque es un módulo).

Supongamos que no es así. Por Bezout,  $1 = ua + vp$  para  $u, v \in A$  adecuados. En dicho caso,  $x = uax + vpx = upz + vpx = p(uz + vx)$ .

$$\text{ann}_A(uz + vx) = \langle p^{t'} \rangle$$

para  $t' \leq t$ . Se deduce que  $p^{t'-1}x = 0$ .  $p^{t-1}x = 0$ , y entonces como el anulador de  $x$  es el de  $M$  y está generado por  $p^t$ , no puede anularlo  $p^{t'-1}$  ya que  $t' - 1 \leq t - 1 < t$ .

Cuenta alternativa:  $p^{t-1}ax = p^tz = 0$  entonces  $p^{t-1}a \in \text{ann}_A(x) = \langle p^t \rangle$ , tenemos que  $a = pa'$

Hemos obtenido un elemento  $s = z + Ax \in M/Ax$  y que  $pz = ax$  y hemos visto que  $p|a$ . Así tenemos que  $pz = pa'x$  y entonces  $p(z - a'x) = 0$ . Llamo  $y = z - a'x \neq 0$  y  $py = 0$  con lo que  $\text{ann}_A(y) = \langle p \rangle$ .

Tenemos que  $Ay$  es simple y  $y \notin Ax$  así que  $Ay \cap Ax = \{0\}$ .

$$Ax \cong Ax/(Ay \cap Ax) \cong (Ax + Ay)/Ay \cong A(x + Ay) \subseteq M/Ay$$

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

con lo cual todas las inclusiones son igualdades.

Tenemos que  $\text{Ann}_A(M/Ay) = \langle p^t \rangle = \text{ann}_A(x + Ay)$ , que están en las mismas condiciones de la hipótesis pero con  $\ell(M/Ay) < \ell(M)$ . Aplicando la hipótesis de inducción, tenemos que  $M/Ay = (Ax + Ay)/Ay \dot{+} N/Ay$  para cierto  $N \in \mathcal{L}(M)$  tal que  $N \supseteq Ay$ . De aquí se deduce que  $M = Ax + Ay + N = Ax + N$ . Tomamos  $Ax \cap N \subseteq (Ax + Ay) \cap N = Ay$ . Entonces  $Ax \cap N = Ax \cap N \cap Ay = Ax \cap Ay = \{0\}$ .

□

**Teorema 8.** Sea  ${}_A M$   $p$ -primario de longitud finita. Existen  $x_1, \dots, x_n \in M \setminus \{0\}$  tales que  $M = Ax_1 \dot{+} \dots \dot{+} Ax_n$  y

$$\text{Ann}_A(M) = \text{ann}_A(x_1) \supseteq \text{ann}_A(x_2) \supseteq \dots \supseteq \text{ann}_A(x_n)$$

Además, si  $y_1, \dots, y_n \in M$  no nulos son tales que  $M = Ay_1 \dot{+} \dots \dot{+} Ay_n$  y  $\text{Ann}_A(M) = \text{ann}_A(y_1) \supseteq \text{ann}_A(y_2) \supseteq \dots \supseteq \text{ann}_A(y_m)$ , entonces  $n = m$  y  $\text{ann}_A(x_i) = \text{ann}_A(y_i)$ .

*Demostración.* Tomo  $x_1 \in M$  tal que  $\text{Ann}_A(M) = \text{ann}_A(x)$ , por la proposición,  $M = Ax_1 \dot{+} N$  para cierto submódulo  $N$  de  $M$ . Es claro que  $\text{Ann}_A(N) \supseteq \text{Ann}_A(M) = \langle p^t \rangle$ , con lo que  $\text{Ann}_A(N) = \langle p^{t'} \rangle$  con  $t' \leq t$  y  $\ell(N) < \ell(M)$ .

Por inducción sobre  $\ell(M)$ , tenemos  $x_1, x_2, \dots, x_n \in N$  y  $N = Ax_2 + \dots + Ax_n$ . De esto se deduce

$$M = Ax_1 + \dots + Ax_n$$

y  $\text{ann}_A(x_1) = \text{Ann}_A(M) \subseteq \text{ann}_A(x_2) \subseteq \dots \subseteq \text{ann}_A(x_n)$ .

Veamos la unicidad. Hacemos inducción sobre  $\ell(M)$ .

Si  $\ell(M) = 1$ , tenemos que es simple y  $M = Ax = Ay$  y  $n = 1 = m$ .

Si  $\ell(M) > 1$ , tenemos que  $M$  no es simple. Consideramos  $M/pM$  donde  $pM := \{pm : m \in M\}$  que es un submódulo por ser  $A$  conmutativo.  $\text{Ann}_A(pM) = \langle p \rangle$ .

$$\text{Soc}(M/pM) = M/pM$$

luego  $M/pM$  es semisimple.

Tengo un homomorfismo de módulos  $M \rightarrow Ax_1/Apx_1 \oplus \dots \oplus Ax_n/Apx_n$  tal que  $\sum A - ix_i \mapsto (a_1x_1 + Apx_1, \dots, a_nx_n + Apx_n)$ .

Se puede demostrar que dicha aplicación es sobreyectivo y su núcleo es  $pM$ .

$$M/pM \cong Ax_1/Apx_1 \oplus \dots \oplus Ax_n/Apx_n$$

$n = \ell(M/pM)$ . Argumentando de forma análoga para  $y$ ; obtenemos  $n = \ell(M/pM) = m$ .

Si  $pM = \{0\}$ , tenemos que todos los anuladores son iguales:  $\text{ann}_A(x_i) = \langle p \rangle = \text{ann}_A(y_i)$ .

Supongamos que  $pM \neq \{0\}$ .

$$pM = Apx_1 + \dots + Apx_r$$

para cierto  $r \leq n$ .

Así,  $\text{ann}_A(x_i) = \langle p \rangle$  si solo si  $i > r$ . y también  $\text{ann}_A(y_i) = \langle p \rangle$  si solo si  $i > r$ . Para cualquier  $i \leq r$ , tenemos que  $\text{ann}_A(px_i) = \langle p^{t_i-1} \rangle$  si  $\text{ann}_A(x_i) = \langle p^{t_i} \rangle$ .

$$\text{ann}_A(px_1) \supseteq \text{ann}_A(px_2) \supseteq \dots \supseteq \text{ann}_A(px_r)$$

$$\text{ann}_A(py_1) \supseteq \text{ann}_A(py_2) \supseteq \dots \supseteq \text{ann}_A(py_s)$$

donde  $\text{ann}_A(y_i) = \langle p^{s_i} \rangle$  si y solo si  $i > s$ . Pero  $\ell(pM) < \ell(M)$ , por inducción  $s = r$  y que  $s_i - 1 = r_i - 1$  y como sabemos que si  $i > r = s$  tenemos que  $\text{ann}_A(x_i) = \text{ann}_A(y_i) = \langle p \rangle$ .

□

*Observación 8.* Si  $A = \mathbb{Z}$ ,  $M$  grupo abeliano,  $x \in M$ ,  $\text{ann}_{\mathbb{Z}}(x) = n\mathbb{Z}$ ,  $n$  recibe el nombre de el orden.

*Observación 9.* Si  $A = K[x]$ ,  $T : V \longrightarrow V$ ,  $n = \dim_K V < \infty$ ,  $v \in V$ ,  $\text{ann}_{K[x]}(v) = \langle f(x) \rangle$ . Tenemos que  $f$  tiene grado  $n$ .  $\{v, Tv, \dots, T^{n-1}v\}$  es una base de  $V$ .

Ejemplo:  $\mathcal{U}(\mathbb{Z}_8) = \{1, 3, 5, 7\}$ . Viendo los ordenes de los elementos:

$$\mathcal{U}(\mathbb{Z}_8) = \langle 3 \rangle \dot{+} \langle 5 \rangle$$

donde  $\langle \cdot \rangle$  es la generación como subgrupo.

Ejemplo: Suponemos un espacio vectorial  $V$  de dimensión 3 y un endomorfismo  $T$  cuyo polinomio mínimo es de la forma  $(x - \lambda)^2$  con  $\lambda \in K$ . Sabemos que existen dos vectores  $v_1, v_2$  tales que

$$V = K[x]v_1 \dot{+} K[x]v_2$$

con  $\text{ann}_{K[x]} v = \langle (x - \lambda)^2 \rangle \subsetneq \langle x - \lambda \rangle = \text{ann}_{K[x]} v_2$ .

**Corolario 8.** Si  ${}_A M$  es un módulo  $p$ -primario, entonces

$$M \cong C_1 \oplus \dots \oplus C_n$$

con  $C_i$  cíclico.

Si  $M \cong D_1 \oplus \dots \oplus D_m$ , con  $D_i$  cíclico, entonces  $n = m$  y tras reordenación,  $D_i \cong C_i$  para todo  $i$ .

*Demostración.* De  $M \cong C_1 \oplus \dots \oplus C_n$ , se puede exigir que  $x_1, \dots, x_n \in M$  tales que

$$M = Ax_1 \dot{+} \dots \dot{+} Ax_n$$

con  $\text{ann}_A(x_1) \subseteq \text{ann}_A(x_2) \subseteq \dots \subseteq \text{ann}_A(x_n)$

Con  $D_1 \oplus \dots \oplus D_m$  hago lo mismo.

$$M = Ay_1 \dot{+} \dots \dot{+} Ay_n$$

ordenados bajo el mismo criterio.

El enunciado se sigue de aplicar el teorema anterior. De  $\text{ann}(x_i) = \text{ann}(y_i)$  se deduce

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

□

Ejercicio: Decimos que un módulo  $M$  es indescomponible si  $M \cong L \oplus N$  implica que  $L = \{0\}$  (o  $N = \{0\}$ ). Razonar que en el corolario cada uno de los  $C_i$  es indescomponible.

Ejemplo:  $M$  grupo abeliano de longitud finita y  $p$ -primario. Aplicando el corolario,  $M \cong C_1 \oplus \dots \oplus C_n$  con  $C_i$  cíclico y de longitud finita  $p$ -primarios. Tenemos que  $M \cong \mathbb{Z}_{p^{m_1}} \oplus \dots \oplus \mathbb{Z}_{p^{m_n}}$ ,  $M$  es finito de cardinal  $p^{m_1 + \dots + m_n}$ .



**Teorema 9** (Estructura de módulos sobre un DIP).  ${}_A M \neq \{0\}$  de longitud finita. Existen irreducibles distintos  $p_1, \dots, p_r \in A$  y enteros positivos  $n_1, \dots, n_r$ , tales que  $e_{i1} \geq \dots \geq e_{in_i}$  con  $i \in \{1, \dots, r\}$  determinados por  $M$ :

$$M = \dot{+}_{i=1}^r \left( \dot{+}_{j=1}^{n_i} Ax_{ij} \right)$$

A esa expresión se le llama la descomposición cíclica-primaria de  $M$  (la primaria sería la primera suma y luego cada factor primario se descompone en factores cíclicos). Los  $x_{ij} \in M$  son tales que verifican:

$$\text{ann}_A(x_{ij}) = \langle p_i^{e_{ij}} \rangle$$

con  $i \in \{1, \dots, r\}, j \in \{1, \dots, n_i\}$ . Se le llaman divisores elementales de  $M$  y determinan  $M$  salvo isomorfismos.

*Demostración.* Supongamos otra descomposición:

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

con  $N_i$   $s_i$ -primario para  $s_1, \dots, s_t \in A$  irreducibles. Entonces

$$\langle \mu \rangle = \text{Ann}_A(M) = \bigcap_{i=1}^t \text{Ann}_A(N_i) = \bigcap_{i=1}^t \langle s_i^{t_i} \rangle = \langle \text{mcm}\{s_i^{t_i}\} \rangle = \left\langle \prod s_i^{t_i} \right\rangle$$

y  $\mu$  es asociado con  $s_1^{t_1} \dots s_t^{t_t}$ . Tras reordenación, por ser  $A$  un DFU,  $t = r$  y  $s_i = p_i$ .

$N_i \subseteq \{m \in M : p_i^{e_i} m = 0\} = M_i$ , entonces  $N_i = M_i$ , argumentando sobre las longitudes.

□

*Observación 10.* Sea  $M$  un grupo abeliano de longitud finita,  $A = \mathbb{Z}$ . Los grupos abelianos son de longitud finita si y solo si son finitos.

*Demostración.*  $\mu = p_1^{e_1} \dots p_r^{e_r}$

$$M = \dot{+}_{i=1}^r \dot{+}_{j=1}^{n_i} \mathbb{Z}x_{ij} \cong \oplus_{i=1}^r \oplus_{j=1}^{n_i} \mathbb{Z}_{p_i^{e_{ij}}}$$

con  $x_{ij}$ . Luego es finito de cardinal:

$$m = \prod_{i=1}^r \prod_{j=1}^{n_i} p_i^{e_{ij}} = p_1^{f_1} \dots p_r^{f_r}$$

donde  $f_i = \sum_{j=1}^{n_i} e_{ij}$ .  
 $\mu | m$ .

□

Ejemplo: si  $m = 12$ ,  $p_1 = 2$  y  $p_2 = 3$ . Entonces  $M \cong \mathbb{Z}_4 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_{12}$  o  $M \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_2 \mathbb{Z}_6$ .

Ejemplo:  $A = K[x]$  y  $V$  un  $K[x]$ -módulo de longitud finita.  $V$  es dimensión finita:

$$V = \dot{+}_{i=1}^r \dot{+}_{j=1}^{n_i} K[x]x_{ij}$$

luego es suma directa de espacios de dimensión finita.

$$V_{ij} = K[x]x_{ij} \subseteq V$$

donde  $T(V_{ij}) \subseteq V_{ij}$ . Tenemos que

$$\text{minpol}(T|_{V_{ij}}) = p_i^{e_{ij}}$$

existen  $x_{ij}$  tales que  $\{x_{ij}, Tx_{ij}, \dots, T^{\dim V-1}x_{ij}\}$  base de  $V_{ij}$ .

Caso particular:  $\dim V = n$ ,  $\text{minpol}(T) = (x - \lambda)^n$ . Existe un  $v \in V$  tal que

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

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

La matriz asociada es:

$$M_B(T) = \begin{pmatrix} \lambda & 1 & 0 & 0 & \dots & 0 \\ 0 & \lambda & 1 & 0 & \dots & 0 \\ 0 & 0 & \lambda & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & 0 & \dots & \lambda \end{pmatrix}$$

A matrices de este tipo las llamaremos bloque de Jordan.

Si le aplicamos al caso general en el que  $\mu = (x - \lambda_1)^{e_1} \dots (x - \lambda_r)^{e_r}$ . Tomamos en cada  $V_{ij} = K[x]x_{ij}$  la base  $\{x_{ij}, \dots, (T - \lambda)^{e_{ij}-1}x_{ij}\}$  y obtenemos uniendo ordenadamente las bases una base de  $V$ , llámase  $B$ , tal que por bloques se expresa:

$$M_B(T) = \begin{pmatrix} J_{e_{i_1}}(\lambda_{i_1}) & 0 & 0 & 0 & \dots & 0 \\ 0 & J_{e_{i_2}}(\lambda_{i_2}) & 0 & 0 & \dots & 0 \\ 0 & 0 & J_{e_{i_3}}(\lambda_{i_3}) & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & 0 & \dots & J_{e_{i_r}}(\lambda_{i_r}) \end{pmatrix}$$

Ejemplo: Sea  $V = \mathcal{C}^\infty(\mathbb{R})^n = \bigoplus_{i=1}^n \mathcal{C}^\infty(\mathbb{R})$ ,  $B \in \mathcal{M}_n(\mathbb{R})$ ,  $y = (y_1, \dots, y_n) \in V$ . Tenemos la ecuación diferencial  $y' = yB$ .

Sea  $M = \{y \in \mathcal{C}^\infty(\mathbb{R})^n : y' = yB\}$  es un subespacio vectorial de  $V$ . Entonces  $V$  es un  $\mathbb{R}[x]$ -módulo. Sabemos que  $M$  es un submódulo ( $xy = y' = yB \in M$ ). Por análisis, sabemos que la dimensión es finita. Entonces  $M$  tiene una descomposición cíclica primaria.

Si  $x \in \mathbb{R}^n$ , tomamos  $y = xe^{tB}$  y  $y' = xe^{tB}B = yB$  donde  $e^S = \sum_{m \geq 0} \frac{1}{m!} S^m$ .

Tomamos la forma canónica de Jordan  $J$  de  $B$ . Existe una matriz  $P \in \mathcal{GL}_n(\mathbb{C})$  tal que  $PBP^{-1} = J$  con lo que:

$$e^{tB} = P^{-1}e^{tJ}P$$

Se puede calcular  $e^{tJ}$ .

Caso particular: Sea  $n = 2$ . Sea  $\mu$  el polinomio mínimo de  $B$  sobre  $\mathbb{C}$ . Tenemos tres casos.

La primera posibilidad es que  $\mu = (x - \lambda_1)(x - \lambda_2)$  o  $\mu = x - \lambda$ . En este segundo caso tomamos  $\lambda_1 = \lambda_2 = \lambda$  y en cualquiera de las dos posibilidades podemos escribir:

$$J = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$$

y por tanto

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

La otra posibilidad es que  $\mu = (x - \lambda)^2$  con  $\lambda \in \mathbb{R}$ . entonces:

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

y por tanto

$$tJ = \begin{pmatrix} t\lambda_1 & t \\ 0 & t\lambda_2 \end{pmatrix} = \begin{pmatrix} t\lambda_1 & 0 \\ 0 & t\lambda_2 \end{pmatrix} + \begin{pmatrix} 0 & t \\ 0 & 0 \end{pmatrix} = tA + tC$$

que son dos matrices que conmutan, luego:

$$e^{tJ} = e^{tA+tC} = e^{tA}e^{tC} = \begin{pmatrix} e^{t\lambda_1} & te^{t\lambda_2} \\ 0 & e^{t\lambda_2} \end{pmatrix}$$

Por último puede suceder que  $\mu = (x - z)(x - \bar{z})$  y tenemos

$$J = \begin{pmatrix} z & 0 \\ 0 & \bar{z} \end{pmatrix}$$

y por tanto

$$e^{tJ} = \begin{pmatrix} e^{tz} & 0 \\ 0 & e^{t\bar{z}} \end{pmatrix}$$

Alternativamente  $\mu = x^2 + bx + c$ , tenemos que  $\alpha = \sqrt{\frac{c-b^2}{4}}$  y  $\beta = -\frac{b}{2}$ . Tenemos que  $T : \mathbb{R}^2 \rightarrow \mathbb{R}^2$  tal que  $T(v) = vB$ . Tomamos  $v \in \mathbb{R}^2 \setminus \{0\}$  y tomamos la base:  $\mathcal{B} = \{-\beta v, (T - \alpha)v\}$ . Vamos a calcular la matriz de  $T$  respecto de esta nueva base:

$$T(-\beta v) = -\beta(T - \alpha)v - \alpha\beta v$$

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

Entonces

$$C = M_T(\mathcal{B}) = \begin{pmatrix} \alpha & -\beta \\ \beta & \alpha \end{pmatrix} = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} + \begin{pmatrix} 0 & -\beta \\ \beta & 0 \end{pmatrix} = A + B$$

que conmutan. Además existe  $Q \in \mathcal{GL}_2(\mathbb{R})$  tal que  $C = Q^{-1}BQ$ . Tenemos que:

$$e^{tC} = e^{tA+tB} = e^{tA}e^{tB} = \begin{pmatrix} e^{t\alpha} & 0 \\ 0 & e^{t\alpha} \end{pmatrix} \begin{pmatrix} \cos(\beta t) & -\sin(\beta t) \\ \sin(\beta t) & \cos(\beta t) \end{pmatrix} = \begin{pmatrix} e^{t\alpha} \cos(\beta t) & -e^{t\alpha} \sin(\beta t) \\ e^{t\alpha} \sin(\beta t) & e^{t\alpha} \cos(\beta t) \end{pmatrix}$$

Ejercicio: Tomamos la sucesión  $c_k = \cos(k\nu)$  con  $\nu \in \mathbb{R}$  fijo.

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

usando este hecho, demostrar que  $\cos((k+2)\nu) = 2\cos((k+1)\nu)\cos\nu - \cos k\nu$  para  $k \geq 0$ . Se pide buscar el polinomio mínimo de la sucesión en  $\mathbb{C}[x]$ .

## 4. Teoría de módulos

Sea  $R$  un anillo,  ${}_R M$  un módulo. Sea la familia no vacía de submódulos  $\Gamma \subseteq \mathcal{L}(M)$  entonces  $\bigcap_{N \in \Gamma} N \in \mathcal{L}(M)$ .

**Definición 33** (Submódulo generado por un conjunto  $X$ ). Si  $X$  es un subconjunto de  $M$ , el menor submódulo de  $M$  que contiene a  $X$  se llama submódulo generado por  $X$ . Lo denotaremos por  $RX$ .

**Lema 5.**

$$RX = \left\{ \sum_{x \in F} v_x x : F \subseteq X \text{ finito, } v_x \in R \right\}$$

*Demostración.*  $X \subseteq RX$  por ser el menor submódulo que contiene a  $X$ .

$$C = \left\{ \sum_{x \in F} v_x x : F \subseteq X \text{ finito}, v_x \in R \right\}$$

Entonces  $C \subseteq RX$ . Tenemos que, como  $C$  es un submódulo, se tiene que dar la igualdad. □

Si  $X = \{x_1, \dots, x_n\}$ , tenemos que  $RX = Rx_1 + \dots + Rx_n$ .

**Definición 34** (Módulo producto). Tomamos  $I \neq \emptyset$  un conjunto de índices, tal que  $i \in I$ , tomamos un módulo  $M_i$ .

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

Son tuplas, pero no ordenadas.

**Proposición 17.** *El producto de módulos es un módulo, con la suma término a término y el producto por escalares también término a término.*

**Definición 35** (Proyecciones e inclusiones canónicas). Vamos a tomar  $M_i$  y  $\prod_{i \in I} M_i$ . Definimos la inclusión canónica  $\iota_i$  mediante la aplicación que asigna  $m_i \mapsto (a_j)_{j \in I}$  dado por  $a_j = \delta_i^j m_i$ . Del mismo modo, definimos la proyección canónica  $\pi_i$  como la aplicación que asigna  $(a_j)_{j \in I} \mapsto a_i$ .

Evidentemente  $\pi_i \circ \iota_i = \text{id}$ .

**Definición 36** (Suma directa externa).

$$\bigoplus_{i \in I} M_i := \{(m_i)_{i \in I} : \text{tiene soporte finito}\}$$

En el caso de  $I$  finito  $\bigoplus_{i \in I} M_i = \prod_{i \in I} M_i$ , y en el caso general  $\bigoplus_{i \in I} M_i \subseteq \prod_{i \in I} M_i$

**Definición 37** (Suma de módulos). Definimos  $\sum_{i \in I} M_i$  como el menor submódulo que contiene a cualquier  $M_i$  o equivalentemente:

$$\sum_{i \in I} M_i = \left\{ \sum_{i \in F} m_i : F \subseteq I \text{ finito} \right\}$$

**Proposición 18** (Relación entre sumas). *Tomamos  $\theta : \bigoplus M_i \longrightarrow \sum M_i$  tal que  $\theta((m_i)_{i \in I}) = \sum_{i \in I} m_i$  es un homomorfismo sobreyectivo de  $R$ -módulos.*

*Para  $\{N_i : i \in I\} \subseteq \mathcal{L}(M)$ , son equivalentes:*

1. Para todo  $j \in I$ ,  $N_j \cap \sum_{i \in I \setminus \{j\}} N_i = \{0\}$ .
2. Para todo  $F \subseteq I$  finito, y para todo  $j \in F$ ,  $N_j \cap \sum_{i \in F \setminus \{j\}} N_i = \{0\}$ .
3. Si  $0 = \sum_{i \in I} m_i$  con  $m_i \in M_i$  para todo  $i \in I$ , entonces  $m_i = 0$  para todo  $i \in I$ .
4.  $\theta$  es inyectivo y por tanto un isomorfismo.
5. Para cada par  $J_1, J_2 \subseteq I$  con  $J_1 \cap J_2 = \emptyset$ , se tiene que  $(\sum_{i \in J_1} N_i) \cap (\sum_{i \in J_2} N_i) = \{0\}$

**Definición 38.** En caso de satisfacerse cualquiera de las condiciones anteriores equivalentes, diremos que la suma  $\sum_{i \in I} N_i$  es una suma directa interna, que notaremos por  $\dot{+}_{i \in I} N_i$ .

**Corolario 9.** Si la familia  $\{N_i : i \in I\} \subseteq \mathcal{L}(M)$  verifican las condiciones y  $N \in \mathcal{L}(M)$  tal que  $N \cap \dot{+}_{i \in I} N_i = \{0\}$ , entonces  $\{N_i : i \in I\} \cup \{N\}$ .

**Definición 39** (Independencia). Si la familia  $\{N_i : i \in I\}$  donde cada módulo es distinto de 0 y satisface alguna de las condiciones anteriores equivalente, entonces diremos que dicha familia es independiente.

Caso particular: El módulo regular  $M_i = R$ , llamamos:

$$R^{(I)} = \bigoplus_{i \in I} M_i = \{(r_i)_{i \in I} \in R^I : \text{con soporte finito}\}$$

**Definición 40.**  $A$  es un DIP,  ${}_A M$  módulo.

$$t(M) = \{m \in M : \text{ann}_A(m) \neq \langle 0 \rangle\}$$

es un submódulo de  $M$ , que se llama submódulo de torsión de  $M$ .

Ejemplo: sea  $A$  un DIP, sea  ${}_A M$  un módulo y consideramos su submódulo de torsión.

Supongamos que  $t(M) \neq \{0\}$ . Definimos  $P$  como el conjunto de representantes de las clases de equivalencia, bajo la relación ser asociados, de los irreducibles de  $A$ .

Sea  $p \in P$ , tomamos  $M_p = \{m \in M : p^e m = 0 \text{ para algún } e \geq 1\}$ . Tenemos que  $M_p \subseteq t(M)$ ,  $M_p$  es un submódulo. Entonces:

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

Demostremos esto.

Tomemos un  $m \in t(M)$ ,  $Am$  es un módulo de longitud finita.

$$Am = N_1 \dot{+} \cdots \dot{+} N_r$$

donde  $N_i$  es una componente  $p_i$ -primaria.

En particular,  $m = m_1 + \cdots + m_r$  de manera que  $m_i \in N_i \subseteq M_{p_i}$ .

Luego  $M = \sum_{p \in P} M_p$ . La unicidad es sencilla de deducir: cada  $m$  estará en una componente primaria.

Caso particular. Tomamos  $M = \mathcal{C}^\infty(\mathbb{R})$ ,  $M$  es un  $\mathbb{R}[x]$ -módulo si  $xf = f'$ . Entonces  $t(M)$  es el conjunto de las funciones que satisfacen una EDO con coeficientes constantes.

$P = \{ \text{Polinomios mónicos o bien lineales o bien cuadráticos irreducibles} \}$ . Es decir, cualquier función que se puede definir mediante una EDO lineal con coeficientes constantes se puede escribir como suma de funciones que resuelven  $(\alpha \frac{d^2}{dx^2} + \beta \frac{d}{dx} + \gamma)^e f = 0$  con  $e \in \mathbb{N}$ .

Como hemos visto en ese caso particular,  $M_p$  no tiene por qué tener longitud finita.

Consideremos  $I$  un conjunto infinito y  $R^{(I)}$  tal y como lo hemos definido antes.

**Lema 6.** *Si  $M$  es un  $R$  módulo, existe una sucesión exacta de la forma*

$$0 \longrightarrow L \longrightarrow R^{(I)} \longrightarrow M \longrightarrow 0$$

para  $I$  adecuado.

*Demostración.* Tomo  $\{m_i : i \in I\}$  tal que  $M = \sum_{i \in I} Rm_i$ . Definimos  $\varphi : R^{(I)} \longrightarrow M$  dada por  $\varphi((r_i)_{i \in I}) = \sum_{i \in I} r_i m_i$ .

$$L = \ker \varphi \xrightarrow{\iota} M.$$

□

**Lema 7** (Existencia de bases). *Para  $\{m_i : i \in I\} \subseteq M$ , son equivalentes:*

1.  $\sum_{i \in I} r_i m_i = 0$  implica que  $r_i = 0$  para todo índice.
2. El homomorfismo  $\varphi : R^{(I)} \longrightarrow M$  con  $\varphi((r_i)_{i \in I}) = \sum_i r_i m_i$  es inyectiva.

*Si se satisface 1, diremos que el conjunto  $\{m_i : i \in I\}$  es linealmente independiente. Si además estos elementos son además un conjunto de generadores, diremos que forman una base.*

La demostración es trivial.

*Observación 11.*  $M$  tiene una base si y solo si  $M \cong R^I$  para algún  $I$ .

**Definición 41** (Módulo libre). Un módulo se llama libre si admite una base.

*Observación 12.* Advertencia: hay muchos módulos que no son libres.

Ejemplos de módulos no libres:

1. Ningún grupo abeliano finito es libre como  $\mathbb{Z}$  módulo.
2.  $t(M)$ ,  ${}_A M$  con  $A$  un DIP, nunca es libre. En otras palabras  $A^{(I)}$  no es nunca un módulo de torsión (por ser un dominio de integridad).

## 4.1. Presentaciones de módulos

**Proposición 19** (Módulo presentado). *Sea  $M$  un módulo. Existe una sucesión exacta*

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

donde  $F_{-n}$  es libre para todo  $n \in \mathbb{N}$ . Esa sucesión se llama resolución libre de  $M$ .

*Demostración.* Tomo un conjunto de generadores de  $M$ , y tomo un homomorfismo de módulos sobreyectivo  $F_0 \xrightarrow{p_0} M$ .

$$F_{-1} \xrightarrow{p_{-1}} K_0 \xrightarrow{\iota} F_0 \xrightarrow{p_0} M \longrightarrow 0$$

y reiteramos el proceso.

Exactitud vista en  $F_{-1}$  ya que otro caso sería análogo.  $\ker f_{-1} =: K_{-1} = \text{Im } p_{-2} = \text{Im } f_{-2}$ .

La resolución puede pero no tiene por qué ser finita.

□

**Definición 42** (Módulo finitamente presentado).  $M$  se dice finitamente presentado si existe un presentación finita que no es sino una sucesión exacta de la forma

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

Ejercicio: dar una presentación finita del  $\mathbb{Z}$ -módulo  $\mathbb{Z}_2 \oplus \mathbb{Z}_4$ .

**Proposición 20.** *Un anillo  $R$  es noetheriano a izquierda si y solo si todo módulo finitamente generado es finitamente presentado.*

*Demostración.* Veamos solo una implicación: que si  ${}_R R$  es noetheriano entonces que submódulo finitamente generado es finitamente presentado.

Como  $M$  es finitamente generado,  $K_0$  es finitamente generado  $F_{-1} \xrightarrow{p_{-1}} K_0 \xrightarrow{\iota} F_0 \xrightarrow{f_0} M \longrightarrow 0$ .

□



Tenemos que  $M \cong F_0 / \text{Im } f_{-1}$ . Tomemos  $E_s, F_t$  módulos libres con bases finitas de cardinales  $s$  y  $t$  respectivamente. Diremos que  $E_s$  tiene rango  $s$  (a pesar de que no es una invariante del módulo, problema de la base de número invariante o INB, incluso se puede dar  $R \cong R \oplus R$ ). Llamamos  $e = \{e_1, \dots, e_s\}$  base de  $E_s$ , y  $f = \{f_1, \dots, f_t\}$  base de  $F_t$ . Sea  $\psi : E_s \rightarrow F_t$ , definido por  $\psi(e_i) = \sum_{j=1}^t a_{ij} f_j$ . Definimos la matriz  $A_\psi = (a_{ij})_{1 \leq i \leq s, 1 \leq j \leq t} \in \mathcal{M}_{s \times t}(R)$ .

Dado  $u = \sum_{i=1}^s x_i e_i$ ,  $x_i \in R$ . Entonces

$$\psi(u) = \sum_{j=1}^t y_j f_j$$

Resulta que si  $u_e = x = (x_1, \dots, x_s)$  y  $y = (y_1, \dots, y_t)$ , tenemos que  $y = x A_\psi$  y por tanto  $\psi(u)_f = u_e A_\psi$ .

Tenemos que  $(\cdot) A_\psi \circ (\cdot)_e = (\cdot)_f \circ \psi$ .

Sean  $E_s \xrightarrow{\psi} F_t \xrightarrow{\varphi} G_r$ , entonces  $A_{\varphi \circ \psi} = A_\varphi A_\psi$ .

Ejemplo: Sea  $T : V \rightarrow V$  un endomorfismo de espacios vectoriales, y  $V$  de dimensión finita.  $_{K[x]}V$  es un módulo finitamente presentado. Buscamos una presentación finita.

Ejemplo:  $T : V \rightarrow V$  aplicación  $K$ -lineal,  $n = \dim_K(V) < \infty$ . Queremos una presentación libre finita de  $_{K[x]}V$ . Tomo una  $K$ -base (base como espacio vectorial)  $\{v_1, \dots, v_n\}$  de  $V$ .

Tenemos que

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

donde  $(b_{ij}) \in \mathcal{M}_n(K)$  es la matriz asociada a  $T$ . Tomo  $F_n$  un  $K[x]$ -módulo libre con base  $\{f_1, \dots, f_n\}$  y  $\phi : F_n \rightarrow V$  tal que  $\phi(f_i) = v_i$  para todo  $i \in \{1, \dots, n\}$ .  $\phi$  es un homomorfismo de  $K[x]$ -módulos sobreyectivo.

Tenemos que  $F_n \xrightarrow{\phi} V \rightarrow 0$ . Tomamos  $Xf_i - \sum_{j=1}^n b_{ij} f_j \in \ker \phi$ .

Afirmamos que  $\{Xf_i - \sum_{j=1}^n b_{ij} f_j : i \in \{1, \dots, n\}\}$  es un conjunto de generadores de  $\ker \phi$ .

Tomemos  $x \in F_n$ , tenemos que  $x = \sum_{i=1}^n p_i(x) f_i$ . Supongamos que  $x \neq 0$ , definimos el peso como  $w(x) := \sum_{i=1}^n \text{gr}(p_i) \geq 0$ .

Observemos que  $w(x) = 0$  es solo posible si  $p_i \in K$  para todo  $i$ . Si  $w(x) = 0$ , entonces  $x = \sum_{i=1}^n p_i f_i$ . Entonces aplicando  $\phi$  tenemos  $0 = \sum_{i=1}^n p_i v_i$ , y por tanto  $x = 0$  lo que es una contradicción.

Así que si  $x \in \ker \phi \setminus \{0\}$ ,  $w(x) \geq 1$ .

Vamos a aplicar inducción sobre  $w(x)$ .  $w(x) = 1$ . Entonces existe un único índice  $k \in \{1, \dots, n\}$  tal que  $p_k$  no es constante y además  $p_k = aX + b$  con

$a, b \in K$ .

$$\begin{aligned} x &= \sum_{i \neq k} p_i f_i + (aX + b)f_k \\ &= \sum_{i \neq k} p_i f_i + a(Xf_k - \sum_j b_{kj} f_j) + a \sum_j b_{kj} f_j + bf_k \end{aligned}$$

Luego

$$\sum_{i \neq k} p_i f_i + a \sum_j b_{kj} f_j + bf_k \in \ker \phi$$

donde como son todos constantes, se tiene

$$\sum_{i \neq k} p_i f_i + a \sum_j b_{kj} f_j + bf_k = 0$$

y por tanto  $x = a(Xf_k - \sum_j b_{kj} f_j)$ .

Supongamos  $w(x) > 1$ . Existe algún  $k \in \{1, \dots, n\}$  para el que  $\text{gr}(p_k) \geq 1$ . Así,  $p_k = q(X)X + b$ , con  $\text{gr}(q) = \text{gr}(p_k) - 1$  y  $b \in K$ .

$$x = \sum_{i \neq k} p_i f_i + q(X)(Xf_k - \sum_j b_{kj} f_j) + q(X) \sum_j b_{kj} f_j + bf_k$$

Tenemos que  $y = \sum_{i \neq k} p_i f_i + q(X) \sum_j b_{kj} f_j + bf_k \in \ker \phi$  y  $w(y) \leq w(x) - 1 < w(x)$ . Por inducción, sabemos que  $y = \sum_i q_i(Xf_i - \sum_j b_{ij} f_j)$ , y tenemos:

$$x = q(X)(Xf_k - \sum_j b_{kj} f_j) + \sum_i q_i(Xf_i - \sum_j b_{ij} f_j)$$

con lo que se demuestra el enunciado, sacando factor común lo que haga falta y redondeando.

Definimos

$$F_n \xrightarrow{\psi} F_n \xrightarrow{\phi} V \longrightarrow 0$$

que es una representación libre finita, donde

$$\psi(f_i) = Xf_i - \sum_j b_{ij} f_j$$

Con lo que la matriz nos queda:

$$A_\psi = \begin{pmatrix} X - b_{11} & -b_{12} & \cdots & -b_{1n} \\ -b_{21} & X - b_{22} & \cdots & -b_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ -b_{n1} & -b_{n2} & \cdots & X - b_{nn} \end{pmatrix} \in \mathcal{M}_n(K[x])$$

o si se quiere,  $A_\psi = XI - A_T$  con  $A_T = (b_{ij})$ .

**Lema 8.** Sea  $F$  un  $R$ -módulo libre y  $\varphi : M \longrightarrow N$  un epimorfismo de  $R$ -módulos. Para cada homomorfismo de  $R$ -módulos  $\alpha : F \longrightarrow N$  existe un homomorfismo de  $R$ -módulos  $\beta : F \longrightarrow M$  tal que  $\varphi \circ \beta = \alpha$ . Es decir,  $\alpha$  se levanta como homomorfismo a  $M$ .

*Demostración.* Tomo en  $F$  una base  $\{e_i : i \in I\}$ . Como  $\varphi$  es sobreyectivo para cada  $\alpha(e_i)$  existe un  $m_i \in M$  tal que  $\varphi(m_i) = \alpha(e_i)$ . Ahora tenemos  $\beta$  dado por  $\beta(e_i) = m_i$ .

□

Sean  ${}_R M$  y  ${}_R N$  finitamente presentados y  $h : M \longrightarrow N$  homomorfismo de  $R$ -módulos.

$$\begin{aligned} E_s &\xrightarrow{\psi} F_t \xrightarrow{\phi} M \longrightarrow 0 \\ E_{s'} &\xrightarrow{\psi'} F_{t'} \xrightarrow{\phi'} N \longrightarrow 0 \end{aligned}$$

Por el lema anterior, existe un  $q$  tal que  $\phi' \circ q = h \circ \phi$ . Observemos que  $\text{Im } q \circ \psi \subseteq \ker \phi' = \text{Im } \psi'$ . Aplicando el lema sobre la imagen de  $\psi'$ , existe un  $p$  tal que  $\psi' \circ p = q \circ \psi$ . Donde  $p : E_s \longrightarrow E_{s'}$  y  $q : F_t \longrightarrow F_{t'}$ .

Supongamos ahora que tenemos que existen  $p$  y  $q$  tales que  $q\psi = \psi'p$ . Vamos a construir un  $h$  homomorfismo. Tomamos  $u \in F_t$  tal que  $\phi(u) = m$ . Queremos definir  $h(m)$  como  $\phi'(q(u)) \in N$ . Hay que demostrar que está bien definida.

Tomamos  $v \in F_t$ , tal que  $\phi(v) = m$ . Tenemos que:

$$\phi'(q(v) - q(u)) = \phi'(q(u - v))$$

tomando un  $x \in E_s$  tal que  $v - u = \psi(x)$ , ya que  $0 = \phi(v - u) \in \ker \phi = \text{Im } \psi$ .

$$\phi'(q(v) - q(u)) = \phi'(q(u - v)) = \phi'(q(\psi(x))) = \phi'(\psi'(p(x))) = 0$$

y entonces  $h$  no depende del representante elegido. Es fácil ver que  $h$  es un homomorfismo de módulos y que  $\phi \circ h = q \circ \phi'$ .

Fijadas bases en  $E_s, F_t, E_{s'}, F_{t'}$ , definir  $h$  se reduce a dar dos matrices  $A_q$  y  $A_p$  tales que

$$A_\psi A_q = A_p A_{\psi'}$$

entonces  $A_\psi, A_{\psi'}$  representan a los módulos  $M$  y  $N$  y  $A_q, A_p$  representan al homomorfismo  $h$ .

Concretamente, si  $f = \{f_1, \dots, f_t\}$  es una base de  $F_t$  y  $f' = \{f'_1, \dots, f'_{t'}\}$  de  $F_{t'}$  y  $A_q = (q_{ij})$  y tomamos  $m_i = \phi(f_i)$  y  $n_j = \phi'(f'_j)$ , tenemos:

1.  $\{m_1, \dots, m_t\}$  genera  $M$ .
2.  $\{n_1, \dots, n_{t'}\}$  genera  $N$ .

$$3. h(m_i) = \sum_{j=1}^{t'} q_{ij} n_j.$$

**Proposición 21** (Teorema de Cayley-Hamilton). *Sea  $T : V \longrightarrow V$  un homomorfismo  $K$ -lineal, con la dimensión de  $V$  finita. Sea  $d \in K[x]$  el polinomio característico de  $T$ . Entonces el polinomio mínimo de  $T$  divide a  $d(x)$ . En particular,  $d(T) = 0$ .*

*Demostración.* Tomamos la presentación finita de  ${}_{K[x]}V$  que vimos anteriormente:

$$F_n \xrightarrow{\psi} F_n \xrightarrow{\phi} V \longrightarrow 0$$

Tomamos  $A_\psi$  y  $P$  su matriz adjunta (o de cofactores), o sea, la que hace que se cumpla la ecuación  $PA_\psi = d(x)I$ .

Sea  $\delta : F_n \longrightarrow F_n$  el homomorfismo que fijada bases  $f$  de  $F_n$  tiene como matriz  $d(x)I$ , o sea,  $\delta(f_i) = d(x)f_i$ . Consideramos la proyección canónica  $\pi : F_n \longrightarrow F_n / \text{Im } \delta$  y nos queda:

$$F_n \xrightarrow{\delta} F_n \xrightarrow{\pi} F_n / \text{Im } \delta \longrightarrow 0$$

Tomando  $p$  la aplicación tal que  $A_p = P$  y  $q = \text{id}$ , de aquí obtenemos que  $\psi_p = \text{id} \circ \delta$ , con lo que se induce  $h$ , un homomorfismo de módulos sobreyectivo ( $h \circ \pi = \phi$ ).

$$\text{Ann}_{K[x]}(V) \supseteq \text{Ann}_{K[x]}(F_n / \text{Im } \delta) = \langle \delta(x) \rangle$$

donde la última igualdad viene de que  $F_n / \text{Im } \delta \cong \bigoplus_{i=1}^n K[x]f_i / K[x]d(x)f_i \cong \bigoplus_{i=1}^n K[x] / \langle d(x) \rangle$ .

Por tanto, el polinomio mínimo de  $T$  (que es el anulador de  $V$ ), divide a  $d(x)$ . Como al evaluar en  $T$  el polinomio mínimo se anula, tenemos que el polinomio característico se anula también. □

**Definición 43** (Matriz quasidiagonal). Sea  $A = (a_{ij}) \in \mathcal{M}_{s \times t}(R)$ . Diremos que  $A$  es quasidiagonal si  $a_{ij} = 0$  para todo  $i \neq j$ . Usaremos  $d_i = a_{ii}$  para  $i = 1, \dots, m$  con  $m = \min\{s, t\}$ . La notación

$$A = \text{diag}_{s \times t}(d_1, \dots, d_m)$$

Ejemplos:

$$\text{diag}_{3 \times 2}(1, 3) = \begin{pmatrix} 1 & 0 \\ 0 & 3 \\ 0 & 0 \end{pmatrix}$$

$$\text{diag}_{2 \times 3}(1, 3) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \end{pmatrix}$$

**Notación.** Denotaremos  $GL_n(R)$  al grupo de unidades de  $\mathcal{M}_n(R)$ : es decir, las matrices  $Q$  tales que existe otra matriz  $Q^{-1}$  que cumpla  $QQ^{-1} = Q^{-1}Q = I_n$ .

**Proposición 22.** Sea la presentación finita:

$$E_s \xrightarrow{\psi} F_t \xrightarrow{\phi} M \longrightarrow 0$$

de  ${}_R M$ . Supongamos que existen  $P \in GL_s(R)$ ,  $Q \in GL_t(R)$  y  $D = \text{diag}_{s \times t}(d_1, \dots, d_m)$  tales que  $PA_\psi = DQ$ . Si  $\{m_1, \dots, m_t\}$  es el conjunto de generadores de  $M$  y tales que  $m_i = \phi(f_i)$  con

$$x_i = \sum_{j=1}^t q_{ij}m_j$$

entonces  $M = \dot{+}_{i=1}^t Rx_i$  y  $\text{ann}_R(x_i) = Rd_i$  si  $i \leq m$  y  $\text{ann}_R(x_i) = \{0\}$  si  $i > m$  si se da el caso.

*Demostración.* Tomemos otra presentación:

$$E_s \xrightarrow{\psi_1} F_t \xrightarrow{\phi_1} M \longrightarrow 0$$

Tomemos  $\text{id} : M \longrightarrow M$  y dos homomorfismos  $p : E_s \longrightarrow E_s$  y  $q : F_t \longrightarrow F_t$ , tales que  $A_p = P$ ,  $A_q = Q$  y  $A_\psi = D$  y que conmuten todas las aplicaciones.

Para que conmuten, definimos  $\phi_1 = \phi \circ q$ , con lo que  $\phi_1(f_i) = \phi(q(f_i)) = \sum_{j=1}^t q_{ij}m_j = x_i$ .

La condición de matrices  $PA_\psi = DQ$  garantiza que  $\psi \circ p = q \circ A_\psi$ .

Hay que comprobar que la sucesión que nos hemos inventado es exacta en  $F_t$ . Para demostrarlo, usamos que  $P$  y  $Q$  son inversibles:  $p, q$  son isomorfismos y podemos recuperar la exactitud de la sucesión del enunciado.

$$M = Rx_1 + \dots + Rx_t$$

porque  $x_i = \phi_1(f_i)$  y  $\phi_1$  es sobreyectiva. Para ver que es directa, tomamos el  $0 = r_1x_1 + \dots + r_tx_t$ . Hay que ver que cada  $r_ix_i = 0$ .

$$0 = \phi_1(r_1f_1 + \dots + r_tf_t) \implies r_1f_1 + \dots + r_tf_t \in \ker \phi_1 = \text{Im } \psi_1$$

Por otro lado,  $\text{Im } \psi_1 = R\psi_1(e_1) + \dots + R\psi_1(e_s)$ . Ahora bien,  $A_{\psi_1} = D$ , con lo que  $\text{Im } \psi_1 = Rd_1f_1 + \dots + Rd_mf_m$ . Tenemos que esos módulos son independientes y la suma es directa:  $\text{Im } \psi_1 = Rd_1f_1 \dot{+} \dots \dot{+} Rd_mf_m$ . Entonces  $r_i \in Rd_i$  para  $i \leq m$ , y si  $t > m$ , entonces  $r_i = 0$  para  $i > m$ .

Así, cada  $r_i f_i = s_i d_i f_i$ . Tomamos  $r_1 x_i \phi_1(r_i f_i)$ , tenemos que  $r_i f_i \in \text{Im } \psi_1 = \ker \phi_1$ , luego  $r_i x_i = 0$ . Luego:

$$M = Rx_1 \dot{+} \cdots \dot{+} Rx_t$$

Se deduce también que  $\text{ann}_R(x_i) \supseteq Rd_i$ .

$$\begin{aligned} M &\cong F_t / \text{Im } \psi_1 = (Rf_1 \dot{+} \cdots \dot{+} Rf_t) / (Rd_1 f_1 \dot{+} \cdots \dot{+} Rd_m f_m) \\ &\cong Rf_1 / Rd_1 f_1 \oplus \cdots \oplus Rf_m / Rd_m f_m \oplus R / \{0\} \oplus \overset{(t-m)}{\cdots} \oplus R / \{0\} \\ &\cong Rf_1 / Rd_1 \oplus \cdots \oplus R / Rd_m \oplus R \oplus \overset{(t-m)}{\cdots} \oplus R \end{aligned}$$

□

Caso particular:  $R = \mathbb{Z}$ . Aquí siempre podemos calcular P y Q. Si  $M$  es un grupo abeliano finitamente generado como  $\mathbb{Z}$ -módulo, entonces existen  $d_1, \dots, d_m \in \mathbb{N}$  tales que

$$M \cong \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_m} \oplus \mathbb{Z}^{t-m}$$

si  $t > m$  y en otro caso:

$$M \cong \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_m}$$

Es la suma de una parte de torsión y una libre de torsión.

¿Es posible encontrar  $P, Q$  cuadradas inversibles tales que  $PA_\psi Q^{-1}$  sea una matriz quasidiagonal?

**Definición 44** (Matrices y operaciones elementales).  $E_{ij} \in \mathcal{M}_n(R)$  definida por su única entrada no nula es la  $(i, j)$ -ésima, que vale 1. Se verifica:

$$E_{ij} = \begin{cases} E_{ie}, & \text{si } j = k \\ 0, & \text{si } j \neq k \end{cases}$$

Para cualquier matriz  $B$  de entradas  $b_{ij}$ , se puede escribir:

$$B = \sum_{i,j} b_{ij} E_{ij} = \sum_{i,j} E_{ij} b_{ij}$$

Sea  $A$  una matriz rectangular de tamaño adecuado,  $r \in R, u \in \mathcal{U}(R)$ .

$$(E_{ij}A)_{rs} = \begin{cases} a_{is}, & \text{si } r = j \\ 0, & \text{si } r \neq j \end{cases}$$

La matriz  $I + rE_{ij}$  es inversible para  $i \neq j$ . (multiplicando por  $I - rE_{ij}$  sale).

La matriz  $I + E_{ij} + E_{ji} - E_{ii} - E_{jj}$  es inversible para  $i \neq j$ , pues al cuadrado es la identidad.

La matriz  $I + (u - 1)E_{ii}$  es inversible, se prueba multiplicando por  $I + (u^{-1} - 1)E_{ii}$ .

A las siguientes matrices las llamamos matrices elementales:

1.  $I + rE_{ij}$  (multiplicar por un escalar una fila o columna y sumársela a otra).
2.  $I + E_{ij} + E_{ji} - E_{ii} - E_{jj}$  (intercambiar sus filas o columnas).
3.  $I + (u - 1)E_{ii}$  (multiplicar una fila o columna por una unidad).

es un grupo.

Ejemplo: Sea  $M$  un grupo aditivo generado por  $\{m_1, m_2, m_3\}$  sujeto a las relaciones:

1.  $2m_1 + m_2 - m_3 = 0$
2.  $4m_1 + m_2 - 3m_3 = 0$

Tomamos  $\mathbb{Z}$ -módulos libres  $F_3$  con bases  $\{f_1, f_2, f_3\}$  y  $E_2$  con bases  $\{e_1, e_2\}$ .

$$F_3 \xrightarrow{\psi} F_3 \xrightarrow{\phi} M \longrightarrow 0$$

Definimos  $\phi(f_i) = m_i$  y

$$A_\psi = \begin{pmatrix} 2 & 1 & -1 \\ 4 & 1 & -3 \end{pmatrix}$$

Solo apuntamos las operaciones por columnas porque solo nos interesa la matriz  $Q$ . Para tener una sencilla, vamos a hacer el máximo número de matrices por filas.

$$\begin{pmatrix} 2 & 1 & -1 \\ 4 & 1 & -3 \end{pmatrix} \sim \begin{pmatrix} 2 & 1 & -1 \\ 0 & -1 & -1 \end{pmatrix} \sim$$

Ahora comenzamos a hacer operaciones por columnas, anotándolas:

$$\begin{pmatrix} 2 & 0 & -2 \\ 0 & -1 & -1 \end{pmatrix} \underset{c_3+c_2}{\sim} \begin{pmatrix} 2 & 0 & -2 \\ 0 & -1 & 0 \end{pmatrix} \underset{c_3-c_1}{\sim} \begin{pmatrix} 2 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}$$

Tenemos que

$$D = \begin{pmatrix} 2 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}$$

y que

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \underset{c_3-c_1}{\sim} \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \underset{c_3-c_2}{\sim} \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = Q$$

$$x_1 = \sum_{j=1}^t q_{ij} m_j = m_1 - m_3$$

$$x_2 = \sum_{j=1}^t q_{ij} m_j = m_2 + m_3$$

$$x_3 = \sum_{j=1}^t q_{ij} m_j = m_3$$

$$M = \mathbb{Z}x_1 \dot{+} \mathbb{Z}x_2 \dot{+} \mathbb{Z}x_3 \dot{+}$$

$$\text{ann}_{\mathbb{Z}}(x_1) = 2\mathbb{Z}$$

$$\text{ann}_{\mathbb{Z}}(x_2) = -1\mathbb{Z}$$

$$\text{ann}_{\mathbb{Z}}(x_3) = \langle 0 \rangle$$

Con lo que

$$M = \mathbb{Z}x_1 \dot{+} \mathbb{Z}x_3 \dot{+} \cong \mathbb{Z}_2 \oplus \mathbb{Z}$$

Ejemplo: Sea  $K$  un cuerpo,  $T : V \longrightarrow V$ , con  $\dim_K V = 3$ ,  $\{v_1, v_2, v_3\}$  es una base de  $V$ .

Sea

$$B = \begin{pmatrix} 1 & -1 & -1 \\ -1 & 1 & -1 \\ -1 & -1 & 1 \end{pmatrix}$$

la matriz de  $T$  en dicha base. Obtengamos la descomposición cíclica primaria de  ${}_{K[x]}V$ .

Tenemos para

$$A = A_\psi = \begin{pmatrix} x-1 & 1 & -1 \\ 1 & x+1 & -1 \\ 1 & -1 & x-1 \end{pmatrix} \in \mathcal{M}(K[x])$$

Busquemos  $P, Q$  y  $D$ .  $v_i = \varphi(f_i)$ . Al final obtendremos  $PAQ^{-1} = D$ .

Partimos de  $A$  y hacemos operaciones por filas:

$$A = \begin{pmatrix} x-1 & 1 & -1 \\ 1 & x+1 & -1 \\ 1 & -1 & x-1 \end{pmatrix} \sim$$



(colocamos el polinomio de menor grado como pivote)

$$\begin{pmatrix} 1 & -1 & x-1 \\ 1 & x+1 & -1 \\ x-1 & 1 & -1 \end{pmatrix} \sim \begin{pmatrix} 1 & -1 & x-1 \\ 0 & x+2 & -x \\ 0 & x & -x^2-2x-2 \end{pmatrix} \sim$$

(Suponiendo que el cuerpo tiene característica distinta de 2)

$$\begin{pmatrix} 1 & -1 & x-1 \\ 0 & 2 & x^2-3x+2 \\ 0 & x+2 & -x \end{pmatrix} \sim \begin{pmatrix} 1 & -1 & x-1 \\ 0 & 2 & x^2-3x+2 \\ 0 & x+2 & -x \end{pmatrix} \sim$$

$$\begin{pmatrix} 1 & -1 & x-1 \\ 0 & 2 & x^2-3x+2 \\ 0 & 0 & -\frac{1}{2}x^3+\frac{1}{2}x^2+x-2 \end{pmatrix} \sim \begin{pmatrix} 1 & -1 & x-1 \\ 0 & 2 & x^2-3x+2 \\ 0 & 0 & x^3-x^2-2x+4 \end{pmatrix}$$

Empezamos con las operaciones por columnas

$$\begin{pmatrix} 1 & -1 & x-1 \\ 0 & 2 & x^2-3x+2 \\ 0 & 0 & x^3-x^2-2x+4 \end{pmatrix} \xrightarrow{c_2+c_1} \begin{pmatrix} 1 & 0 & x-1 \\ 0 & 2 & x^2-3x+2 \\ 0 & 0 & x^3-x^2-2x+4 \end{pmatrix} \xrightarrow{c_3-(x-1)c_1}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & x^2-3x+2 \\ 0 & 0 & x^3-x^2-2x+4 \end{pmatrix} \xrightarrow{c_3-(\frac{1}{2})(x^2-3x+2)c_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & x^3-x^2-2x+4 \end{pmatrix} = D$$

Calculamos ahora  $Q$ :

$$Q = \begin{pmatrix} 1 & 1 & x \\ 0 & 1 & \frac{1}{2}(x^2-3x+2) \\ 0 & 0 & 1 \end{pmatrix}$$

Quiero encontrar  $x_1, x_2, x_3$  tales que  ${}_{K[x]}V = K[x]x_1 + K[x]x_2 + K[x]x_3$ .

Tenemos que  $\text{ann}_{K[x]}(x_1) = K[x]$ ,  $\text{ann}_{K[x]}(x_2) = 2K[x] = K[x]$  y  $\text{ann}_{K[x]}(x_3) = \langle x^3 - x^2 - 2x + 4 \rangle$ . Con esto,  $x_1 = x_2 = 0$  y por tanto

$${}_{K[x]}V = K[x]v_3$$

donde la última igualdad es porque  $q_{33} = 1$ .

Es cíclica primaria si  $x^3 - x^2 - 2x + 4$  es una potencia del irreducible. Vamos a estudiar según quien sea el cuerpo  $K$ , al menos en un par de casos.

Caso particular  $K = \mathbb{Q}$ : Probando con  $\pm 1, \pm 2, \pm 4$  vemos que no tiene raíces en  $\mathbb{Q}$ . Por tanto, como el grado es 3,  $\mu = x^3 - x^2 - 2x + 4$  es el polinomio mínimo y es irreducible.

$${}_{\mathbb{Q}[x]}V = \mathbb{Q}[x]v_3$$

es la descomposición cíclica primaria. Además,  $_{\mathbb{Q}[x]}V$  es simple, al ser  $\mu$  maximal y  $\mathbb{Q}[x]v_3 \cong \mathbb{Q}[x]/\langle \mu \rangle$ .

Sobre  $\mathbb{Q}$  la matriz tomando la base  $\{v_3, T(v_3), T^2(v_3)\}$ :

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -4 & 2 & 1 \end{pmatrix}$$

Caso particular  $K = \mathbb{R}$ : Por análisis, al ser grado impar, existe al menos una raíz real.  $\mu'(x) = 3x^2 - 2x - 2$ , que tiene como raíces  $\frac{1 \pm \sqrt{7}}{3}$  y tenemos una parábola con coeficiente líder positivo. Luego hay 1 raíces o 3 si los máximos y mínimos son positivos o negativos:  $\mu(\frac{1+\sqrt{7}}{3}) > 0$  luego  $\mu$  tiene una única raíz en  $\mathbb{R}$ .

Tenemos que, si  $\alpha$  es la raíz real y  $z \in \mathbb{C} \setminus \mathbb{R}$ ,  $\mu = (x - \alpha)(x - z)(z - \bar{z}) = (x - \alpha)(x^2 - 2\operatorname{Re}(z)x + |z|^2)$  en  $\mathbb{R}[x]$ .

La descomposición cíclica primaria se consigue mediante el siguiente procedimiento. Sea  $u_1 = (x - \alpha)v_3 = (T - \alpha)v_3$ .  $\operatorname{ann}_{\mathbb{R}[x]} u_1 = \langle x^2 - 2\operatorname{Re}(z)x + |z|^2 \rangle$  y sea  $u_2 = (x^2 - 2\operatorname{Re}(z)x + |z|^2)v_3 = (T^2 - 2\operatorname{Re}(z)T + |z|^2)v_3$ .  $\operatorname{ann}_{\mathbb{R}[x]} u_1 = \langle (x - \alpha) \rangle$ .

La descomposición cíclica primaria queda:

$$_{\mathbb{R}[x]}V = \mathbb{R}[x]u_1 \dot{+} \mathbb{R}[x]u_2$$

Tomamos la base de  $V$  dada por  $\{u_1, T(u_1), u_2\}$ . La matriz de  $T$  con respecto de esa base por filas es:

$$\begin{pmatrix} 0 & 1 & 0 \\ -|z|^2 & 2\operatorname{Re}(z) & 0 \\ 0 & 0 & \alpha \end{pmatrix}$$

donde hemos usado que  $T^2(u_1) = 2\operatorname{Re}(z)T(u_1) - |z|^2u_1$  y que  $T(u_2) = \alpha u_2$ . Como vemos es diagonal por bloques.

Caso particular,  $K = \mathbb{C}$ . Al ser algebraicamente cerrado,  $\mu = (x - \alpha)(x - z)(x - \bar{z})$  donde  $x \in \mathbb{R}$  y  $z \in \mathbb{C} \setminus \mathbb{R}$ .

$$_{\mathbb{C}[x]}V = \mathbb{C}[x]u_1 \dot{+} \mathbb{C}[x]u_2$$

Pero podemos dividir  $\mathbb{R}[x]u_1$  aún más. Llamamos  $x_1 = (x - z)u_1$ ,  $\operatorname{ann}_{\mathbb{C}[x]}(x_1) = \langle x - \bar{z} \rangle$  y  $\operatorname{ann}_{\mathbb{C}[x]}(x_2) = \langle x - z \rangle$ , con lo que queda

$$_{\mathbb{C}[x]}V = \mathbb{C}[x]x_1 \dot{+} \mathbb{C}[x]x_2 \dot{+} \mathbb{C}[x]u_2$$

En la base  $\{x_1, x_2, u_2\}$  la matriz de  $T$  es:

$$\begin{pmatrix} \bar{z} & 0 & 0 \\ 0 & z & 0 \\ 0 & 0 & \alpha \end{pmatrix}$$

Caso particular,  $K$  con característica 2:

$$B = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

Tenemos que

$$\begin{aligned} X - B &= \begin{pmatrix} x+1 & 1 & 1 \\ 1 & x+1 & 1 \\ 1 & 1 & x+1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & x+1 \\ 1 & x+1 & 1 \\ x+1 & 1 & 1 \end{pmatrix} \sim \\ &\begin{pmatrix} 1 & 1 & x+1 \\ 0 & x & x \\ 0 & x & x^2 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & x+1 \\ 0 & x & x \\ 0 & 0 & x^2+x \end{pmatrix} \end{aligned}$$

Y ahora por columnas

$$\begin{aligned} \begin{pmatrix} 1 & 1 & x+1 \\ 0 & x & x \\ 0 & 0 & x^2+x \end{pmatrix} &\stackrel{c_2+c_1}{\sim} \begin{pmatrix} 1 & 0 & x+1 \\ 0 & x & x \\ 0 & 0 & x^2+x \end{pmatrix} \stackrel{c_3+(\widetilde{x+1})c_1}{\sim} \\ &\begin{pmatrix} 1 & 0 & 0 \\ 0 & x & x \\ 0 & 0 & x^2+x \end{pmatrix} \stackrel{c_3+c_2}{\sim} \begin{pmatrix} 1 & 0 & 0 \\ 0 & x & 0 \\ 0 & 0 & x^2+x \end{pmatrix} = D \\ Q &= \begin{pmatrix} 1 & 1 & x+1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \end{aligned}$$

Tenemos que:

$${}_{K[x]}V = K[x]x_2 \dot{+} K[x]x_3$$

donde  $\text{ann}_{K[x]}(x_2) = \langle x \rangle$  y  $\text{ann}_{K[x]}(x_3) = \langle x^2 + x \rangle$ , con lo que  $x_2 = v_2 + v_3$  y  $x_3 = v_3$  (como el anulador de  $x_1$  es  $K[x]$ ,  $x_1 = 0$  y no nos interesa).

Como  $x^2 + x = x(x+1)$ , tomamos  $y_1 = (x+1)x_3 = (T+1)x_3$  y  $\text{ann}_{K[x]}(y_1) = \langle x \rangle$ . Como  $x^2 + x = x(x+1)$ , tomamos  $y_2 = xx_3 = Tx_3$  y  $\text{ann}_{K[x]}(y_2) = \langle x+1 \rangle$ . La descomposición cíclica primaria queda:

$${}_{K[x]}V = K[x]x_2 \dot{+} K[x]y_1 \dot{+} K[x]y_2$$

Y la matriz de  $T$  en la base  $\{x_2, y_1, y_2\}$  es:

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

**Teorema 10.** Si  $A$  es un dominio euclídeo con función euclídea  $\nu$  y  $B$  es una matriz con coeficientes en  $A$ , existen  $P, Q$  inversibles de tamaño adecuado y  $D$  quasidiagonal tal que:

$$PB = DQ$$

*Demostración.* Necesitamos demostrar que  $PBQ^{-1} = D$ . Suponemos que  $B \neq 0$ . Vamos a demostrar que mediante operaciones elementales sobre filas y columnas, podemos reducir  $B$  a una del tipo

$$\begin{pmatrix} b & O \\ O & B' \end{pmatrix}$$

Llamemos  $\nu(B) = \min\{\nu(b_{ij}) : b_{ij} \neq 0\}$ . Intercambiando filas y columnas en  $B$  podemos conseguir  $\nu(B) = \nu(b_{11})$ .

Caso *a*: Si  $b_{11}|b_{i1}$  y  $b_{11}|b_{1j}$  para todos  $i, j$ , entonces reduzco haciendo ceros en las filas y columnas.

Caso *b*: Si  $b_{11}|b_{i1}$  o  $b_{11}|b_{1j}$  para algún  $i$  o  $j$  (supongamos  $i$ ), entonces

$$b_{i1} = qb_{11} + r$$

y tenemos que  $\nu(r) < \nu(b_{11})$ . Basta restar a la fila  $i$  la primera multiplicada por  $q$  e intercambiarlas.

Hacemos finalmente inducción sobre  $\nu(B)$ .

□

## 4.2. Módulos semisimples

**Proposición 23.** Sea  $M$  un módulo. Sea  $\{M_i : i \in I\}$  una familia no vacía de submódulos simples (no cero y que sus únicos submódulos son el 0 y el total).

Ponemos  $M' = \sum_{i \in I} M_i$ , es decir, el menor submódulo que los contiene a todos. Tomamos  $N \subsetneq M'$ . Entonces existe un  $J \subseteq I$  tal que  $\{M_i : i \in J\}$  es independiente,  $N \cap (\sum_{i \in J} M_i) = \{0\}$  y  $M' = N + (\sum_{j \in J} M_j)$ .

*Demostración.* La demostración pasa por utilizar el lema de Zorn. Sea  $\Gamma$  el conjunto de los subconjuntos  $J$  de  $I$  tales que  $\{M_i : i \in J\}$  es independiente y  $N \cap (\sum_{i \in J} M_i) = \{0\}$ .

Veamos que  $\Gamma \neq \emptyset$ . Si  $N = \{0\}$ , tomamos  $i \in I$  y tenemos que  $\{i\} \in \Gamma$ , que cumple trivialmente ambas propiedades. Si  $N \neq \{0\}$ , pero  $N \cap M_i = \{0\}$ , tomamos de nuevo  $\{i\} \in \Gamma$  que es otro caso trivial.

Supongamos que  $N \neq \{0\}$  y  $N \cap M_i = \{0\}$  para todo  $i \in I$ . Como cada  $M_i$  es simple,  $N \cap M_i = M_i$  para todo  $i \in I$ , con lo que  $N = M'$ , caso que hemos excluido.

El orden que definimos en  $\Gamma$  es la inclusión. Tenemos que ver que cualquier cadena (subconjunto totalmente ordenado) tiene un elemento maximal. Sea  $\chi \subseteq \Gamma$ . Definimos  $J = \bigcup_{C \in \chi} C$ . Lo que tenemos que demostrar es que  $J \in \Gamma$ .

Veamos que  $\{M_i : i \in J\}$  es independiente. Por una proposición anterior, basta ver que cualquier  $\{M_i : i \in F\}$  es independiente para cualquier  $F \subseteq J$  finito. Por ser  $\chi$  una cadena, existe un  $C \in \chi$  tal que  $F \subseteq C$ . Pero  $C \in \Gamma$ , luego  $\{M_i : i \in C\}$  es independiente, y en particular,  $\{M_i : i \in F\}$  es independiente.

Tomamos  $m \in N \cap (\dot{+}_{j \in J} M_j)$ . Entonces existe un  $F \subseteq J$  finito tal que  $m \in N \cap (\dot{+}_{j \in F} M_j)$ , entonces existe un  $C \in \chi$  tal que  $F \subseteq C$  y por consiguiente  $m \in N \cap (\dot{+}_{j \in C} M_j) = \{0\}$ .

Por tanto  $\Gamma$  es inductivo y el lema de Zorn nos asegura que existe un  $J \in \Gamma$  maximal.

Solo basta ver que  $M' = N \dot{+} (\dot{+}_{j \in J} M_j)$  y basta ver que es la suma (ya sabemos que es directa). Para  $i \notin J$ ,  $M_i \cap (N + (\dot{+}_{j \in J} M_j)) \neq \{0\}$ . De lo contrario,  $J \cup \{i\} \in \Gamma$  y  $J$  no sería maximal. Como  $M_i$  es simple,  $M_i \subseteq (N + (\dot{+}_{j \in J} M_j))$ . Al final tenemos que  $M_i \subseteq (N + (\dot{+}_{j \in J} M_j))$  para todo  $i \in I$ , con lo que  $M' = N \dot{+} (\dot{+}_{j \in J} M_j)$ . □

**Definición 45** (Anillo de división). Un anillo  $D$  se dice que es un anillo de división si para todo  $d \in D \setminus \{0\}$  existe un  $d^{-1}$  tal que

$$dd^{-1} = d^{-1}d = 1$$

Si  $D$  es además conmutativo, es entonces un cuerpo.

**Corolario 10.** Sea  $D$  un anillo de división y  ${}_D V$  un  $D$ -espacio vectorial no nulo. Si  $\{v_i : i \in I\}$  es un conjunto de generadores no nulos de  $V$ , existe  $J \subseteq I$  tal que  $\{v_j : j \in J\}$  es una base de  ${}_D V$ .

*Demostración.* Tomo la familia  $\{Dv_i : i \in I\}$ . Cada  $Dv_i \cong D/\text{ann}_D(v_i) \cong {}_D D$  ya que el anulador de cualquier elemento en un anillo de división es cero.  ${}_D D$  es un módulo simple.

$$V = \sum_{i \in I} Dv_i$$

Tomando  $N = \{0\}$  en la proposición, existe un  $J \in I$  tal que

$$V = \dot{+}_{j \in J} Dv_j$$

o equivalentemente  $\{v_j : j \in J\}$  es base de  $V$ . □

*Observación 13.* En la proposición anterior se ve que  $V \cong D^{(J)}$ .

**Definición 46** (Homomorfismo escindido). Dado homomorfismos de módulos  $N \xrightarrow{g} M \xrightarrow{f} N$  tales que  $f \circ g = \text{id}_N$ , diremos que  $f$  es un epimorfismo escindido (o roto o partido) y que  $g$  es un monomorfismo escindido (o roto o partido).

**Lema 9.** *Todo módulo finitamente generado no nulo contiene un submódulo propio maximal.*

*Demostración.* Sea  $M$  el módulo y  $\Gamma$  el conjunto de los submódulos propios de  $M$ , o sea,

$$\Gamma = \{N : N \in \mathcal{L}(M), N \neq M\}$$

Tenemos que  $\{0\} \in \Gamma$ , luego es no vacío. Tomamos  $\chi$  cadena en  $\Gamma$  y  $N = \bigcup_{C \in \chi} C$ . Veamos que  $N \in \Gamma$ .

Tomamos  $m_1, \dots, m_t$  generadores de  $M$ . Si  $N = M$ , tendríamos que  $m_1, \dots, m_t \in N$  y existiría en ese caso un  $C \in \chi$  tal que  $m_1, \dots, m_t \in C$ , con lo que  $M \subseteq C \subseteq M$  con lo que  $C = M$  y en particular  $C \notin \Gamma$ , lo cuál es una contradicción.

Aplicando el lema de Zorn a  $\Gamma$ , tenemos que tiene elementos maximales. □

**Teorema 11.** *Las siguientes condiciones son equivalentes para un módulo  $M$ :*

1. *Todo submódulo de  $M$  es un sumando directo.*
2. *Todo monomorfismo  $L \rightarrow M$  es escindido.*
3. *Todo epimorfismo  $M \rightarrow N$  es escindido.*
4.  $\text{Soc}(M) = M$ .
5.  *$M$  es suma de una familia de submódulos simples.*
6.  *$M$  es suma directa interna de una familia de submódulos simples.*

*En cualquiera de los casos diremos que  $M$  es semisimple.*

*Demostración.* Como todas las afirmaciones son triviales ciertas si  $M = \{0\}$ , suponemos que  $M \neq \{0\}$ .

Vamos a ver que la primera afirmación implica la tercera. Sea  $\phi : M \rightarrow N$ . Tomemos  $L = \ker \phi$ . Por hipótesis  $M = L \dot{+} X$  para cierto  $X \in \mathcal{L}(M)$ . Tenemos que, por los teoremas de isomorfía:

$$N \cong M/L = (L \dot{+} X)/L \cong X/(L \cap X) \cong X/\{0\} \cong X$$

Tenemos que para cada  $x \in X$  se va identificando con  $x + \{0\}$ , y  $x + L$ , que se identifica con  $\phi(x)$  a través de los isomorfismos anteriores.

Es decir, la aplicación anterior es  $\phi|_X : X \rightarrow N$ .

Definimos  $\varphi : N \rightarrow M$  como  $\varphi := \iota \circ (\phi)^{-1}$ , que cumple que  $\phi \circ \varphi = \text{id}_N$ .

Veamos que la tercera afirmación implica la segunda. Sea  $\varphi : L \rightarrow M$  un monomorfismo. Consideramos la sucesión exacta corta dada por  $0 \rightarrow L \xrightarrow{\varphi} M \xrightarrow{\kappa} C \rightarrow 0$  donde  $C = M/\text{Im } \varphi$  y  $\kappa$  es la proyección canónica.

Existe un  $g : C \rightarrow M$  tal que  $\kappa \circ g = \text{id}_C$ . Defino  $h = \text{id}_M - g \circ \kappa : M \rightarrow M$ .

$$\kappa \circ h = \kappa - \kappa \circ g \circ \kappa = \kappa - \kappa = 0$$

con lo que  $\text{Im } h \subseteq \ker \kappa$ .

Tenemos  $f : M \rightarrow L$  tal que  $\varphi \circ f = h$  (es decir,  $h$  pero visto en  $L$ ). Se dejan como ejercicio los detalles.

$$\varphi \circ (f \circ \varphi) = h \circ \varphi = \varphi - g \circ \kappa \circ \varphi = \varphi$$

donde el segundo sumando se anula por exactitud.

Por la inyectividad de  $\varphi$ , tenemos que podemos cancelar a izquierda y por tanto  $f \circ \varphi = \text{id}_L$ .

Veamos que la segunda afirmación implica la primera, con lo que tendremos ya que las tres primeras son equivalentes.

Tomamos  $X \in \mathcal{L}(M)$ , tenemos que  $\iota : X \rightarrow M$  es un monomorfismo. Por hipótesis, existe un  $p : M \rightarrow X$  tal que  $p|_X = \text{id}_X$ . Entonces se tiene que:

$$M = X \dot{+} \ker p$$

que es un ejercicio sencillo.

Vamos a ver que de la cuarta afirmación se deduce la quinta. La cuarta afirmación dice que  $M = \sum N_i$  donde  $N_i$  son los submódulos simples de  $M$ .

Veamos ahora que de la quinta se sigue la sexta. Por una proposición anterior (la 23) tomando  $N = 0$ , tenemos que es cierta.

Trivialmente, la última afirmación implica la primera, tomando  $N$  cualquiera en la proposición 23.

Basta ver ahora que la primera afirmación implica la cuarta. Por hipótesis  $M = \text{Soc}(M) \dot{+} X$  para cierto  $X$ . Veamos que  $X = \{0\}$ . Si no fuera así, tomamos  $m \in X \setminus \{0\}$ . El lema previo nos asegura que hay un epimorfismo  $p : Rm \rightarrow S$  para  $S$  simple.

De nuevo,  $Rm$  es un sumando directo de  $M$ , existe un epimorfismo  $\pi : M \rightarrow Rm$ . Hacemos la composición  $p \circ \pi : M \rightarrow S$ .

Como la hipótesis primera equivale a la tercera, existe  $\iota : S \rightarrow M$  (por una vez no es inclusión) tal que  $p \circ \pi \circ \iota = \text{id}_S$ .

$$S \cong \text{Im}(\pi \circ \iota) \subseteq Rm \subseteq X$$

donde hemos usado el primer teorema de isomorfía a una aplicación inyectiva. luego  $X$  contiene a una copia de un simple y no es simple. Así que  $X = 0$  y  $M = \text{Soc}(M)$ . □

**Corolario 11.** Si  $M$  es finitamente generado y no nulo, existe un  $N \leq M$  tal que  $M/N$  es simple.

**Corolario 12.** Todo cociente de y todo submódulo de un módulo semisimple es semisimple.

*Demostración.* Sea  $M$  semisimple y tomamos  $N$  un submódulo. Veamos que  $M/N$  es también semisimple.  $M$  es semisimple, luego es suma de módulos simples:

$$M = \sum_{i \in I} S_i$$

Consideremos  $p : M \rightarrow M/N$  la proyección canónica ( $m \mapsto m + N$ ). Tenemos que  $M/N = \sum_{i \in I} p(S_i)$ . Para cada  $i \in I$  puede que  $p(S_i) = 0$  (que sobran de la suma) o  $p(S_i) \neq 0$ .

$p(S_i)$  es simple porque  $p : S_i \rightarrow p(S_i)$  es un isomorfismo (inyectiva y definida sobre su imagen).

Veamos que pasa con los submódulos.  $M = N \dot{+} X$  para algún  $X$ . Esto implica que  $m = n + x \xrightarrow{\pi} n$  es un epimorfismo de módulos entre  $M$  y  $N$ . Entonces  $N \cong N / \ker \pi$ , luego es semisimple. □

**Corolario 13.**  $M$  es semisimple finitamente generado si y solo si  $M = S_1 \dot{+} \dots \dot{+} S_n$  para  $S_i$  simple.

*Demostración.* La implicación hacia la izquierda es una aplicación directa del teorema.

Por otro lado,  $M = \dot{+}_{i \in I} S_i$ , por ser simple. Sean  $m_1, \dots, m_t$  generadores de  $M$ . Entonces existe  $F \subseteq I$  finito tal que

$$m_j \in \dot{+}_{i \in F} S_i$$

para todo  $j$ . Entonces

$$M \subseteq \dot{+}_{i \in F} S_i \subseteq M$$

con lo que  $M$  es una suma finita. □



### 4.2.1. Anillos semisimples

**Definición 47** (Anillos semisimples). Un anillo  $R$  es semisimple si todo  $R$ -módulo es semisimple.

*Observación 14.* Todo anillo de división es semisimple. ¿Hay más?

**Teorema 12.**  $R$  es semisimple si y solo si  ${}_R R$  es semisimple. Es decir, todos los módulos sobre  $R$  son semisimples si y solo si lo es el regular.

*Demostración.* Sea  ${}_R M$  un módulo. Está claro que  $Rm \cong R/\text{ann}_R(m)$ , que es un cociente de un semisimple, luego semisimple para cualquier  $m$ . Tenemos que para ciertos  $m \in M$ :

$$M = \sum_{m \in M} Rm$$

con lo que  $M$  es suma de semisimples, luego semisimple. □

**Definición 48** (Anillo de endomorfismos). Sea  $M$  un  $R$ -módulo, definimos:

$$\text{End}_R(M) = \{f : M \longrightarrow M : f \text{ homomorfismo de módulos sobre } R\}$$

es un subanillo de  $\text{End}(M)$ .

Llamemos  $S = \text{End}_R(M)$ , tenemos que  $M$  es un  $S$ -módulo puesto que  $S \subseteq \text{End}(M)$ .  $\text{End}_R(M)$  es el anillo de endomorfismos de  $M$ .

¿Cuál es la acción en  $M$ ? La inclusión:  $f \in S$ , tenemos  $fm = f(m)$ .

**Definición 49** (Biendomorfismos). ¿Quién es  $\text{End}_S(M)$ ? Obviamente,  $\text{End}_S(M) \subseteq \text{End}(M)$  subanillo.

Dado  $g \in \text{End}(M)$ ,  $g \in \text{End}_S(M)$  si y solo si  $g(fm) = fg(m)$  para todo  $f \in S = \text{End}_R(M)$ . Pero  $g(f(m)) = g(fm) = fg(m) = f(g(m))$  con  $m \in M$ . Pero esto es lo mismo que decir que  $g \circ f = f \circ g$ .

$$\text{End}_S(M) = \{g \in \text{End}(M) : g \circ f = f \circ g \quad \forall f \in \text{End}_R(M)\}$$

Llamaremos  $T = \text{End}_S(M)$ .

**Lema 10.**  $R \xrightarrow{\lambda} \text{End}_S(M)$  dado por  $\lambda(r) : M \longrightarrow M$  y  $\lambda(r)(m) = rm$ . Dicho  $\lambda$  es un homomorfismo de anillos.

*Demostración.* Basta con ver que  $\text{Im } \lambda \subseteq \text{End}_S(M)$ . O sea que  $\lambda(r) \circ f = f \circ \lambda(r)$  para todo  $r \in R$ . En efecto:

$$(\lambda(r) \circ f)(m) = rf(m) = f(rm) = (f \circ \lambda(r))(m)$$

para todo  $f \in S$  y todo  $m \in M$ . □

*Observación 15.* El conjunto de “triendomorfismos” coincide con el de endomorfismos. Es decir,  $S = \text{End}_T(M)$ .

**Proposición 24.** *Los  $R$ -sumandos directos de  $M$  son los mismos que los  $T$ -sumandos directos de  $M$ .*

*Como consecuencia, si  ${}_R M$  es semisimple, entonces  ${}_T M$  también lo es.*

*Demostración.* Si  $N$  es un  $T$ -sumando directo de  $M$  tenemos que  $M = N \dot{+} X$  para cierto  $X \in \mathcal{L}({}_T M)$ . Entonces  $N \dot{+} X = M$  como  $R$ -módulos.

Recíprocamente,  ${}_R M = X \dot{+} Y$  con  $X, Y \in \mathcal{L}({}_R M)$ . Basta ver que  $X$  es un  $T$ -módulo.

Tomo  $p : M \longrightarrow M$ , tal que  $p(m) = p(x + y) = x$  y  $p \in S = \text{End}_R(S)$ , y  $X = \text{Im } p$ . Tomo  $g \in T$ ,  $x \in X$ ,

$$gx = g(x) = g(p(x)) = (g \circ p)(x) = (p \circ g)(x) = p(g(x)) \in \text{Im } p = X$$

luego  $X \in \mathcal{L}({}_T M)$ .

Veamos que si uno es semisimple lo es el otro. Entonces si  $N$  es un sumando directo de  $M$  visto como  $R$ -módulo, entonces lo es como sumando directo como  $T$  módulo, luego  $M$  es semisimple. □

**Corolario 14.** Si  ${}_R M$  es semisimple,  $\ell({}_R M) < \infty$ , entonces  ${}_T M$  y  $\ell({}_R M) = \ell({}_T M)$ .

Tenemos que, dado  ${}_R M$ ,  ${}_R M^n = M \oplus \cdots \oplus M$ . Sea  $S' = \text{End}_R(M^n)$ .

Sea  $\iota_i$  la aplicación dada por  $m \mapsto (0, \dots, 0, m, 0, \dots, 0)$  y  $\pi_j$  la que aplica  $m_i = (m_1, \dots, m_j, \dots, m_n) \mapsto m_j$ .

Tenemos que  $\text{id}_{M^n} = \sum_{i=1}^n \iota_i \circ \pi_i \in S'$ . Dado  $f \in \text{End}_S(M)$ , definimos  $\bar{f} = \sum_{i=1}^n \iota_i \circ f \circ \pi_i \in \text{End}(M^n)$ , en concreto

$$\bar{f}(m_1, \dots, m_n) = (f(m_1), \dots, f(m_n))$$

A partir de ahora prescindimos del símbolo  $\circ$  para indicar composición.

Tomando  $g \in S'$ , tenemos que

$$g\bar{f} = \sum_{i,j=1}^n \iota_i \pi_i g \iota_j f \pi_j = \sum_{i,j=1}^n \iota_i f \pi_i g \iota_j \pi_j = \bar{f}g$$

con lo que  $f \in \text{End}_{S'}(M^n)$ .

**Teorema 13** (de densidad de Jacobson). *Sea  $M$  un  $R$ -módulo semisimple. Sean  $m_1, \dots, m_n \in M$  y  $S = \text{End}_R(M)$ . Para cada  $f \in \text{End}_S(M)$  existe un  $r \in R$  tal que  $f(m_i) = rm_i$  para todo  $i \in \{1, \dots, n\}$ .*

*Demostración.* Sea  $m = (m_1, \dots, m_n) \in M^n$ . Sé que  $M^n$  es  $R$ -semisimple.  $Rm$  es un  $R$ -sumando directo de  $M^n$ . Entonces  $Rm$  es un  $\text{End}_{S'}(M^n)$ -submódulo de  $M^n$ .

Como  $\bar{f} \in \text{End}_{S'}(M^n)$ , entonces  $(f(m_1), \dots, f(m_n)) = \bar{f}(m) = \bar{f}m \in Rm$ , con lo que existe un  $r \in R$  tal que  $f(m_i) = rm_i$ . □

**Lema 11** (de Schur). Sean  ${}_R M$ ,  ${}_R N$  y  $f : M \longrightarrow N$  es homomorfismo de  $R$ -módulos, entonces  $f$  o es 0 o es un isomorfismo.

Así,  $\text{End}_R(M)$  es una anillo de división.

**Proposición 25.** Sea  $R$  tal que  ${}_R R$  es artiniano y  ${}_R M$  un módulo simple. Si  ${}_R M$  es fiel ( $\text{Ann}_R(M) = \{0\}$ ), entonces  $\lambda : R \longrightarrow \text{End}_D(M)$  es un isomorfismo, donde  $D = \text{End}_R(M)$ . Además,  $\dim_D M < \infty$ .

*Demostración.* Supongamos que  ${}_D M$  no fuera de dimensión finita. Entonces  $M$  admite una base  $B$  infinita. Tomamos  $\{x_i : i \in \mathbb{N}\} \subseteq B$  linealmente independiente.

Dado  $i \in \mathbb{N}$ , tomamos  $f_i : M \longrightarrow M$  la aplicación  $D$ -lineal que vale 0 sobre todo elemento de  $B$  y sobre  $f_i(x_i) = x_i$ .

Cada  $f_i \in \text{End}_D(M)$ . El teorema de densidad nos permite asegurar que existe  $r_i \in R$  tal que  $f_i(x_j) = r_i x_j$  para  $j = 0, \dots, i$ .

$r_i \in \text{ann}_R(x_0) \cap \dots \cap \text{ann}_R(x_{i-1})$ , pero el  $r_i \in \text{ann}_R(x_0) \cap \dots \cap \text{ann}_R(x_{i-1}) \cap \text{ann}_R(x_i)$ . Tenemos que

$$\text{ann}_R(x_0) \cap \dots \cap \text{ann}_R(x_{i-1}) \supsetneq \text{ann}_R(x_0) \cap \dots \cap \text{ann}_R(x_{i-1}) \cap \text{ann}_R(x_i)$$

con  $i \geq 1$  y tenemos una cadena descendente y por tanto  ${}_R R$  no es artiniano.

Tomo  $\{m_1, \dots, m_n\}$  una base de  $M$ . Dado  $f \in \text{End}_D(M)$ , el teorema de densidad asegura que existe  $r \in R$ , entonces  $f(m_i) = rm_i$  para todo  $i \in \{1, \dots, n\}$ . Basta tomar  $\lambda(r) = f$  y tenemos que es sobreyectivo. Como además  $M$  es fiel,  $\lambda$  es un isomorfismo. □

**Definición 50** (Idempotentes). Un elemento  $e \in R$  se dice idempotente si  $e^2 = e$ .

Un conjunto  $e_1, \dots, e_n \in R$  de idempotentes se dice un conjunto completo de idempotentes ortogonales (CCIO) si:

$$e_i e_j = 0$$

siempre que  $i \neq j$  y además:

$$e_1 + \dots + e_n = 1$$

**Proposición 26.** Si  $\{e_1, \dots, e_n\}$  es CCIO, entonces  $R = Re_1 + \dots + Re_n$ .

*Demostración.* Sea  $r \in R$ , tenemos que  $r = r1 = re_1 + \dots + ren$ .

Por otro lado, si  $0 = r_1e_1 + \dots + r_ne_n$  para  $r_i \in R$ , entonces multiplicando la identidad por  $e_i$  nos queda  $0 = r_ie_i^2 = r_ie_i$  para cada  $i \in \{1, \dots, n\}$ .  $\square$

**Definición 51** (Anillo simple).  $R$  es simple si y solo si los únicos ideales de  $R$  son  $\{0\}$  y  $R$ .

**Teorema 14.** Son equivalentes, para un anillo no trivial:

1.  ${}_R R$  semisimple y todos los  $R$ -módulos simples son isomorfos entre sí.
2.  $R$  es isomorfo como anillo a  $\text{End}_D(M)$  con  $D$  de división y  ${}_D M$  es de dimensión finita.
3.  ${}_R R$  artiniano y existe un  $R$ -módulo simple y fiel.
4.  ${}_R R$  es artiniano y simple.

Además, para la segunda afirmación se da necesariamente que  $D \cong \text{End}_R(\Sigma)$  para cualquier  ${}_R \Sigma$  el único sumódulo simple salvo isomorfismo dado en la primera afirmación. Por último, necesariamente,  $\dim_D(M) = \ell({}_R R)$ .

*Demostración.* Veamos que la primera afirmación implica la cuarta. Sabemos que  ${}_R R$  tiene longitud finita. Sea  $I$  un ideal de  $R$  propio ( $R \neq \{0\}$ ).  $R/I$  es semisimple como  $R$ -módulo. Como es finitamente generado, es suma directa finita de simples. Todos esos submódulos son isomorfos entre sí.

$$R/I \cong \Sigma^n$$

donde  ${}_R \Sigma$  es simple.

Tenemos que  $I = \text{Ann}_R(R/I)$  (aquí es donde hace falta que sea ideal y no solo ideal por la izquierda).

$$I = \text{Ann}_R(R/I) = \text{Ann}_R(\Sigma^n) = \text{Ann}_R(\Sigma)$$

Por otro lado  $R \cong \Sigma^m$ , con  $m = \ell({}_R R)$ .

$$I = \text{Ann}_R(\Sigma) = \text{Ann}_R(\Sigma^m) = \text{Ann}_R(R) = \{0\}$$

Demostremos ahora que la cuarta afirmación implica la tercera. Tomamos  ${}_R \Sigma$  simple (existe tomando el primero de la serie de descomposición, por ser artiniano).  $R \neq \text{Ann}_R(\Sigma)$  por ser simple, luego  $\text{Ann}_R(\Sigma) = \{0\}$ . Luego  ${}_R \Sigma$  fiel.

La segunda afirmación se deduce de la tercera por la proposición anterior.

Veamos finalmente que la cuarta afirmación implica la primera. Tomamos  $S = \text{End}_D(M)$ . Si  $m, m' \in M$  con  $m \neq 0$ , existe entonces un  $f \in S$  tal que  $f(m) = m'$ .

Así,  $Sm = M$  con lo que  ${}_S M$  es simple. Sea  $\{m_1, \dots, m_n\}$   $D$ -base de  $M$ . Para  $i \in \{1, \dots, n\}$  defino  $e_i \in S$  tal que

$$e_i(m_j) = \begin{cases} 0 & \text{si } j \neq i \\ m_i & \text{si } j = i \end{cases}$$

$\{e_1, \dots, e_n\}$  es CCIO de  $S$ , entonces  $S = Se_1 + \dots + Se_n$ . Veamos que  $Se_i$  es simple. Basta con demostrar que si  $f \in S$  tal que  $fe_i \neq 0$  entonces  $Sfe_i = Se_i$ .

$$fe_i = f(e_i) = \sum_{j=1}^n a_j m_j$$

con  $a_j \in D$ . Tomamos un índice  $k$  tal que  $a_k \neq 0$  (posible porque  $fe_i \neq 0$ ). Tenemos que  $s(m_k) = a_k^{-1}m_i$  y  $s(m_j) = 0$  si  $j \neq k$ .

Tenemos entonces

$$sfe_i(m_i) = s\left(\sum_j a_j m_j\right) = a_k^{-1}a_k m_i = m_i$$

con lo que  $sfe_i = e_i$  y por tanto  $Se_i = Sfe_i$  con lo que  ${}_S S$  es semisimple.

Veamos que cualquier módulo simple es isomorfo a  ${}_S S$ . Para ver que cada  $Se_i$  es isomorfo a  ${}_S M$ , por el lema de Schur, basta encontrar un homomorfismo no nulo  $Se_i \rightarrow M$ . Sea  $F : Se_i \rightarrow M$  dado por  $F(f) := f(m_i) = fm_i$ . Es fácil ver que  $F$  es un  $S$ -módulo.  $F(e_i) = e_i(m_i) = m_i \neq 0$ , con lo que  $F \neq 0$  y por el lema de Schur es un isomorfismo.

Si  ${}_S \Sigma$  es simple, luego existe un epimorfismo  $p : S \rightarrow \Sigma$  de  $S$ -módulos (descomponer por anuladores de cualquiera de sus elementos). Como  $p \neq 0$ , existe un  $i$  tal que  $p|_{Se_i} \neq 0$  y por tanto es un isomorfismo.

Sea  $\phi : S \rightarrow R$  un isomorfismo de anillos.  $\{\phi(e_1), \dots, \phi(e_n)\}$  es claramente CCIO de  $R$ . En particular,  $R = \sum_{i=1}^n R\phi(e_i)$ . Cada  $R\phi(e_i)$  es simple como  $R$ -módulo.  $Se_i \cong {}_S M$ , y  ${}_R M$  por restricción de escalares. Comprobando que  $\mathcal{L}({}_S M) = \mathcal{L}({}_R M)$ , deducimos que  ${}_R M$  es simple.

$R\phi(e_i)$ , veamos que  $\mathcal{L}R\phi(e_i) \cong \mathcal{L}R\phi(e_i)$  dados por  $I \mapsto \phi(I)$  y  $J \mapsto \phi^{-1}(J)$ , luego son dos conjuntos ordenados por la inclusión isomorfos. Luego como uno solo tiene dos elementos, en el otro también.

$R\phi(e_i)$  es simple y por tanto  ${}_R R$  es semisimple. Además:

$$\dim_D(M) = n = \ell({}_S S) = \ell({}_R R)$$

Sea  $\Sigma$  un  $R$ -módulo simple. Mediante restricción de escalares es un  $S$ -módulo simple, luego  ${}_S\Sigma \cong {}_SM$  con lo que  ${}_R\Sigma \cong {}_RM$ .

$$\lambda : D \longrightarrow \text{End}_S(M) = \text{End}_R(M)$$

es, por densidad, un isomorfismo. □

**Lema 12.** Sea  $R$  un anillo. Existe un conjunto  $\Omega_R$  (y es un conjunto y no una clase) de  $R$ -módulos simples no isomorfos entre sí tal que cualquier  $R$ -módulo simple es isomorfo a uno de los  $\Omega_R$ .

*Demostración.* Sea  ${}_R\Sigma$  simple. Tomo  $0 \neq s \in \Sigma$  entonces  ${}_R\Sigma \cong R/\text{ann}_R(s)$ . Tomo  $\Omega_R$  un conjunto de representantes de los  $R$ -módulos  $R/I$  para  $I$  ideal izquierda maximales bajo la relación de equivalencia  $I \sim J$  si y solo si  $R/I \cong R/J$ . □

**Proposición 27.**  ${}_RM$  un módulo. Para  $\Sigma \in \Omega_R$ , defino  $\text{Soc}_\Sigma(M)$  como la suma de todos los submódulos simples de  $M$  isomorfos a  $\Sigma$ . Entonces:

$$\text{Soc}(M) = \dot{+}_{\Sigma \in \Omega_R} \text{Soc}_\Sigma(M)$$

*Demostración.*

$$\text{Soc}(M) = \sum_{\Sigma \in \Omega_R} \text{Soc}_\Sigma(M)$$

por la definición de  $\Omega_R$ . Muchos de ellos serán cero.

Llamamos  $N = \text{Soc}_{\Sigma'}(M) \cap \sum_{\Sigma \neq \Sigma'} \text{Soc}_\Sigma(M)$ . Tomamos  $m \in N \setminus \{0\}$ , suponiendo que  $N \neq \{0\}$ . Tenemos que  $Rm$  es semisimple y es finitamente generado y por tanto de longitud finita. Entonces contiene un  $S$   $R$ -submódulo simple de  $Rm$ .

Tenemos que  $S \subseteq \text{Soc}_{\Sigma'}(M)$ . Existe entonces  $g : \text{Soc}_{\Sigma'}(M) \longrightarrow S$  epimorfismo (porque escinde). Existe  $S' \in \text{Soc}_{\Sigma'}(M)$  tal que  $S' \cong \Sigma'$  tal que  $g|_{S'} \neq 0$  entonces por Schur  $S' \cong S$ . Análogamente, se demuestra que  $S'' \cong \Sigma \neq \Sigma'$  tal que  $S'' \cong S$ . Resulta que  $\Sigma' \cong S \cong \Sigma$  y están relacionados, lo que contradice la definición de  $\Omega_R$ . □

*Observación 16.* Sea  $f \in \text{End}_R(M)$ . Entonces:

$$f(\text{Soc}_\Sigma(M)) = f\left(\sum_{S \cong \Sigma, S \in \mathcal{L}(M)} S\right) = \sum_{S \cong \Sigma, S \in \mathcal{L}(M)} f(S) \subseteq \text{Soc}_\Sigma(M)$$

Tomando  $M = R$  y  $f = \rho_r$  para  $\rho_r : R \longrightarrow R$  definida por  $\rho_r(r') = r'r$ , entonces  $\rho_r(\text{Soc}_\Sigma(R)) \subseteq \text{Soc}_\Sigma(R)$  y tenemos que  $\text{Soc}_\Sigma(R)$  es un ideal de  $R$ .

*Observación 17.*  $\Omega_{\mathbb{Z}}$  es biyectivo con  $\{\mathbb{Z}_p : p \text{ es primo}\}$ , luego es un conjunto infinito.

**Teorema 15** (Estructura de anillos semisimples). *Sea  $R$  un anillo semisimple. Entonces  $\Omega_R$  es finito. Si ponemos  $\Omega_R = \{\Sigma_1, \dots, \Sigma_t\}$  y  $D_i = \text{End}_R(\Sigma_i)$ , entonces*

$$R \cong \text{End}_{D_1}(\Sigma_1) \times \cdots \times \text{End}_{D_t}(\Sigma_t)$$

*y  $\dim_{D_i}(\Sigma_i)$  es finita.*

*Demostración.* Sé que  ${}_R R = S_1 \dot{+} \cdots \dot{+} S_n$  donde  ${}_R S_i$  es simple. Así, si  ${}_R \Sigma$  es simple, entonces  $\mathbb{R} \xrightarrow{p} \Sigma$  epimorfismo, donde  $p|_{S_i}$  es un isomorfismo para algún  $i$  y por Schur,  $S_i \cong \Sigma$ . Así que  $\Omega_R$  es finito.

Tenemos que  $\text{Soc}_{\Sigma_i}(R) \text{Soc}_{\Sigma_j}(R) \subseteq \text{Soc}_{\Sigma_i}(R) \cap \text{Soc}_{\Sigma_j}(R) = \{0\}$ . Eso implica que  $\text{Soc}_{\Sigma_j}(R) \subseteq \text{Ann}_R(\text{Soc}_{\Sigma_j}(R)) = \text{Ann}_R(\Sigma_j)$ .

Llamo a  $I_i = \sum_{j \neq i} \text{Soc}_{\Sigma_j}(R)$ . Tenemos que  $I_i + I_j = R$  si  $i \neq j$ . De la inclusión anterior se deduce  $\text{Ann}_R(\Sigma_i) + \text{Ann}_R(\Sigma_j) = R$  si  $i \neq j$ . Se cumple que:

$$R \longrightarrow R/\text{Ann}_R(\Sigma_1) \times \cdots \times R/\text{Ann}_R(\Sigma_t)$$

tal que

$$r \mapsto (r + \text{Ann}_R(\Sigma_1), \dots, r + \text{Ann}_R(\Sigma_t))$$

es un homomorfismo de anillos cuyo núcleo es  $\bigcap_{i=1}^t \text{Ann}_R(\Sigma_i) = \bigcap_{i=1}^n \text{Ann}_R(S_i) = \{0\}$ . donde simplemente puede haber algún  $\text{Ann}_R(S_i)$  repetido.

Cada  $R/\text{Ann}_R(\Sigma_i)$  es artinian (de longitud finita por ser cociente de uno de longitud finita).  $\Sigma_i$  es un  $R/\text{Ann}_R(\Sigma_i)$ -módulo simple fiel. Nuestro teorema nos garantiza que  $R/\text{Ann}_R(\Sigma_i) \cong \text{End}_{D_i}(\Sigma_i)$  para  $D_i = \text{End}_{R/\text{Ann}_R(\Sigma_i)}(\Sigma_i) \cong \text{End}_R(\Sigma_i)$  y  $\dim_{D_i}(\Sigma_i)$  es finita. □

Ejemplo:  $R, S$  dos anillos. Sea  $T = R \times S$ . Vamos a definir  $e = (1, 0)$ ,  $\mathcal{L}_T(Te) \longrightarrow \mathcal{L}_R(R)$  dada por  $I \mapsto \pi(I)$  donde  $\pi$  es la proyección en la primera componente, es una biyección que preserva la inclusión.

Como consecuencia  ${}_T Te$  es semisimple si y solo si  ${}_R R$ .

Así,  $T$  es semisimple si y solo si  $R$  y  $S$  si y solo si  $T$  son semisimples, ya que:

$${}_T T = Te \dot{+} T(1 - e)$$

Ejercicio: Sean  $D, E$  dos anillos de división,  ${}_D M, {}_E N$  espacios vectoriales. Se pide demostrar que

$$\text{End}_D(M) \cong \text{End}_E(N) \iff \begin{cases} D \cong E \\ \dim_D(M) = \dim_E(N) \end{cases}$$

### 4.3. Descomposición de anillos en ideales indescomponibles

**Definición 52** (El centro de un anillo). Sea  $R$  un anillo. El conjunto

$$Z(R) = \{r \in R : rs = sr \quad \forall s \in R\}$$

es un subanillo conmutativo de  $R$  que se llama centro de  $R$ .

**Definición 53** (Idempotente central). Si  $e \in Z(R)$  verifica  $e^2 = e$  diremos que es un idempotente central de  $R$ .

Si  $e$  es un idempotente central,  $Re$  es ideal y de  $R$  y además es un anillo con la suma y el producto heredados de  $R$  cuyo 1 es  $e$ .

Ejemplo: dados  $R_1$  y  $R_2$  anillos,  $R = R_1 \times R_2$ ,  $e = (1, 0)$  que es idempotente central, entonces  $Re = R_1 \times \{0\}$  es un anillo isomorfo a  $R_1$ .

*Observación 18.* Si  $e$  es idempotente central,  $1 - e$  es idempotente central.

Tenemos que  $\{e, 1 - e\}$  CCIO centrales. De hecho:

$$R = Re + R(1 - e) \cong Re \times R(1 - e)$$

Al revés, si  $R = I + J$  con  $I, J$  son ideales,  $1 = e + (1 - e)$ , con  $e \in I$ ,  $1 - e \in J$  con ambos centrales y  $I = Re$  y  $J = R(1 - e)$ .

Contraejemplo:  $R = \mathcal{M}_{2 \times 2}(K)$  con  $K$  un cuerpo.

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

es idempotente no central.

$$Re = \begin{pmatrix} K & 0 \\ K & 0 \end{pmatrix}$$

pero

$$eR = \begin{pmatrix} K & K \\ 0 & 0 \end{pmatrix}$$

**Definición 54** (Ideal indescomponibles). Si  $I = I_1 + I_2$  con  $I_i$  ideales implica que al menos uno de ellos es  $\{0\}$ , entonces diremos que es indescomponible.

**Definición 55** (Anillos indescomponibles). Diremos que  $R$  anillo es indescomponible si lo es como ideal.

**Definición 56** (Idempotentes indescomponibles). Sea  $e$  un idempotente central de  $R$ .  $e$  se dice indescomponible si  $e = e' + e''$ ,  $e'$  y  $e''$  idempotentes centrales ortogonales ( $e'e'' = 0$ ), uno de ellos es cero.



*Observación 19.* Hay una equivalencia entre los ideales indescomponibles y los idempotentes indescomponibles.

Ejercicio:  $R$  es indescomponible si y solo si no es isomorfo a ningún anillo de la forma  $R_1 \times R_2$  con  $R_1, R_2$  anillos no triviales.

*Observación 20.* Ningún dominio de integridad puede expresarse como producto de dos anillos. Luego es indescomponible.

**Proposición 28.** *Si un anillo tiene un CCIO centrales indescomponibles, entonces es único. Además, si  $\ell(R) < \infty$ , entonces  $R$  admite un CCIO central indescomponibles.*

*Demostración.* Supongamos que haya dos tales conjuntos  $\{e_1, \dots, e_n\}$  y  $\{f_1, \dots, f_m\}$ . Basta ver que uno está incluido en el otro.

$e_i f_j$  es idempotente central. Tenemos que

$$e_i = e_i f_j + e_i(1 - f_j)$$

es una descomposición de un idempotente indescomponible, así que o bien  $e_i f_j$  o bien  $e_i(1 - f_j)$  es cero. Si ocurriera que  $e_i f_j \neq 0$ ,  $e_i = e_i f_j$ . Análogamente  $f_j = e_i f_j$ , aplicando el razonamiento a  $f_j$ . Entonces  $e_i = f_j$ .

Dado  $e_i$ ,  $0 \neq e_i = e_i 1 = e_i(f_1 + \dots + f_m)$  y al menos hay algún  $j$  tal que  $e_i f_j \neq 0$  con lo que  $e_i = f_j$ .

Para la segunda parte vamos a aplicar inducción sobre la longitud. Si  $R$  es indescomponible no hay nada que demostrar. Si no, es porque  $R = Re + R(1 - e)$  para  $e \notin \{0, 1\}$  idempotente central. Tenemos que  $\ell(Re) < \ell(R)$ , y podemos aplicar la hipótesis de inducción.

□

*Observación 21.*  $R, S$  anillos. Si es  $\{e_1, \dots, e_t\}$  CCIO centrales indescomponibles y  $\phi : R \rightarrow S$  es un isomorfismo de anillos. Entonces  $\{\phi(e_1), \dots, \phi(e_t)\}$  es el CCIO centrales indescomponibles de  $S$ . Además se tiene

$$R = Re_1 + \dots + Re_t$$

entonces

$$S = S\phi(e_1) + \dots + S\phi(e_t)$$

donde  $Re_i \cong S\phi(e_i)$  como anillos.

Imaginemos que sabemos que  $R$  es semisimple y que disponemos de un isomorfismo de anillos  $R \cong R_1 \times \dots \times R_s$  con  $R_i$  indescomponibles.

Por otra parte,  $\Omega_R = \{\Sigma_1, \dots, \Sigma_t\}$ , tengo un isomorfismo de anillos  $R \cong \text{End}_{D_1}(\Sigma_1) \times \dots \times \text{End}_{D_t}(\Sigma_t)$ , donde  $D_i = \text{End}_R(\Sigma_i)$ .

Se deduce de la observación:

$$\text{End}_{D_1}(\Sigma_1) \times \cdots \times \text{End}_{D_t}(\Sigma_t) \cong R_1 \times \cdots \times R_s$$

sin más que componer isomorfismos. En primer lugar,  $s = t$  y tras reordenación  $\text{End}_{D_i}(\Sigma_i) \cong R_i$ . Conocemos los  $e_i$  CCIO centrales del segundo factor.

**Teorema 16** (Teorema de Artin-Wedderburn). *Si  $R \cong \text{End}_{D_1}(\Sigma_1) \times \cdots \times \text{End}_{D_t}(\Sigma_t) \cong \text{End}_{E_1}(T_1) \times \cdots \times \text{End}_{E_s}(T_s)$  donde  $D_i, E_i$  son todos anillos de división y  $\Sigma_i, T_i$  de dimensión finita como espacios vectoriales.*

*Entonces  $s = t$  y tras reordenación  $D_i \cong E_i$  y  $\dim_{D_i}(\Sigma_i) = \dim_{T_i}(T_i)$ .*

La demostración consiste en juntar observaciones, comentarios y teoremas anteriores.

#### 4.4. Módulos a derecha

**Definición 57** (Anillo opuesto). Sea  $R$  un anillo. Mantengo su estructura de grupo aditivo, pero cambiamos el producto. El nuevo producto va a ser el producto opuesto dado por  $r * s := sr$ .

A  $R$  con este nuevo producto lo vamos a llamar  $R^{op}$ , el anillo opuesto.

Ejemplo:

$$R = \begin{pmatrix} \mathbb{Z} & \mathbb{Q} \\ 0 & \mathbb{Q} \end{pmatrix} \leq \mathcal{M}_2(\mathbb{Q})$$

Tenemos que  ${}_R R$  no es noetheriano, pero  ${}_{R^{op}} R^{op}$  sí que lo es. Es decir, es noetheriano a derecha pero no a izquierda.

**Definición 58** (Anillo noetheriano a derecha). Un anillo es noetheriano a derecha si el anillo opuesto es noetheriano a izquierda.

**Definición 59** (Módulo a derechas). Definimos  $M$  módulo a derechas como  $M_R := {}_{R^{op}} M$ .

**Definición 60** (Ideal bilátero). Un ideal bilátero es un ideal a izquierda que es ideal a derecha también.

**Definición 61** (Dual de un módulo). Sea  ${}_R M$  un módulo. Tomamos

$${}^* M := \{f : M \longrightarrow R : f \text{ es homomorfismo de } R\text{-módulos}\}$$

que es un grupo aditivo y un módulo a derechas, es decir,  $R^{op}$ -módulo, por la acción:

$$(r\varphi)(m) := \varphi(m)r$$

con  $r \in R, m \in M$  y  $\varphi \in {}^* M$ . Es decir,  ${}^* M_R$ .

**Lema 13.**  $\theta : (\text{End}_R(M))^{op} \longrightarrow \text{End}_{R^{op}}(*M)$  tenemos que  $\theta(f)(\varphi) := \varphi \circ f$  es un homomorfismo de anillos. Nota: el producto en  $(\text{End}_R(M))^{op}$  es  $f * g = g \circ f$ .

Si  $M = \mathbb{Z}_n$  como  $\mathbb{Z}$  módulos,  $*M = \{0\}$  así que nos olvidamos de cualquier idea de reflexividad o isomorfismo.

**Definición 62** (Módulos reflexivos). Un módulo en el que la anterior  $\theta$  es un isomorfismo.

**Proposición 29.** Si  ${}_R M$  tiene una base  $\{v_1, \dots, v_n\}$ , puedo definir  $\{^*v_1, \dots, ^*v_n\}$ , definidos mediante  $v_i(^*v_j) = \delta_{ij}$ . Los  $^*v_i$  forman una base de  $^*M_R$ . Además,  $\theta$  es un isomorfismo de anillos.

*Demostración.* Veamos que es una base. Observemos que para cualquier  $m \in M$ :

$$m = \sum_{i=1}^n ^*v_i(m)v_i$$

Sea  $\varphi \in ^*M$ :

$$\varphi(m) = \sum_{i=1}^n ^*v_i(m)\varphi(v_i) = \left( \sum_{i=1}^n \varphi(v_i)^*v_i \right) (m)$$

luego  $\varphi = \sum_{i=1}^n \varphi(v_i)^*v_i$ . Con lo que los  $^*v_i$  generan  $^*_{R^{op}}M$ .  
Si

$$0 = \sum_i r_i ^*v_i$$

entonces:

$$0 = \sum_i (r_i ^*v_i)(v_j) = r_j$$

$\text{End}_R(M)^{op} \xrightarrow{\theta} \text{End}_{R^{op}}(*M)$  dado por  $\theta(f)(\varphi) := \varphi \circ f$ .

Veamos que  $\theta$  es inyectivo: tomo  $f$  tal que  $\theta(f) = 0$ . Dado  $m \in M$  tenemos:

$$f(m) = \sum_i ^*v_i(f(m))v_i = \sum_i \theta(f)(^*v_i)(m)v_i = 0$$

luego es inyectivo. Veamos que es sobreinyectivo.

Dado  $\psi \in \text{End}_{R^{op}}(*M)$  definimos  $f : M \longrightarrow M$  por:

$$f(m) = \sum_i \psi(^*v_i)(m)v_i$$

Es fácil ver que  $f \in \text{End}_R(M) \cong \text{End}_R(M)^{op}$ .

$$\begin{aligned}
\theta(f)(\varphi)(m) &= (\varphi \circ f)(m) = \sum_i \psi(*v_i)(m) \varphi(v_i) \\
&= \left( \sum_i \varphi(v_i) \psi(*v_i) \right) (m) \\
&= \psi \left( \sum_i \varphi(v_i) * v_i \right) (m) \\
&= \psi(\varphi)(m)
\end{aligned}$$

Por lo tanto,  $\theta(f)(\varphi) = \psi(\varphi)$ , y se sigue  $\varphi = \theta(f)$ , con lo que  $\theta$  es sobreyectivo. □

**Definición 63.** Si  ${}_R R$  es semisimple, entonces  $R \cong \text{End}_{D_1}(\Sigma_1) \times \cdots \times \text{End}_{D_t}(\Sigma_t)$  donde  $D_i$  de dimensión  $n_i = \dim_{D_i}(\Sigma_i) < \infty$  con  $D_i$  únicos salvo isomorfismo y reordenación y  $n_i$  únicos. Diremos que  $R$  es de tipo  $(D_1, \dots, D_t, n_1, \dots, n_t)$ .

**Teorema 17.** Si  $R$  es semisimple de tipo  $(D_1, \dots, D_t, n_1, \dots, n_t)$ , entonces  $R^{op}$  es semisimple de tipo  $(D_1^{op}, \dots, D_t^{op}, n_1, \dots, n_t)$ .

*Demostración.* Tenemos que  $R^{op} \cong \text{End}_{D_1}(\Sigma_1)^{op} \times \cdots \times \text{End}_{D_t}(\Sigma_t)^{op} \cong \text{End}_{D_1^{op}}(*\Sigma_1) \times \cdots \times \text{End}_{D_t^{op}}(*\Sigma_t)$  y  $\dim_{D_i}(\Sigma_i) = \dim_{D_i^{op}}(*\Sigma_i)$ .  $R^{op}$  es semisimple con la estructura del enunciado. □

**Corolario 15.**  $R$  es semisimple si y solo si  $R^{op}$  es semisimple.

Ejemplo:  $(\mathbb{C}, \mathbb{R}, 1, 2)$ . Tenemos que  $R \cong \mathbb{C} \times \mathcal{M}_{2 \times 2}(\mathbb{R})$ .

Ejemplo:  $(\mathbb{H}, 2)$ . Sea  ${}_H V$  un espacio de dimensión 2. Cuidado que  $\text{End}_H(V) \cong \mathcal{M}_{2 \times 2}(\mathbb{H}^{op})^{op}$ . Se puede demostrar que  $\mathbb{H}^{*1} \cong \mathbb{H}$ , pero no es automático, con lo que añadiendo la transposición  $\text{End}_H(V) \cong \mathcal{M}_{2 \times 2}(\mathbb{H})$ .

## 5. Algunas aplicaciones

### 5.1. $\mathbb{C}$ -álgebras de grupos finitos

Sea  $\mathbb{C}$  el cuerpo de los números complejos y  $G$  un grupo con elemento neutro  $e$ . Sea  $\mathbb{C}G$  el  $\mathbb{C}$  espacio vectorial con base  $G$ .

$\mu : \mathbb{C}G \times \mathbb{C}G \longrightarrow \mathbb{C}G$  la aplicación bilineal dada por  $\mu(g, h) = gh$  para  $g, h \in G$ .

Si para  $r, s \in \mathbb{C}G$  denotamos  $rs = \mu(r, s)$  donde si  $r = \sum_{g \in G} r_g g$  y  $s = \sum_{g \in G} s_g g$ ,  $r_g, s_g \in \mathbb{C}$ , se tiene:

$$rs = \sum_{g, h \in G} r_g s_h \mu(g, h) = \sum_{g, h \in G} r_g s_h gh$$

Tenemos que  $\mu$  define un producto que es asociativo.

$\mathbb{C}G \times \mathbb{C}G \times \mathbb{C}G \xrightarrow{\mu \times \text{id}} \mathbb{C}G \times \mathbb{C}G \xrightarrow{\mu} \mathbb{C}G$  proporciona el mismo resultado que  $\mathbb{C}G \times \mathbb{C}G \times \mathbb{C}G \xrightarrow{\text{id} \times \mu} \mathbb{C}G \times \mathbb{C}G \xrightarrow{\mu} \mathbb{C}G$ . Pero esto es trivial porque son dos aplicaciones trilineales que evaluadas en una base dan lo mismo (porque el producto en  $G$  es asociativo). Este es un ejemplo de un funtor del producto en  $G$  al producto en  $\mathbb{C}G$ .

Al ser bilineal, es distributiva respecto de la suma.

El elemento neutro de este producto es  $1e \in \mathbb{C}G$ .

**Proposición 30.**  $\mathbb{C}G$  con la estructura que hemos discutido, es un anillo.

La aplicación  $\eta : \mathbb{C} \longrightarrow \mathbb{C}G$  dada por  $z \mapsto ze$  es un homomorfismo de anillos, distinto de 0 y parte de un cuerpo, luego es inyectivo. Luego consideraremos que  $\text{Im } \eta$  es un subanillo de  $\mathbb{C}G$  y  $\text{Im } \eta \cong \mathbb{C}$ . Vamos a considerar entonces que  $1e = 1 = e$  y que  $\mathbb{C} \subseteq \mathbb{C}G$ .

Además,  $\mathbb{C} \subseteq \mathbb{C}G$ .  $gz = g\eta(z) = gze = zge = zg$ , es decir, los complejos son centrales.

**Definición 64** ( $\mathbb{C}$ -álgebra del grupo  $G$ ).  $\mathbb{C}G$  se llama  $\mathbb{C}$ -álgebra del grupo  $G$ .

Definimos  $\mu(G) := \{f : G \longrightarrow \mathbb{C} : f \text{ es aplicación}\}$ , es un  $\mathbb{C}$ -espacio vectorial con base  $G$ . Vamos a darle estructura de módulo.

$\mu(G)$  es un  $\mathbb{C}G$ -módulo definiendo para todo  $g \in G$  y  $\varphi \in \mu(G)$  y  $x \in G$ :

$$(g\varphi)(x) = \varphi(xg)$$

Vemos que  $g(h\varphi)(x) = (h\varphi)(xg) = \varphi(xg)h = \varphi(x(gh)) = (gh)\varphi(x)$ . Entonces  $g(h\varphi) = (gh)\varphi$ .

Hemos dado una aplicación  $G \longrightarrow \text{Map}(\mu(G), \mu(G))$  con  $g \mapsto (\varphi \mapsto g\varphi)$ . Queremos ver que  $G \longrightarrow \text{End}(\mu(G), \mu(G))$ , es decir  $g(\varphi + \psi) = g\varphi + g\psi$ .

$$g(\varphi + \psi)(x) = (\varphi + \psi)(xg) = \varphi(xg) + \psi(xg)$$

y por otro lado

$$g\varphi(x) + g\psi(x) = \varphi(xg) + \psi(xg)$$

Además:

$$g(z\varphi)(x) = z\varphi(xg) = z(g\varphi)(x)$$

$\mathbb{C}G \longrightarrow \text{End}_{\mathbb{C}}(\mu(G), \mu(G))$ , es  $\mathbb{C}$ -lineal.

En resumen, tenemos la siguiente proposición:

**Proposición 31.**  $\mu(G)$  es un  $\mathbb{C}G$ -módulo.

Nuestro objetivo es demostrar que si  $G$  es finito,  $\mathbb{C}G$  es semisimple y  $\mu(G)$  semisimple como  $\mathbb{C}G$ -módulo.

**Definición 65** (Producto hermítico). Sea  $V$  un espacio vectorial complejo de dimensión finita. Un producto interno hermítico es una aplicación  $\langle \cdot | \cdot \rangle : V \times V \longrightarrow \mathbb{C}$  cumpliendo:

1.  $\langle v | w \rangle = \overline{\langle w | v \rangle}$ .
2.  $\langle v' + v | w \rangle = \langle v | w \rangle + \langle v' | w \rangle$ .
3.  $\langle av | w \rangle = a \langle v | w \rangle$ .
4.  $\langle v | v \rangle \implies v = 0$ .

Es decir, es un espacio de Hilbert complejo de dimensión finita.

Sea  $V$  un  $\mathbb{C}G$ -módulo. Como  $\mathbb{C} \subseteq \mathbb{C}G$  por restricción de escalares,  ${}_{\mathbb{C}}V$  es un espacio vectorial.  $\rho : \mathbb{C}G \longrightarrow \text{End}_{\mathbb{C}}(V)$ ,  $\rho$  de anillos y  $\mathbb{C}$ -lineal.

$$\rho\left(\sum_{g \in G} r_g g\right)(v) = \sum_{g \in G} r_g g v$$

¿Qué pasa si restringimos  $\rho$  a  $G$ ? Como respeta el producto en  $G$ ,  $\rho|_G : G \longrightarrow GL_{\mathbb{C}}(V)$ , donde  $\rho|_G$  es un homomorfismo de grupos. Es una representación lineal de  $G$  con espacio de representación  $V$ .

Si  $W \subseteq V$ , es un  $\mathbb{C}G$ -submódulo si y solo si es un  $\mathbb{C}$ -subespacio vectorial y  $W$  es  $G$  invariante: para todo  $w \in W$  y todo  $g \in G$  se tiene que  $gw \in W$ .

$\mu(G)$  es el espacio de representación  $\rho : G \longrightarrow GL_{\mathbb{C}}(\mu(G))$  dado por:

$$\rho(g)(\varphi)(x) = \varphi(xg) =: g\varphi(x)$$

donde  $g, x \in G$  y  $\varphi \in \mu(G)$ .

**Teorema 18.** Si  $G$  es finito entonces  $\mathbb{C}G$  es semisimple.

*Demostración.* Supongamos que  $G$  es finito. Tomamos  $V$  un  $\mathbb{C}G$ -módulo de dimensión finita. Tomamos  $\langle \cdot | \cdot \rangle$  un producto interno en  $V$ .

Definimos  $\langle \cdot | \cdot \rangle_G$  producto interno sobre  $V$  así:

$$\langle v | u \rangle_G = \sum_{g \in G} \langle gv | gu \rangle$$

que cumple la siguiente propiedad para todo  $h \in G$ :

$$\langle hv | hu \rangle_G = \sum_{g \in G} \langle ghv | ghv \rangle = \sum_{f \in G} \langle fv | fu \rangle = \langle v | u \rangle_G$$

con lo que es un operador unitario (es un operador que conserva el producto interno de un espacio de Hilbert) y una isometría.

Sea  $W$  un  $\mathbb{C}G$ -submódulo de  $V$ . Se tiene:

$$V = W \dot{+} W^\perp$$

donde  $\perp$  se toma respecto al producto interno nuevo:

$$W^\perp := \{v \in V : \langle v | w \rangle_G = 0 \quad \forall w \in W\}$$

O sea  $W^\perp$  es  $G$ -invariante. En otras palabras, hemos de ver que si  $v \in W^\perp$ ,  $g \in G$  entonces  $gv \in W^\perp$ , entonces para todo  $w \in W$  tenemos que:

$$\langle gv | w \rangle_G = \langle gv | gg^{-1}w \rangle_G = \langle v | g^{-1}w \rangle = 0$$

ya que  $g^{-1}w \in W$  y  $v \in W^\perp$ . Luego  $W^\perp$  es  $G$ -invariante.

Como hemos demostrado que cualquier submódulo es sumando directo, tenemos que es semisimple. □

**Corolario 16.** Si  $G$  es finito,  $\mu(G)$  es un  $\mathbb{C}G$ -módulo semisimple.

Dotamos de a  $\mu(G)$  del producto interno:

$$\langle \varphi | \psi \rangle := \frac{1}{|G|} \sum_{g \in G} \varphi(g) \overline{\psi(g)}$$

Sea  $G$  un grupo,  $V$  un  $\mathbb{C}G$ -módulo, de dimensión finita como espacio vectorial complejo. Fijamos una base de  $v_i$ . Tomamos  $x \in G$ :

$$xv_i = \sum_j t_{ij}(x)v_j$$

A las funciones  $t_{ij} \in \mu(G)$  se les llama funciones matriciales de  $V$  en la base  $\{v_1, \dots, v_n\}$ .

Definimos  $C(V)$  como el subespacio vectorial de  $\mu(G)$  generado por  $\{t_{ij} : 1 \leq i, j \leq n\}$ . Veamos que  $C(V)$  no depende de la base fijada. Recordemos que todo cambio de bases puede interpretarse como un automorfismo.

Supongamos  $V'$  otro  $\mathbb{C}G$ -módulo con otra base  $\{v'_1, \dots, v'_m\}$ . Sea  $f : V \rightarrow V'$  homomorfismo de  $\mathbb{C}G$ -módulos. Las funciones matriciales de  $V'$  fijaremos una base  $v'_i$  y denotamos las funciones matriciales  $t'_{ij}$ .

$$f(v_i) = \sum_j a_{ij} v'_j$$

y sea  $A$  la matriz con coeficientes  $a_{ij}$ .

Tenemos que  $xf(v_i) = \sum_j a_{ij} \sum_k t'_{jk}(x) v'_k$  y  $fx(v_i) = \sum_j t_{ij}(x) \sum_k a_{ik} v'_k$ . Igualando lo anterior  $xf(v_i) = f(xv_i)$ , tenemos que  $A(t'_{ij}(x)) = (t_{ij}(x))A$  o si se quiere  $A(t'_{ij}) = (t_{ij})A$ .

Si  $f$  es un isomorfismo, entonces  $A$  es invertible y se tiene que los  $t'_{ij}$  y  $t_{ij}$  son combinaciones lineales los unos de los otros, luego si  $V' = V$  y  $f = \text{id}$  se tiene que  $C(V)$  no depende de la base elegida. Si  $V' \cong V$ , tenemos  $C(V) = C(V')$ .

**Lema 14.**  $C(V)$  es un  $\mathbb{C}G$ -submódulo de  $\mu(G)$ .

*Demostración.* Sean  $x, y \in G$ .  $t_{ij}(xy)$  es la matriz de la aplicación lineal dada por hacer actuar  $xy$  sobre cualquier vector:

$$t_{ij}(xy) = \sum_k t_{ik}(y) t_{kj}(x)$$

es decir, el producto de matrices (por filas, es decir, con el orden al revés que en la composición).

$$yt_{ij}(x) = t_{ij}(xy) = \sum_k t_{ik}(y) t_{kj}(x) = \left( \sum_k t_{ik}(y) t_{kj}(x) \right) (x)$$

con lo que:

$$yt_{ij} = \sum_k t_{ik}(y) t_{kj} \in C(V)$$

Luego  $C(V)$  es un submódulo. □

**Lema 15.** Sea  $f : V \rightarrow \mu(G)$  un homomorfismo de  $\mathbb{C}G$ -módulos. Entonces  $\text{Im } f \subseteq C(V)$ .



*Demostración.* Sea  $v_i$  un elemento de la base de  $V$ .

$$f(v_i)(x) = f(v_i)(ex) = xf(v_i)(e) = f(xv_i)(e) = \sum_j t_{ij}(x)f(v_j)(e) = \left( \sum_j f(v_j)(e)t_{ij} \right)(x)$$

$$f(v_i) = \sum_j f(v_j)(e)t_{ij} \in C(V)$$

□

**Lema 16.** Sean  $G$  finito,  $U, W$   $\mathbb{C}G$ -módulos (no necesariamente de dimensión finita) y  $f : U \rightarrow W$  lineal. La aplicación  $\tilde{f} : U \rightarrow W$  dada por:

$$\tilde{f}(u) = \sum_{x \in G} x^{-1}f(xu), \quad u \in U$$

es un homomorfismo de  $\mathbb{C}G$ -módulos.

*Demostración.* Hemos de ver que  $\tilde{f}(yu) = y\tilde{f}(u)$  para todo  $y \in G$  y todo  $u \in U$ .

$$\tilde{f}(yu) = \sum_{x \in G} x^{-1}f(xyu) = \sum_{z \in G} yz^{-1}f(zu) = y\tilde{f}(u)$$

donde  $z = xy$ .

□

**Lema 17.** Sea  $G$  finito y  $V$  un  $\mathbb{C}G$ -módulo de dimensión finita. Existe un producto interno  $\langle \cdot | \cdot \rangle$  en  $V$  tal que  $\langle xv | xw \rangle = \langle v | w \rangle$  con  $v, w \in V$  y  $x \in G$ .

Es decir, que la representación  $G \rightarrow U(V)$ , donde  $U(V)$  es el grupo unitario.

**Definición 66** (Espacio de coeficientes). A  $C(V)$  se le llama espacio de coeficientes.

**Lema 18** (de Schur). Sea  $\Sigma$  un  $\mathbb{C}G$ -módulo simple. Entonces:

$$\text{End}_{\mathbb{C}G}(\Sigma) = \{\lambda \text{id}_{\Sigma} : \lambda \in \mathbb{C}\} \cong \mathbb{C}$$

*Demostración.* Tenemos que  $\dim_{\mathbb{C}} \Sigma < \infty$ . Tomamos  $\phi : \Sigma \rightarrow \Sigma$  homomorfismo de  $\mathbb{C}G$ -módulos. Sea  $\phi$  es  $\mathbb{C}$  lineal. Tomamos  $\lambda \in \mathbb{C}$  valor propio de  $\phi$  y sea  $V_{\lambda}$  el subespacio propio asociado.

Sea  $g \in G, v \in V_{\lambda}$ ,  $\phi(gv) = g\phi(v) = g\lambda v = \lambda gv$  con  $gv \in V_{\lambda}$  entonces  $V_{\lambda}$  es un  $\mathbb{C}G$ -submódulo de  $\Sigma$ . Si  $\phi \neq 0$  entonces  $V_{\lambda} \neq \{0\}$ .

Como  $\Sigma$  es simple,  $V_{\lambda} = \Sigma$ .

□

**Definición 67** (Matriz unitaria). Su inversa coincide con su conjugada transpuesta

**Teorema 19** (de Peter-Weyl). *Dotemos a  $\mu(G)$  con el producto interno:*

$$\langle \varphi | \psi \rangle = \frac{1}{|G|} \sum_{x \in G} \varphi(x) \overline{\psi(x)}$$

*Tomamos  $\Omega_{\mathbb{C}G} = \{\Sigma_1, \dots, \Sigma_t\}$ .*

*Entonces  $\mu(G) = C(\Sigma_1) \dot{+} \dots \dot{+} C(\Sigma_t)$ , suma directa ortogonal de  $\mathbb{C}G$ -módulos.*

*Además, tomando en cada  $\Sigma_i$  un producto interno tal que la representación asociada a  $\Sigma_i$  sea unitaria, entonces  $\{t_{jk}^{\Sigma_i} : i \in \{1, \dots, s\}, j, k \in \{1, \dots, d_i\}\}$  es una base ortonormal de  $\mu(G)$  siempre que  $d_i = \dim_{\mathbb{C}} \Sigma_i$  y  $\{t_{jk}^{\Sigma_i}\}$  son las funciones matriciales asociados a  $\Sigma_i$  con respecto de una base ortonormal de  $\Sigma_i$ .*

*Demostración.*  $\mu(G) = \text{Soc}_{\Sigma_1}(\mu(G)) \dot{+} \dots \dot{+} \text{Soc}_{\Sigma_t}(\mu(G))$  y  $\text{Soc}_{\Sigma_i}(\mu(G)) \subseteq C(\Sigma_i)$ . Es suma de módulos isomorfos a  $\Sigma_i$  cada uno en  $C(\Sigma_i)$ . Tenemos que:

$$\mu(G) = C(\Sigma_1) + \dots + C(\Sigma_t)$$

Tomo  $V$  con base  $\{v_1, \dots, v_n\}$  y  $W$  con base  $\{w_1, \dots, w_m\}$   $\mathbb{C}G$ -módulos simples. Para cada  $i, j$  definimos  $p_{ij} : V \rightarrow W$  lineal dada por  $p_{ij}(v_k) = w_j \delta_{ki}$ . Entonces tomamos  $\tilde{p}_{ij}$  la extensión dada por

$$\tilde{p}_{ij}(v) = \sum_{x \in G} x^{-1} p_{ij}(xv)$$

con  $v \in V$ .

$$\tilde{p}_{ij}(v_k) = \sum_{x \in G} x^{-1} p_{ij}(xv_k) = \sum_{x \in G} x^{-1} p_{ij} \left( \sum_l t_{kl}^V(x) v_l \right) =$$

$$\sum_{x \in G} x^{-1} \sum_l t_{kl}^V(x) p_{ij}(v_l) = \sum_{x \in G} x^{-1} t_{ki}^V(x) w_j = \sum_l \sum_{x \in G} t_{ki}^V(x) t_{jl}^W(x^{-1}) w_l$$

En concreto si las bases  $v_i$  y  $w_j$  son ortonormales, entonces los coeficientes de  $t_{ki}^V$  y  $t_{jl}^W$  son de matrices unitarias. En ese caso la expresión anterior queda:

$$\sum_l \sum_{x \in G} t_{ki}^V(x) \overline{t_{jl}^W(x)} w_l$$

Si  $V \not\cong W$  entonces  $\tilde{p}_{ij} = 0$  y por tanto

$$\sum_l \sum_{x \in G} t_{ki}^V(x) \overline{t_{jl}^W(x)} w_l = 0$$

Sean  $a \neq b$  y tomamos  $V = \Sigma_a, W = \Sigma_b$ , entonces

$$0 = \sum_{x \in G} t_{ki}^V(x) \overline{t_{lj}^W(x)}$$

con lo que  $C(\Sigma_a) \perp C(\Sigma_b)$ .

Luego  $\mu(G) = C(\Sigma_1) \dot{+} \dots \dot{+} C(\Sigma_t)$ .

Supongamos ahora  $V = W = \Sigma_a$ . En ese caso, por el lema de Schur  $\tilde{p}_{ij}(v) = \alpha_{ij}v$ . Entonces  $(v_i = w_i)$ :

$$\alpha_{ij}v_k = \tilde{p}_{ij}(v_k) \sum_l \sum_{x \in G} t_{ki}^V(x) \overline{t_{lj}^V(x)} v_l$$

Si  $k \neq l$ , entonces  $\alpha_{ij}v_k = 0$  y por tanto:

$$\sum_l \sum_{x \in G} t_{ki}^V(x) \overline{t_{lj}^V(x)} v_l = 0$$

Si  $k = l$  e  $i \neq j$ , entonces:

$$0 = \sum_{x \in G} t_{ik}^{\Sigma_a}(x^{-1}) \overline{t_{jk}^{\Sigma_a}(x^{-1})} = \sum_{x \in G} t_{ki}^{\Sigma_a}(x) \overline{t_{kj}^{\Sigma_a}(x)}$$

luego  $\{t_{ij}^{\Sigma_a}\}$  es un sistema ortogonal generador, en particular es una base ortogonal. Veamos que no es ortonormal.

$$\sum_{x \in G} t_{ki}^{\Sigma_a}(x) \overline{t_{ki}^{\Sigma_a}(x)} = |G|$$

Luego son una base ortogonal.

$\tilde{p}_{ii}(v) = \sum_{x \in G} x^{-1} p_{ii}(xv)$ , con lo que  $\tilde{p}_{ii} = \sum_{x \in G} \rho(x^{-1}) \circ p_{ii} \circ \rho(x)$  donde  $\rho : G \rightarrow GL(\Sigma_a)$  donde  $\rho(x)(v) := xv$ . Por ser homomorfismo de grupos:

$$\tilde{p}_{ii} = \sum_{x \in G} \rho(x)^{-1} \circ p_{ii} \circ \rho(x)$$

Luego la traza del endomorfismo es  $d_a \alpha_{ii} = |G|$ . Tenemos:

$$\alpha_{ii} = \sum_l \sum_{x \in G} t_{ki}^V(x) \overline{t_{li}^V(x)} \sum_l \sum_{x \in G} |t_{ki}^V(x)|^2$$

con lo que  $|t_{ij}^{\Sigma_a}|^2 = \langle t_{ij}^{\Sigma_a} | t_{ij}^{\Sigma_a} \rangle = \frac{1}{|G|} \alpha_{ii} = \frac{1}{d_a}$ .

Luego la base

$$\{\sqrt{d_a} t_{ij}^{\Sigma_a} : a \in \{1, \dots, t\}, i, j \in \{1, \dots, d_a\}\}$$

es una base ortonormal.

□

**Corolario 17.**

$$|G| = d_1^2 + \cdots + d_t^2$$

*Demostración.*  $\mu(G) = C(\Sigma_1) \dot{+} \cdots \dot{+} C(\Sigma_t)$  con lo que:

$$|G| = \sum_{i=1}^t \dim_{\mathbb{C}} C(\Sigma_i) = \sum_{i=1}^t d_i^2$$

□

**Proposición 32.** Sea  $G$  abeliano finito,  $\Sigma$  un  $\mathbb{C}G$ -módulo simple. Entonces  $\dim_{\mathbb{C}} \Sigma = 1$ .

*Demostración.*  $\Sigma$  tiene dimensión compleja finita,  $x \in G$ ,  $f_x : \Sigma \rightarrow \Sigma$ ,  $f_x(v) = xv$  con  $y \in G$ :

$$f_x(yv) = xyv = yxv = yf_x(v)$$

entonces  $f_x \in \text{End}_{\mathbb{C}G}(\Sigma) = \{\lambda \text{id}_{\Sigma} : \lambda \in \mathbb{C}\}$ . Así que  $f_x = \lambda_x \text{id}_{\Sigma}$  para cierto  $\lambda_x \in \mathbb{C}$ .

Sea  $v \in \Sigma \setminus \{0\}$ ,  $w \in \Sigma$ ,  $w = (\sum_{x \in G} \alpha_x x)v$  porque todo módulo simple está generado por cualquiera de sus elementos. Pero entonces:

$$w = \sum_{x \in G} \alpha_x f_x(v) = \sum_{x \in G} \alpha_x \lambda_x v$$

luego  $\dim_{\mathbb{C}} \Sigma = 1$ .

□

**Corolario 18.** Si  $G$  es abeliano,  $n = |G|$ , entonces  $|\Sigma_{\mathbb{C}G}| = n$ .

*Demostración.*  $\Sigma_{\mathbb{C}G} = \{\Sigma_1, \dots, \Sigma_t\}$ , por el teorema de Webber-Artin,

$$\mathbb{C}G \cong \text{End}_{\mathbb{C}G}(\Sigma_1) \times \cdots \times \text{End}_{\mathbb{C}G}(\Sigma_t) \cong \mathbb{C} \times \cdots^{(t)} \times \mathbb{C}$$

con lo que  $n = t$ .

□

Ejemplo:  $G = \mathbb{Z}_n = \{0, 1, \dots, n-1\}$ . Tenemos que ver que  $\Omega_{\mathbb{C}G} = \{\Sigma_0, \dots, \Sigma_{n-1}\}$ , con  $\dim_{\mathbb{C}} \Sigma_j = 1$  para todo  $j \in \{1, \dots, n-1\}$ .

Sea  $u_j$  una base de  $\Sigma_j$  ( $\Sigma_j = \mathbb{C}u_j$ ). Sea  $\omega = e^{2\pi i/n} \in \mathbb{C}$ , ponemos  $ku_j := \omega^{kj}u_j$  para  $k \in \mathbb{Z}_n$ .

Es claro que  $(k+k')u_j = \omega^{kj+k'j}u_j = (k \circ k')u_j$  y el 0 va a la identidad.  $\Sigma_j$  es un  $\mathbb{C}\mathbb{Z}_n$ -módulo simple (tiene dimensión 1). Basta ver que ningún par de ellos son isomorfos entre sí.

Supongamos  $f : \Sigma_j \longrightarrow \Sigma_k$   $\mathbb{C}G$ -lineal y no nulo. Veamos que  $k = j$ .  
 $\exists \alpha \in \mathbb{C} \setminus \{0\}$  tal que  $f(u_j) = \alpha u_k$ .

$$\omega^j \alpha u_k = \omega^j f(u_j) = f(\omega^j u_j) = f(1u_j) = 1\alpha u_k = \alpha \omega_k u_k$$

Luego  $\omega^j = \omega^k$  y por tanto  $j = k$ .

Cada  $C(\Sigma_j)$  tiene como base  $\{t^{\Sigma_j}(k)\}$ , donde  $t^{\Sigma_j}(k) = ku_j = \omega^{kj}$ . Son una base ortonormal de  $\mu(\mathbb{Z}_n)$  respecto del producto interno:

$$\langle \varphi | \psi \rangle = \frac{1}{n} \sum_{k \in \mathbb{Z}_n} \varphi(k) \overline{\psi(k)}$$

Si  $\varphi \in \mu(\mathbb{Z}_n)$ ,  $\varphi = \sum_{j=0}^{n-1} \langle \varphi | t^{\Sigma_j} \rangle t^{\Sigma_j}$ . Es decir, obtenemos la transformada de Fourier Discreta.