Universidad de Granada

Álgebra Moderna

Pedro Ramos Suárez

Doble Grado de Ingeniería Informática y Matemáticas

7 de junio de 2022

Índice

0. Información de la asignatura

- Profesor: José Gómez Torrecillas.
- Tutorías: Martes y Miércoles, 9:00 - 12:00, Despacho 36.
- Evaluación:
  - 40 % entrega de ejercicios.
  - 30 % exposición de ejercicios.
  - 30 % examen final.

1. Repaso

Definición 1.1 (Anillo)
A conjunto.
$(A, +, 0)$ grupo abeliano (en ocasiones diremos "grupo aditivo").
$(A, \cdot, 1)$ monoide $\rightarrow$ algo menos que un grupo:

- *$\cdot$ es asociativa: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.*
- *1 es el neutro de $\cdot$: $a \cdot 1 = 1 \cdot a = a$.*
- *$\cdot$ no es necesariamente conmutativa.*
- *$a \in A$ no tiene por qué tener inverso.*
- *Propiedad distributiva:* $\begin{cases} (a+b) \cdot c = a \cdot c + b \cdot c \\ c \cdot (a+b) = c \cdot a + c \cdot b \end{cases}$

Ejemplos: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_n, \ldots$.

Se dice que A es conmutativo si $\cdot$ es conmutativo, esto es, si $a \cdot b = b \cdot a \quad \forall a, b \in A$.

Definición 1.2 (Ideales y anillos cociente o factor)
Sea A un anillo (no necesariamente conmutativo). Un ideal I de A es un subgrupo aditivo de A tal que $\forall x \in I$ y $\forall a \in A$, se tiene $ax, xa \in I$.

Nota: I es un subgrupo aditivo de A si $I \neq \emptyset, I \subseteq A$ y $\forall a, b \in I$, $a - b \in I$.

Consideramos el grupo aditivo ${}^{A}/_{I}$, en el que podemos considerar el producto $(a + I)(b + I) = ab + I$, $\forall (a + I), (b + I) \in {}^{A}/_{I}$.

La operación está bien definida, esto es, es independiente del representante escogido: si $a + I = a' + I$, $b + I = b' + I$, entonces $ab - a'b' = ab - a'b + a'b - a'b' = (a - a')b + a'(b - b') \in I \Rightarrow ab + I = a'b' + I$.

El neutro para este producto es $1 + {}^{A}/_{I}$, donde 1 es el neutro para el producto de A.

La suma en ${}^{A}/_{I}$ estaba definida por $(a + I) + (b + I) = a + b + I$.

Teníamos también la aplicación proyección:

$$\pi : A \rightarrow {}^{A}/_{I}$$

$$a \mapsto a + I$$

que verifica:

- $\pi(a)\pi(b) = \pi(ab)$.
- $\pi(a) + \pi(b) = \pi(a + b)$.

- $\pi(1) = 1 + I$.

$\Rightarrow \pi$ *es un homomorfismo de anillos.*

Teorema 1.3 (Isomorfía)
Sea $f : A \to B$ *un homomorfismo de anillos. Entonces el núcleo* $Kerf = \{a \in A / f(a) = 0\}$ *es un ideal de* A *y la imagen* $Imf = \{f(a)/a \in A\}$ *es un subanillo de* B. *Si* $I \in Kerf$ *es un ideal, entones existe un único homomorfismo de anillos* $\bar{f} : {}^{A}/_{I} \to B$ *tal que* $\bar{f}(a + I) = f(a), \forall a \in A$.

Además, $\bar{f}$ *es inyectivo* $\iff I = Kerf$, *en cuyo caso* $\bar{f}$ *es un isomorfismo de anillos* $\bar{f} : {}^{A}/_{Kerf} \to Imf$.

Definición 1.4 (Homomorfismo de anillos)
Sean A, B *dos anillos. Una aplicación* $f : A \to B$ *se dice un homomorfismo de anillos si para todo* $a, a' \in A$ *se tiene:*

- $f(a + a') = f(a) + f(a')$.
- $f(aa') = f(a)f(a')$.
- $f(1) = 1$.

Definición 1.5 (Anillos primos)
Dos ideales I, J *de un anillo* A *se dicen primos entre sí (o coprimos) si* $I + J = A$, *esto es, si:*

$$I + J = \{a + b / a \in I, b \in J\} = A$$

Equivalentemente, si $\exists x \in I, \exists y \in J$ *tales que* $x + y = 1$.

Nota: $I + J$, el ideal suma, es el menor ideal que contiene a $I \cup J$.

Ingredientes para el Teorema Chino del Resto

Sean $A, A_1, ..., A_t$ anillos y $f_i : A \to A_i, i \in \{1, ..., t\}$ homomorfismos de anillos. Recordemos que $Imf_i \subseteq A_i$ es un subanillo, $\forall i$. Tomamos el anillo producto $Imf_1 \times ... \times Imf_t$ y definimos:

$$f : A \to Imf_1 \times ... \times Imf_t$$

$$x \mapsto f(x) = (f_1(x), ..., f_t(x))$$

Es fácil demostrar que f es un homomorfismo de anillos.

Calculamos ahora el núcleo de f:

$$Kerf = \{x \in A / f(x) = 0\} \Rightarrow (x \in Kerf \iff f_i(x) = 0, \forall i \in \{1, ..., t\})$$

$$\Rightarrow (x \in Kerf \iff x \in \bigcap_{i=1}^{t} Kerf_i = Kerf)$$

En otras palabras, $I = \bigcap_{i=1} tKerf_i = Kerf$.

Por el Teorema de Isomorfía, sabemos que:

$$\begin{aligned} &\exists! \bar{f} : {}^{A}/_{I} \to Imf_1 \times ... \times f_t \text{ homomorfismo de anillos} \\ &\quad x + I \mapsto (f_1(x), ..., f_t(x)) \end{aligned}$$

que además es inyectivo.

El Teorema Chino del Resto nos dirá si $\bar{f}$ es también sobreyectiva ya que garantizará que $\bar{f}$ sea biyectiva bajo ciertas condiciones.

Lema 1.6
Sean I, J, K ideales de un anillo A. Entones:

$$I + J = I + K = A \iff I + (J \cap K) = A$$

Demostración. $\circledRightarrow$ $I + J = I + K = A \iff 1 = x + y = x' + z$, con $x, x' \in I, y \in J, z \in K$
$\Rightarrow 1 = x+y = x+y\cdot 1 = x+y(x'+z) = x+yx'+yz$, con $x+yx' \in I, yz \in J \cap K$
$\Rightarrow A = I + (J \cap K)$.

$\circledLeftarrow$ $A = I + J \cap K \subseteq I + J \subseteq A \Rightarrow I + J = A$.
$A = I + J \cap K \subseteq I + K \subseteq A \Rightarrow I + K = A$. □

Lema 1.7
$I_1, ..., I_t (t \geq 2)$ ideales de un anillo A. Entonces:

$$I_1 + I_i = A, \forall i \in \{2, ..., t\} \iff I_1 + \bigcap_{i=2}^{t} I_i = A$$

Demostración. Inducción sobre t.

- Caso $t = 2$ ya demostrado.
- Supuesta la implicación "⇒" cierta para t, veamos que es cierta para $t + 1$.
  Llamamos $I = I_1, J = \bigcap_{i=2}^{t} I_i, K = I_{t+1}$.
  Tomemos $I + J = A, I + K = A$ (hipótesis de inducción), por el lema anterior tenemos que $I + J \cap K = A \Rightarrow I + \bigcap_{i=2}^{t+1} I_i = A$.

  La implicación "⇐" se razona de forma análoga al lema anterior.

□

Teorema 1.8 (Teorema Chino del Resto)
Llamando $I_i = Kerf_i, \forall i \in \{1, ..., t\}$, tenemos que:

$$\bar{f} \text{ es un isomorfismo} \iff I_i + I_j = A, \forall i \neq j$$

Demostración. Teníamos $I = \bigcap_{i=1}^{t} I_i, \bar{f} : {}^{A}/_{I} \to Imf_1 \times ... \times f_t$.

$\circledRightarrow$ Dado $i \in \{1, ..., t\}$, tomamos $x \in A$ tal que $f_i(x) = 1$ y $f_j(x) = 0, \forall i \neq j$, que debe existir pues, al ser $\bar{f}$ isomorfismo, para cada $(y_1, ..., y_t) \in Imf_1 \times ... \times f_t, \exists (x + I) \in {}^{A}/_{I}$ tal que $\bar{f}(x + I) = f(x) = (y_1, ..., y_t)$.

Por lo tanto, tenemos $x-1 \in I_i$, pues $f_i(x-1) = 0$, y $x \in \bigcap_{j \neq i} I_j$. Consideramos $1 = 1 - x + x \in I_i + \bigcap_{j \neq i} I_j \Rightarrow I_i + \bigcap_{j \neq i} I_j = A \underset{\text{(lema)}}{\Rightarrow} I_i + I_j = A, \forall i \neq j$.

$\circledLeftarrow$ Un elemento de $Imf_1 \times ... \times Imf_t$ es de la forma $(f_1(b_1), ..., f_t(b_t)$, con $b_i in A, \forall i \in \{1, ..., t\}$.

Para cada $i \in \{1, ..., t\}$, tomamos $1 = a_i + p_i$, con $a_i \in I_i, p_i \in \bigcap_{j \neq i} I_j$, que existen como resultado del lema anterior.
Llamamos $x = \sum_{i=1}^{t} b_i p_i$. Tenemos $f(x) = (f_1(x), ..., f_t(x))$, luego:

$$f_j(x) = f_j(\sum_{i=1}^{t} b_i p_i) = \sum_{i=1}^{t} f_j(b_i p_i) = \sum_{i \neq j} f_j(b_i) \underbrace{f_j(p_i)}_{=0} + f_j(b_j f_j(p_j) =$$

$$= f_j(b_j p_j) = f_j(b_j(1 - a_j)) = f_j(b_j) - \underbrace{f_j(b_j a_j)}_{=0} = f_j(b_j)$$

De este modo, hemos encontrado un elemento $x \in A$ tal que
$f(x) = (f_1(b_1), ..., f_t(b_t)) \Rightarrow f$ sobreyectiva $\Rightarrow \bar{f}$ sobreyectiva. $\square$

Caso particular

$A = K[X]$ anillo de polinomios sobre un cuerpo $K, A_i = K, \forall i \in \{1, ..., t\}$, $\alpha_1, ..., \alpha_t \in K$.

Definimos $\mathcal{X}_i : K[X] \to K, \mathcal{X}_i(g) = g(\alpha_i)$, que es un homomorfismo de anillos. Es evidente que $Im\mathcal{X}_i = K, \forall i$.

Definimos entonces $\mathcal{X} : K[X] \to K^t, \mathcal{X}(g) = (g(\alpha_1), ..., g(\alpha_t))$. Se tiene que $Ker\mathcal{X}_i =< x - \alpha_i >$.

Notación: Si A es un anillo conmutativo (como en el caso del anillo de polinomios) y $a \in A$, se denota por $< a >= \{ba / b \in A\}$ el ideal principal generado por a.

Recordatorio: $Ker\mathcal{X}_i = \{g \in A = K[X] / \mathcal{X}_i(g) = g(\alpha_i) = 0\}$, esto es, $Ker\mathcal{X}_i$ es el conjunto de los polinomios que se anulan en α_i. Para calcular $Ker\mathcal{X}_i$, hay que buscar el polinomio mónico de menor grado contenido en $Ker\mathcal{X}_i$. En el caso anterior, $x - \alpha_i$ es mónico, de grado 1 y contenido en $Ker\mathcal{X}_i$, luego hemos acabado. En general, esto no tiene por qué ser siempre así, si fuese $a \notin K$ (por ejemplo, en $\mathbb{Z}[X]$, si definimos $\mathcal{X}_i$ como $\mathcal{X}_i(g) = g(i)$, donde i es la unidad imaginaria, tenemos que $\mathcal{X}_i : \mathbb{Z}[X] \to \mathbb{C}$ y $Ker\mathcal{X}_i \neq < x - i >$,

porque no tiene sentido escribir $< x - i >$ como ideal de $\mathbb{Z}[X]$ ya que $i \notin \mathbb{Z}$. En este caso, $Ker\mathcal{X}_i =< x^2 + 1 >$).

En consecuencia, $I = \bigcap_{i=1}^{t} < x - \alpha_i >=< p(x) >$, donde $p(x)$ es el polinomio $p(x) = \text{mcm}\{x - \alpha_1, ..., x - \alpha_t\}$.

El TCR nos dice que $\bar{\mathcal{X}} : {}^{K[X]}/_{< p(x) >} \to K^t$ es un isomorfismo si, y sólo si, $\text{mcd}\{x - \alpha_i, x - \alpha_j\} = 1, \forall i \neq j \iff \alpha_i \neq \alpha_j, \forall i \neq j$.

Nota:

- $< p_1(x) > \cap < p_2(x) >=< \text{mcm}\{p_1(x), p_2(x)\} >$.
- $< p_1(x) > + < p_2(x) >=< \text{mcd}\{p_1(x), p_2(x)\} >$.

Nota: En realidad ya sabíamos que $\forall (y_1, ..., y_t) \in K^t, \exists g(x) \in K[X]$ tal que $g(\alpha_i) = y_i, \forall i \in \{1, ..., t\} \iff \alpha_i \neq \alpha_j, \forall i \neq j$ (interpolación en nodos distintos). En tal caso, $p(x) = \prod_{i=1}^{t}(x - \alpha_i) \Rightarrow p(x)$ es de grado t.

En consecuencia, en $\frac{K[X]}{I} = \frac{K[X]}{<p(x)>}$ habrá un único representante de cada clase de grado menor que t ($\Rightarrow$ si $\alpha_i \neq \alpha_j$, se tiene que $\forall (y_1, ..., y_t) \in K^t, \exists! g(x) \in K[X]$ de grado menor que t y tal que $g(\alpha_i) = y_i, \forall i$).

Sean entonces $\alpha_1, ..., \alpha_t \in K$, con $\alpha_i \neq \alpha_j, \forall i \neq j$. Consideramos $\bar{\mathcal{X}} : \frac{K[X]}{<p(x)>} \to K^t$ isomorfismo de anillos. Además, $\frac{K[X]}{<p(x)>}$ también es un espacio vectorial sobre K, pues es el espacio vectorial cociente del espacio vectorial $K[X]$ sobre el subespacio vectorial $< p(x) >$.

Concretamente, dado $\alpha \in K$ y dado $g + < p(x) > \in \frac{K[X]}{<p(x)>}$, definíamos:

$$\alpha \cdot (g + < p(x) >) = \alpha g + < p(x) > \equiv (\alpha + < p(x) >)(g + < p(x) >)$$

Básicamente, estamos diciendo que la multiplicación por escalares de la estructura de espacio vectorial se hereda del producto interno del anillo.

Tenemos entonces que $\bar{\mathcal{X}}$ es un homomorfismo de espacios vectoriales (es lineal), pues sabemos que $\bar{\mathcal{X}}(f + g) = \bar{\mathcal{X}}(f) + \bar{\mathcal{X}}(g)$ (ya que la suma es la misma, al haber la misma estructura de grupo aditivo adyacente a las estructuras de espacio vectorial y de anillo), y por otra parte,

$$\bar{\mathcal{X}}(\alpha(g + < p(x) >) = \bar{\mathcal{X}}((\alpha + < p(x) >)(g + < p(x) >)) =$$

$$= (\alpha, ..., \alpha)(g(\alpha_1), ..., g(\alpha_t)) = (\alpha g(\alpha_1), ..., \alpha g(\alpha_t)) = \alpha \bar{\mathcal{X}}(g + < p(x) >)$$

Notación: $\underset{\text{Clase de equivalencia}}{x} = x + < p(x) > \in \frac{K[X]}{<p(x)>}$.

Una K-base de $\frac{K[X]}{<p(x)>}$ es $\{1 + < p(x) >, x + < p(x) >, ..., x^{t-1} + < p(x) > \} = \{1, x, x^2, ..., x^{t-1}\}$.

Tomamos en K^t la k-base canónica.
Sabemos que en $\frac{K[X]}{<p(x)>}$ hay un único representante de cada clase de grado menor que t. Para encontrarlo, definimos $L_i = \frac{g_i(x)}{g_i(\alpha_i}$, con $g_i(x) = \prod_{i \neq j}(x - \alpha_j)$, que verifica que $\mathcal{X}(L_i(\alpha_1), ..., L_i(\alpha_t)) = (0, 0, ..., 0, \overset{(i)}{1}, 0, ..., 0) = e_i$.
A los L_i se les denomina "interpoladores de Lagrange".
Dado entonces $(y_1, ..., y_t) \in K^t$, el polinomio $g(x) = \sum_{i=1}^{t} y_i L_i(x)$ satisface $g(\alpha_i) = y_i, \forall i \in \{1, ..., t\}$.
$\Rightarrow$ La interpolación es un caso particular del Teorema Chino del Resto.

Tenemos $\{1, x, ..., x^{t-1}\}$ base de $\frac{K[X]}{<p(x)>}$ y $\{e_1, ..., e_t\}$ base de K^t. La matriz de $\bar{\mathcal{X}}$ en estas bases (por filas) es:

$$M = \begin{pmatrix} 1 & 1 & ... & 1 \\ \alpha_1 & \alpha_2 & ... & \alpha_t \\ \alpha_1^2 & \alpha_2^2 & ... & \alpha_t^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{t-1} & \alpha_2^{t-1} & ... & \alpha_t^{t-1} \end{pmatrix}$$

Es invertible, por se la matriz de un isomorfismo de e.v.
$\bar{\mathcal{X}}$ es lineal y biyectiva (pues es isomorfismo de anillos), luego $\bar{\mathcal{X}}$ es isomorfismo de espacios vectoriales.

Aplicación: Transformada Discreta de Fourier

Supongamos que K contiene una raíz n-ésima primitiva de la unidad (como es el caso de $\mathbb{C}, \forall n$, pero no de $\mathbb{R}$, salvo $n = 2$), esto es, $\exists w \in K$ tal que $w^n = 1$ y $1, w, w^2, ..., w^{n-1}$ son distintos. Esto implica que $car K \nmid n$, ya que $1, w, ..., w^{n-1}$ son las raíces del polinomio $x^n - 1 \in K[X]$.

Tomamos entonces $\alpha_j = w^j, \forall j \in \{0, ..., n-1\}$ y definimos:

$$M = A_w = \begin{pmatrix} 1 & 1 & ... & 1 \\ \alpha_0 & \alpha_1 & ... & \alpha_{n-1} \\ \alpha_0^2 & \alpha_1^2 & ... & \alpha_{n-1}^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_0^{n-1} & \alpha_1^{n-1} & ... & \alpha_{n-1}^{n-1} \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 1 & ... & 1 \\ w^0 & w^1 & ... & w^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ (w^0)^{n-1} & (w^1)^{n-1} & ... & (w^{n-1})^{n-1} \end{pmatrix} = (w^{ij})$$

Como $w^j \neq 1, \forall 0 < j < n$ y w^j es raíz de $x^{n-1} = (x-1)(x^{n-1} + ... + 1) \Rightarrow (w^j - 1)(w^{(n-1)j} + ... + w^j + 1) = 0 \Rightarrow w^{(n-1)j} + .. + w^j + 1 = 0$.

En consecuencia, $\sum_{k=0}^{n-1} w^{ik} = 0, \forall i \in \{1, ..., n-1\}$.
Como además, $w^n = 1 \Rightarrow w^{-i} = w^n w^{-i} = w^{n-i}$, y por lo tanto se tiene:

- Si $i > j$: $\sum_{k=0}^{n-1} w^{k(i-j)} = 0$, pues $i - j \in \{1, ..., n-1\}$.
- Si $i < j$: $\sum_{k=0}^{n-1} w^{k(i-j)} = \sum_{k=0}^{n-1} w^{nk} w^{k(i-j)} = \sum_{k=0}^{n-1} w^{k(n+(i-j))} = 0$, pues $n + (i - j) \in \{1, ..., n-1\}$.
- Si $i = j$: $\sum_{k=0}^{n-1} w^{k(i-j)} = \sum_{k=0}^{n-1} 1 = n$.

En resumen,

$$\begin{pmatrix} w^i & w^{2i} & ... & w^{(n-1)i} \end{pmatrix} \begin{pmatrix} w^{-j} \\ w^{-2j} \\ \vdots \\ w^{-(n-1)j} \end{pmatrix} = n\delta_{ij}$$

En conclusión, $A_w A^T_{w^{-1}} = nI_n \Rightarrow A_w^{-1} = \frac{1}{n} A^T_{w^{-1}}$.

Por otra parte, teníamos $\bar{\mathcal{X}} : \frac{K[X]}{<p(x)>} \to K^n, \bar{\mathcal{X}}(g + < p(x) >) = \mathcal{X}(g)$, con $\mathcal{X}(g) = (g(w^0), g(w^1), ..., g(w^{n-1})) = (g(1), g(w), ..., g(w^{n-1}))$, y sabíamos que $\bar{\mathcal{X}}$ era un isomorfismo.

Dado entonces $y = (y_0, ..., y_{n-1}) \in K^n, \bar{\mathcal{X}}^{-1}(y)$ es el único polinomio (en realidad, clase de equivalencia $\equiv$ único representante de grado menor que n) de grado menor que n tal que $\mathcal{X}(g) = y$, o lo que es lo mismo, $\bar{\mathcal{X}}(g + < p(x) >) = y$ ó $g(w^i) = y_i, \forall i$.

Resumiendo: $\bar{\mathcal{X}}$ evaluar, $\bar{\mathcal{X}}^{-1}$ interpolar.

Si tenemos entonces $y = (y_0, ..., y_{n-1}) \in K^n$, el polinomio interpolador de esos datos en los nodos $1, w, ..., w^{n-1}$ viene dado por $\hat{y} = \sum_{j=0}^{n-1} \hat{y}_j x^j$, donde $(\hat{y}_0, ..., \hat{y}_{n-1}) = (y_0, ..., y_{n-1}) \frac{1}{n} A^T_{w^{-1}}$.
Explícitamente, $\hat{y}_j = \frac{1}{n} \sum_{k=0}^{n-1} y_k w^{-jk}$.

Caso particular: $K = \mathbb{C} \to$ la suposición anterior de que existe una raíz n-ésima de 1 es cierta, $\forall n$.
Entonces $w = e^{2\pi/n}$, de modo que $\hat{y}_j = \frac{1}{n} \sum_{k=0}^{n-1} y_k e^{-2\pi ijk/n}$, que es la transformada de Fourier de y.

Interpretación: Tenemos f función 2π-periódica, y la conocemos en $[0, 2\pi]$, esto es, tenemos $f : [0, 2\pi] \to \mathbb{C}$.
Tomamos como muestra $y_j = f(\frac{2\pi j}{n}), \forall j \in \{0, ..., n-1\}$, y tomamos $g : [0, 2\pi] \to \mathbb{C}$ dada por $g(t) = \sum_{k=0}^{n-1} \hat{y}_k e^{itk}$.
Evaluando esta función en los nodos tenemos que $g(\frac{2\pi j}{n}) = \sum_{k=0}^{n-1} \hat{y}_k e^{2\pi ijk/n} = y_j = f(\frac{2\pi j}{n}), \forall j \in \{0, ..., n-1\}$.

Nota: A $\hat{y} = (\hat{y}_0, ..., \hat{y}_{n-1})$ se le denomina "espectro" de f.

Nota:

$$\sum_{k=0}^{n-1} \hat{y}_k e^{2\pi ijk/n} = \sum_{k=0}^{n-1} (\sum_{l=0}^{n-1} \frac{1}{n} y_l e^{-2\pi ilk/n}) e^{2\pi ijk/n} = \frac{1}{n} \sum_{l=0}^{n-1} y_l \sum_{k=0}^{n-1} e^{2\pi ik(j-l)/n} =$$

$$= \frac{1}{n} \sum_{l=0}^{n-1} y_l \sum_{k=0}^{n-1} w^{k(j-l)} = \frac{1}{n} \sum_{l=0}^{n-1} y_l n \delta_l = y_j$$

Esto es general (y esperable, pues es el polinomio interpolador):

$$\hat{y} = \sum_{j=0}^{n-1} \hat{y}_j x^j \Rightarrow \hat{y}(w^l) = \sum_{j=0}^{n-1} (\frac{1}{n} \sum_{k=0}^{n-1} y_k w^{-jk}) w^{lj} = y_l$$

2. Módulos

Definición 2.1 (Módulos)
Sean M, N grupos aditivos. Definimos $Ad(M,N) =$
$= \{f : M \to N$ homeomorfismos$\}$. Entonces $Ad(M,N)$ es un grupo aditivo con la suma dada para cada $f, g \in Ad(M,N)$, por $f+g : M \to N, (f+g)(m) = f(m)+g(m), \forall m \in M$.

Definimos $End(M) = Ad(M,M)$, denominado "anillo de endomorfismos de M".

Proposición 2.2
$(End(M), +, 0, \circ, id_m)$ es un anillo.

Demostración. Hay que comprobar:

- $f, g \in End(M) \Rightarrow f \circ g \in End(M)$.
- $\circ$ es asociativa.
- $(f+g)\circ h = f\circ h + g\circ h$ y $h\circ(f+g) = h_0 f + h\circ g, \forall f, g, h \in End(M)$.

□

Ejemplo 2.3
$End(\{0\}) = \{0\}$ se llama anillo cero o trivial. Si $M \neq \{0\} \Rightarrow End(M) \neq \{0\}$, pues contiene al menos dos elementos: el cero y la identidad.

Definición 2.4 (A-Módulo)
Sea M un grupo aditivo, y A un anillo. Una estructura de A-módulo sobre M es un homomorfismo de anillos $\rho : A \to End(M)$.

Ejemplo 2.5
$A = \mathbb{Z}$ y M grupo aditivo $\to$ hay una única estructura de $\mathbb{Z}-$módulo, pues $\rho(1) = \underset{=id_M}{1}, \rho(2) = 1+1$, etc. $\to$ todas las imágenes están determinadas $\to$ además, el núcleo de este homomorfismo dará la característica de $End(M)$.

Ejemplo 2.6
Sea K un cuerpo y $A = K$. Veamos que un $K-$ espacio vectorial es un $K-$módulo.
Si V es un $K-$espacio vectorial, definimos $\rho : K \to End(V)$ por $\rho(\alpha) : V \to V \mid \rho(\alpha)(v) = \alpha v, \alpha \in K, v \in V$. Con esta definición, ρ es un homomorfismo de anillos (ejercicio). En consecuencia, V tiene también la estructura de $K-$módulo.

Nos podemos preguntar lo contrario, ¿todo $K-$módulo tiene la estructura de espacio vectorial? La respuesta es sí.

Notación: En lugar de decir que M tiene una estructura de $A-$módulo, diremos que M es un $A-$módulo.

Observación: Sean X, Y, Z conjuntos. Denotamos $Map(X,Y) = \{f : X \to Y \text{ aplicación}\}$. Consideramos $Map(X \times Y, Z) \overset{\mathcal{X}}{\cong} Map(X, Map(Y,Z))$, pues $\mathcal{X}$ viene dado por $f : X \times Y \to Z$:

$$\begin{aligned} \mathcal{X}(f) : X \to & \quad Map(Y,Z) \\ x \mapsto & \quad \mathcal{X}(f)(x) : Y \to Z \\ & \qquad\qquad y \mapsto f(x,y) \end{aligned}$$

$$\begin{aligned} \mathcal{X}^{-1}(f) : Map(X, Map(Y,Z)) \to & \quad Map(X \times Y, Z) \\ g \mapsto & \quad \varphi^{-1}(g) : X \times Y \to Z \\ & \qquad (x,y) \mapsto \varphi^{-1}(g)(x,y) = g(X)(y) \end{aligned}$$

Se comprueba que efectivamente $\mathcal{X}^{-1}$ es la inversa de φ.

Consideramos la observación anterior que en lugar de conjuntos tenemos grupos aditivos M, N, L.
Se tiene entonces $Ad(M, Ad(N,L)) \subseteq Map(M, Map(N,L))$. Pero sabemos además que $\varphi^{-1} : Map(M, Map(N,L)) \to Map(M \times N, L)$ es una biyección. Se puede comprobar que $Im(\varphi^{-1}_{|_{Ad(M,Ad(N,L))}}) = Biad(M \times N, L)$, donde $b \in Biad(M \times N, L)$ si b es biaditiva, esto es, si:

$$\forall m, m' \in M, n, n' \in N \begin{cases} b(m+m', n) = b(m,n) + b(m',n) \\ b(m, n+n') = b(m,n) + b(m',n) \end{cases}$$

Si A es un anillo, entonces podemos considerar:

$$\begin{array}{ccc} Biad(A \times M, M) & \overset{\varphi}{\to} & Ad(A, Ad(M,M)) \\ & & \bigcup | \\ \underset{\text{Noción de A-módulo en muchos textos}}{?} & \overset{\varphi^{-1}}{\leftarrow} & Ring(A, End(M)) \end{array}$$

Proposición 2.7
Dados un grupo aditivo M y un anillo A, se tiene una correspondencia biyectiva entre:

- *Los homomorfismos de anillos, $\rho : A \to EndM$.*
- *Las aplicaciones $\cdot : A \times M \to M$ que satisfacen:*
  - *a)* $(a+a') \cdot m = a \cdot m + a' \cdot m, \forall a, a' \in A, \forall m \in M$.
  - *b)* $a \cdot (m+m') = a \cdot m + a \cdot m', \forall a \in A, \forall m \in M$.

c) $(aa') \cdot m = a \cdot (a' \cdot m), \forall a, a' \in A, \forall m \in M.$

d) $1 \cdot m = m, \forall m \in M.$

Demostración. Tomamos la biyección $Map(A, Map(M, M)) \underset{\psi^{-1}}{\overset{\psi}{\leftrightarrows}} Map(A \times M, M)$. Para dos anillos R, S, llamo $Ring(R, S) = \{\varphi : R \to S$ homomorfismo de anillos $\}$. Consideramos $Ring(A, EndM) \subseteq Map(A, Map(M, M))$ y tomamos $Im(\psi^{-1}_{|_{Ring(A,EndM)}})$, que serán las aplicaciones $\varphi \in Map(A \times M, M)$ que satisfacen $a), ..., d)$. $\circledast$

Análogamente, se comprueba que si $\varphi \in Map(A \times M, M)$ verifica $a), b), c), d)$, entonces $\psi(\varphi) \in Ring(A, EndM)$. En conclusión, ambos conjuntos son biyectivos. Esta biyección corresponde a la fórmula $a \cdot m = \rho(a)(m)$.

En resumen, podemos ver un $A-$módulo como un homomorfismo de anillos $\rho : A \to EndM$, o como una acción de A sobre M. □

Ejercicio 2.8 ($\circledast$)
Si $\rho \in Ring(A, EndM) \Rightarrow \psi^{-1}(\rho)$ verifica $a), b), c), d)$. Por ejemplo, para $c)$ vemos que dados $a, a' \in A, m \in M$ se cumple que $(aa') \cdot m = a \cdot (a' \cdot m)$. Llamamos $\psi^{-1}(\rho)(a, m) = a \cdot m$. Como $\psi^{-1}(\rho)(a, m) = \rho(a)(m) \Rightarrow a \cdot m = \rho(a)(m)$.
Consideramos $(aa') \cdot m = \rho(aa')(m) = (\rho(a) \cdot \rho(a'))(m) = \rho(a)(\rho(a')(m)) = \rho(a)(a' \cdot m) = a \cdot (a' \cdot m)$.

Nota: $\cdot$ es una acción de A sobre M (por la izquierda).

Notación: Se suele abreviar $am = a \cdot m$.

Ejemplo 2.9
Como ya se adelantó, si K es un cuerpo, es lo mismo un $K-$módulo que un $K-$espacio vectorial.

Ejemplo 2.10 (Módulo regular)
A es un $A-$módulo, tomando

$$\begin{array}{rlll} \lambda : A & \to EndA & & \\ a & \mapsto \lambda(a) : \quad A \to A & & \Rightarrow \lambda(a)(a') = aa') a \cdot a' \\ & \qquad\qquad a' \mapsto & aa' & \end{array}$$

$\Rightarrow$ Eso da coherencia a la notación anterior, pues en el caso $M = A$ es lo mismo.

Restricción de escalares

Sea $\varphi : R \to S$ un homomorfismo de anillos y sea M un $S-$módulo vía un homomorfismo de anillos $\rho : S \to EndM$. Entonces M es también un

$R-$módulo vía $\rho_o\varphi : R \to EndM$ (que es homomorfismo de anillos).

$$R \xrightarrow{\varphi} S \underset{\rho_o\varphi}{\xrightarrow{\rho}} EndM$$

Equivalentemente, si $r \in R$ y $m \in M$, definimos $r \cdot m = (\rho_o\varphi)(r)(m) = \rho(\varphi(r))(m) = \varphi(r) \cdot m$.

Definición 2.11 ($K[X]-$módulos (K cuerpo))
Sea M un $K[X]-$módulo, esto es, M es un grupo aditivo y tenemos un homomorfismo de anillos $\rho : K[X] \to EndM$.
Podemos ver K como subanillo de $K[X]$. En consecuencia, la aplicación inclusión $i : K \hookrightarrow K[X]$ es un homomorfismo de anillos. Por restricción de escalares, deducimos que M es también un $K-$módulo $\to K-$espacio vectorial.

Veamos como actúa ρ. Tomamos $\rho(x) \in EndM$. Veamos que $\rho(x)$ es lineal: dado $m \in M, \alpha \in K$, tenemos que $\rho(x)(\alpha m) = x \cdot (\alpha m) \underset{\alpha \cong i(\alpha) \in K[X]}{=} x \cdot (\alpha \cdot m) = (xa) \cdot m \underset{\text{el anillo de polinomios es conmutativo}}{=} (\alpha x) \cdot m = \alpha \cdot (x \cdot m) = \alpha\rho(x)(m)$.

De este modo, $\rho(x) \in End_K(M) \to$ endomorfismo $K-$lineal. En consecuencia, ya tenemos ρ completamente caracterizado:

$$Si \sum_i p_i x^i \Rightarrow \rho(p) = \rho(\sum_i p_i x^i) \underset{\rho \text{ lineal}}{=} \sum_i \rho(p_i x^i) \underset{p \text{ lineal}}{=} \sum_i p_i \rho(x^i) =$$

$$\underset{\rho \text{ homomorfismo de anillos}}{=} \sum_i p_i \rho(x)^i$$

En conclusión, $\rho(p)(m) = p(x)(m) = p(x)m$.
Si tengo un $K-$espacio vectorial V y una aplicación lineal $T : V \to V$, podemos definir para cada $p \in K[x]$ y $v \in V, \rho(T)(v) = (\sum_i p_i T^i)(v) = \sum_i p_i T^i(v) := p(x) \cdot v \Rightarrow V$ es un $K[x]$-módulo.

Ejemplo 2.12
$C^\infty(\mathbb{R})$ es un $\mathbb{R}-$espacio vectorial. Tomamos $T = \frac{d}{dt}$, esto es, $T(f) = f'$. Entonces $T \in End_{\mathbb{R}}(C^\infty(\mathbb{R}))$. En consecuencia, $C^\infty(\mathbb{R})$ es un $\mathbb{R}[x]-$módulo.

$C^\infty(\mathbb{R})$ dotado de estructura de $R[X]-$módulo a través del endomorfismo lineal $T : C^\infty(\mathbb{R}) \to C^\infty(\mathbb{R}), T(f) = f'$, para $f \in C^\infty(\mathbb{R})$.

$$sint \in C^\infty(\mathbb{R})$$

$$Xsint = T(sint) = cost$$

$$X^2 sint = X(Xsint) = Xcost = -sint = -1sint$$

$$(X^2+1)sint = 0$$

En un $A-$módulo M, puede pasar que $am = 0$ con $a \neq 0, m \neq 0$.

Ejemplo: En el $\mathbb{Z}-$modulo $\mathbb{Z}_4$ ocurre que $\bar{2} \cdot \bar{2} = \bar{0}$.

Definición 2.13 (Módulos abstractos)
Sean A un anillo, M un $A-$módulo ($_AM$), $\varphi : A \to End(M)$ homomorfismo de anillos.
$Ker\varphi$ es un ideal de A y el Primer Teorema de Isomorfía nos dice que:

$$\frac{A}{Ker\varphi} \xrightarrow{\sim} Im\varphi \subseteq End(M) \Rightarrow M \text{ es un } \frac{A}{Ker\varphi} - \text{modulo}$$

De hecho, $(a + Ker\varphi)m = \varphi(a)m$.

$$Ker\varphi = \{a \in A \mid \varphi(a) = 0\} = \{a \in A \mid \varphi(a)(m) = 0\} =$$

$$= \{a \in A \mid am = 0\} = Ann_A(M)$$

$Ann_A(M) \equiv$ *"Anulador de M".*

$$(a + Ann_A(M)) \cdot m = am$$

Ejercicio 2.14
$T : V \to V$ aplicación $K-$lineal.

$$Ann_{K[X]}(V) =< \mu(x) >$$

Demostrar que si $dim_K V < \infty \Rightarrow \mu(x) \neq 0$ (polinomio mínimo de T).

Definición 2.15 (Submódulo)
Un submódulo de un módulo $_AM$ es un subgrupo aditivo N de M tal que:

$$an \in N, \forall a \in A, \forall m \in N$$

Los submódulos del módulo regular A se llaman ideales a izquierda de A.

Observación: Todo ideal es un ideal a izquierda.
Si A es conmutativo, los ideales y los ideales a izquierda son los mismos.

Ejemplo 2.16
Tomo $A = M_2(K)$ con K cuerpo.

$$M_2(K) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in K\}$$

$\{\begin{pmatrix} 0 & b \\ 0 & d \end{pmatrix} : b, d \in K\}$ *es un ideal a izquierda, pero no es un ideal.*

Ejemplo 2.17
$V \xrightarrow{T} V, K-lineal \rightarrow_{K[X]} V$.
W es un $K[X]-$submódulo si W es un $K-$espacio vectorial y además:

$$T(w) = Xw \in W, \forall w \in W$$

W es $T-$invariante.
W es $K[X]-$submódulo $\iff$ W es $K-$subespacio de V tal que $T(W) \subseteq W$.

Definición 2.18
A anillos, ${}_AM$ módulo.

$$\mathcal{L}({}_AM) \equiv \text{ Conjunto de los submódulos de } M$$

Definición 2.19 (Submódulo cíclico)
Dado ${}_AM$ y $m \in M$. Es claro que $Am = \{am : a \in A\}$ es un submódulo de ${}_AM$ llamado submódulo cíclico generado por m.

Ejemplo 2.20
$\mathbb{R}[X] \sin t = \{a \sin t + b \sin' t + c \sin'' t + ...\} = \{a \sin t + b \cos t : a, b \in \mathbb{R}\}$.

Definición 2.21 (Generadores de un submódulo)
Si $m_1, ..., m_n \in M, Am_1 + ... + Am_n = \{a_1m_1 + ... + a_nm_n : a_1, ..., a_n \in A\}$ es un submódulo generado por $m_1, ..., m_n$.

Si $M = Am_1 + ... + Am_n$, diremos que M es finitamente generado con generadores $m_1, ..., m_n$.

Definición 2.22 (Suma de submódulos)
Dados $N_1, ..., N_n$ submódulos de ${}_AM$, defino:

$$N_1 + ... + N_n = \{m_1 + ... + m_n : m_i \in N_i, \forall i \in \{1, ..., n\}\}$$

que es un submódulo de M llamado "suma" de $N_1 + ... + N_n$.

Notación: $N_1 + ... + N_n = \sum_{i=1}^{n} N_i = \sum N_i$.

Proposición 2.23
Sean $N_1, ..., N_t$ submodulos de ${}_AM$. Son equivalentes:

a) Para cada $i \in \{1, ..., t\}, N_i \cap \sum_{j \neq i} N_j = \{0\}$.

b) Si $0 = n_1 + ... + n_t, n_i \in N_i \Rightarrow n_i = 0, \forall i \in \{1, ..., t\}$.

c) Cada $n \in N_1 + ... + N_t$ admite una expresión única como:

$$n = n_1 + ... + n_t \text{ con } n_i \in N_i$$

Demostración. *a) $\Rightarrow$ b)*: $0 = n_1 + ... + n_t \Rightarrow$
$\Rightarrow -n_i = \sum_{j \neq i} n_j \in N_i \cap (\sum_{j \neq i} N_j) \overset{a)}{=} \{0\} \Rightarrow -n_i = 0 \Rightarrow n_i = 0.$

$\underline{b) \Rightarrow c)}$: Si $n = n_1 + ... + n_t = n_1' + ... + n_t'$ con $n_i, n_i' \in N_i \Rightarrow 0 = \underset{\in N_1}{n_1 - n_1'} + n_2 - \underset{\in N_2}{n_2'} + ... + n_t - \underset{\in N_t}{n_t'} \Rightarrow n_i = n_i', \forall i \in \{1, ..., t\}$.

$\underline{c) \Rightarrow a)}$: Si $n \in N_i \cap \sum_{j \neq i} N_j \Rightarrow n = \sum_{j \neq i} n_j$ con $n_j \in N_j \Rightarrow 0 = n - \sum_{j \neq i} n_j \overset{c)}{\Rightarrow} n = 0$. □

Definición 2.24 (Suma directa interna)
Si $M = N_1 + ... + N_t$ tal que $N_1, ..., N_t$ satisfacen a), diré que $M = N_1 + ... + N_t$ es una suma directa interna y usaré la notación $M = N_1 \dot{+} ... \dot{+} N_t$.

Nota: Cualquiera de estos N_i puede ser $\{0\}$ ($M + \{0\} = M$).

Definición: Si $\{N_1, ..., N_t\}$ verifican a) y $N_i \neq \{0\}, \forall i \in \{1, ..., t\}$, diré que $\{N_1, ..., N_t\}$ es una familia independiente.

Ejemplo 2.25
: $\mathbb{Z}_6$ es un $\mathbb{Z}-$módulo, $Z_6 = \{0, 1, 2, 3, 4, 5\}$.
$N_1 = \{0, 3\}, N_2 = \{0, 2, 4\}, N_1 \cap N_2 = \{0\} \Rightarrow \{N_1, N_2\}$ familia independiente.

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

Módulos acotados sobre un DIP

Sean A DIP (Dominio de ideales principales), ${}_AM$ un módulo y
$Ann_A(M) =< \mu >$ para cierto $\mu \in A$.
Si $\mu \neq 0$, diré que M es acotado. Supongamos que ${}_AM$ es acotado y $\mu \notin \underset{\text{Unidades}}{\mathcal{U}(A)}$ (ya que si $\mu \in \mathcal{U}(A) \Rightarrow M = \{0\}$).

$$\mu) p_1^{e_1} ... p_t^{e_t}, p_i \in A \text{ irreducible y } e_i > 0, \forall i \in \{1, ..., t\}$$

Definimos:

$$q_i = \frac{\mu}{p_i^{e_i}} = p_1^{e_1} ... p_{i-1}^{e_{i-1}} p_{i+1}^{e_{i+1}} ... p_t^{e_t}, i \in \{1, ..., t\}$$

$$M_i = \{q_i m : m \in M\} \subseteq M \qquad M_i \in \mathcal{L}({}_AM)$$

Queremos $M = M_1 \dot{+} ... \dot{+} M_t$ (supongo $t > 1$).

$$mcd(q_1, ..., q_t) = 1 \Rightarrow 1 = \sum_{i=1}^{t} q_i a_i \text{ para ciertos } a_i \in A$$

$m \in M, m = 1 \cdot m = (\sum_{i=1}^t q_i a_i) = \sum_{i=1}^t q_i a_i m \Rightarrow M = M_1 + ... + M_t$.

Veamos que es $\dot{+}$:

$$q_i q_j \in < \mu > \text{ si } i \neq j \iff (\text{si } m \in M_i \Rightarrow q_j m = 0 \text{ si } i \neq j) \Rightarrow$$

$$\Rightarrow M_i = \{m \in M : m = q_i a_i m\}$$

Si $0 = \sum_{i=1}^{t} m_i, m_i \in M_i \overset{b)}{\Rightarrow} 0 = q_i a_i 0 = m_j, \forall j \in \{1, ..., t\} \Rightarrow M = M_1 \dot{+} ... \dot{+} M_t$.

Proposición 2.26
Es claro que

$$M_i = \{m \in M : p_i^{e_i} m = 0\} \Rightarrow Ann_A(M_i) =< p_i^{e_i} >$$

Así, $< \mu >= Ann_A(M) = \cap_{i=1}^{t} Ann_A(M_i) \supset \cap_{i=1}^{t} < p_i^{e_i} >=< \mu >$.

Recordatorio: En un DIP, mcm corresponde con $\cap$.

Definición 2.27 (Descomposición primaria)
Cada M_i *se llama componente* p_i-*primaria de* M.

La descomposición primaria de M *es* $M = M_1 \dot{+} ... \dot{+} M_t$.

Ejercicio 2.28
Obtener la descomposición primaria usando $\dot{+}$ *de* $\mathbb{Z}_{8000}$.

Ejemplo 2.29
$T : V \to V, K-$*lineal* $\to V$ *es un* $K[X]-$*módulo.*
W *es un submodulo de* ${}_{K[X]}V$ *es un* $K-$*subespacio vectorial de* V *tal que* $T(W) \subseteq W$ *(*W *es* $T-$*invariante).*

Si $Ann_{K[X]}(V) \neq \{0\}$, *tomo* $\mu(x) \in K[X]$ *tal que* $Ann_{K[X]} =< \mu(X) >$ *(*$\mu(x)$ *polinomio mínimo de* T*).*

$$\mu(x) = p_1(x)^{e_1} ... p_t(x)^{e_t}, p_1, ..., p_t \text{ irreducibles en } K[X]$$

La descomposición primaria de V *es* $V = V_1 \dot{+} ... \dot{+} V_t$, *con* V_i $T-$*invariante y* $V_i = \{v \in V : p_i(x) \cdot v = 0\}$.

Caso particular: $dim_K V < \infty$ *y* $\mu(x) = (x - \alpha_1)...(x - \alpha_t), \alpha_1, ..., \alpha_t \in K, \alpha_i \neq \alpha_j$.

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

$$= \{v \in V : T(v) = \alpha_i v\} = \text{subespacio propio del valor propio } \alpha_i$$

$$\Rightarrow T \text{ es diagonalizable}$$

Si cogemos bases de $V_1, ..., V_t$ *y representamos el endomorfismo con respecto de esas bases, obtenemos una matriz diagonal. Así que si el polinomio mínimo del endomorfismo se factoriza completamente, entonces el endomorfismo es diagonalizable.*

El polinomio mínimo del endomorfismo identidad es $(x - 1)$.

Problemas:

- *¿Cómo se calcula el polinomio mínimo de un endomorfismo?*
- *Factorización del polinomio.*

Ejercicio 2.30
Sea V espacio vectorial real euclídeo (tiene producto escalar) de dim $< \infty$. $T : V \to V$ isometría (preserva distancias).

Demostrar que si W es un subespacio $T-$invariante de V, entonces su otrogonal $W^{\perp}$ es también $T-$invariante ($\Rightarrow V = W \dot{+} W^{\perp}$ como $\mathbb{R}[X]-$módulo).

Como consecuencia, usando el Teorema Fundamental del Álgebra, deducir que admite una base ortonormal con respecto de la cual la matriz de T es diagonal por bloques, con bloques de dimensión 1 ó 2. ¿Qué aspecto tienen esos bloques? (± 1 los bloques de 1, análogos a los de una rotación los de 2).

Nota: En espacios Hilbertianos, tomando T unitaria, tenemos que se puede diagonalizar completamente (utilizando complejos).

3. Homomorfismos de módulos

Definición 3.1 (Módulo cociente)
Sea ${}_AM$ módulo y $L \in \mathcal{L}({}_AM)$. Sé que tengo un grupo cociente $\frac{M}{L}$ aditivo, que deviene un $A-$módulo a través de la acción:

$$a \cdot (m + L) = am + L, a \in A, m \in M$$

Nota: Hay que probar que está bien definido.

Se llama módulo cociente ${}^M/_L$.

La proyección canónica: $\pi : M \to {}^M/_L$, dada por $\pi(m) = m + L$ es un homomorfismo de módulos en el siguiente sentido:

Definición 3.2 (Homomorfismos de módulos)
Una aplicación $f : M \to N$, con ${}_AM$,${}_A N$ módulos, es un homomorfismo de módulos si:

$$f(m + m') = f(m) + f(m') \quad f(am) = af(m) \quad \forall m, m' \in M, \forall a \in A$$

Proposición 3.3 (1^{er} Teorema de Isomorfía)
$f : M \to N$ homomorfismo de $A-$módulos. Entonces:

1. *$Kerf \in \mathcal{L}({}_AM), Imf \in \mathcal{L}({}_AN)$.*
2. *Para cada $L \in \mathcal{L}({}_AM)$ tal que $L \subseteq Kerf$, existe un único homomorfismo de módulos $\bar{f} : \frac{M}{L} \to N$ tal que $\bar{f}(m + L) = f(m), \forall m \in M$.*
3. *$\bar{f}$ inyectivo $\iff L = Kerf$, en cuyo caso, $\bar{f}$ da un isomorfismo de $A-$módulos $\frac{M}{Kerf} \cong Imf$.*

Definición: Isomorfismo de $A-$módulos $\equiv$ Homomorfismo de $A-$módulos biyectivo.

Ejemplo 3.4
${}_AM, m \in M$, defino $f : A \to M$ dada por $f(a) = am, \forall a \in A$.
f homomorfismo de $A-$módulos: $Imf = Am, ann_A(m) = Kerf = \{a \in A : am = 0\}$, que es un ideal a izquierda de A.

El Primer Teorema de Isomorfía nos dice:

$$\frac{A}{ann_A(m)} \cong Am$$

Ejemplo 3.5
$S = Map(\mathbb{N}, K)$, con K cuerpo. S es un $K-$espacio vectorial. Tomamos $T : S \to S$, con $T(s)(n) = S(n + 1), \forall n \in \mathbb{N}, \forall s \in S$. Se tiene que T es $K-$lineal $\Rightarrow S$ es un $K[X]-$módulo, y $(Xs)(n) = T(s)(n) = s(n + 1)$.

Sea $f \in K[X], f = f_0 + f_1 x + ... + f_m x^m$, *con* $f_i \in K, \forall i \in \{1, ..., m\}$. *Entonces:*

$$(fs)(n) = [(f_0 + f_1 x + ... + f_m x^m)s](n) =$$

$$= f_0 s(n) + f_1 s(n+1) + ... + f_m s(n+m) = \sum_{i=0}^{m} f_i s(n+i)$$

Supongamos que $ann_{K[X]}(s) \neq <0> \Rightarrow \exists f \in K[X]$ *tal que* $fs = 0$. *Podemos tomar* f *mónico, sin pérdida de generalidad, en cuyo caso,* $s(n+m) = -\sum_{i=0}^{m-1} f_i s(n+i), \forall n \in \mathbb{N}$. *En particular,* $s(m) = -\sum_{i=0}^{m-1} f_i s(i)$ *(estamos tomando* $0 \in \mathbb{N}$*). En este caso, a* s *se le llama sucesión linealmente recursiva.*

Caso particular: Tomamos $s(0) = s(1) = 1$, *y* $s(n+2) = s(n) = s(n+1)$ $(\Rightarrow m = 2, f_0 = f_1 = -1) \Rightarrow x^2 - x - 1 \in ann_{\mathbb{Q}[X]}(s) \rightarrow$ *esta es la sucesión de FIbonacci.*

Sabemos que $K[X]/_{ann_{K[X]}(s)} \cong K[X]s$ *(por el teorema de isomorfia). Por tanto,* $dim_K K[X]s \leq \infty \iff ann_{K[X]}(s) \neq <0> \iff s$ *es linealmente recursiva.*

De hecho, si $ann_{K[X]}(s) \neq <0> \Rightarrow dim_K K[X]s$ *es el grado del polinomio que genere a* $ann_{K[X]}(s)$.

Al generador de $ann_{K[X]}(s) = <p(x)>$ *se le denomina polinomio mínimo de la sucesión* s. *En consecuencia, el grado de* $p(x)$ *es el número de coeficientes necesarios para determinar recursivamente* s, *y por ello se llama complejidad lineal de* s. *Si* $ann_{K[X]}(s) = <0>$, *la complejidad de* s *es infinita.*

Supongamos que s, t *son sucesiones linealmente recursivas. Entonces* $K[X](s+t) \overset{\bigstar}{\subseteq} K[X]s \overset{\bigstar\bigstar}{K}[X]t$. *Como* $K[X]s$ *y* $K[X]t$ *tienen dimensión finita, entonces* $K[X](s+t)$ *tiene dimensión finita* $\Rightarrow s+t$ *es linealmente recursiva y su complejidad lineal es menor o igual que la suma de las complejidades lineales de* s *y de* t.

$\bigstar$ *En general,* $m, m' \in M \Rightarrow A(m+m') \subseteq Am + Am'$.
$\bigstar\bigstar$ *Suma de módulos.*

Llamamos ahora $S^l = \{s \in S \mid s$ *es linealmente recursiva*$\} \subseteq S$. *Entonces* S^l *es un* $K[X]-$*submódulo de* S *(basta ver que es invariante por la acción de* x.

Ejemplo 3.6
$T : C^\infty(\mathbb{R}) \rightarrow C^\infty(\mathbb{R}), T(\varphi) = \varphi', \forall \varphi \in C^\infty(\mathbb{R})$. *Como* T *es lineal* $\Rightarrow C^\infty(\mathbb{R})$ *es un* $\mathbb{R}[X]-$*módulo.*

Dada $\varphi \in C^\infty(\mathbb{R}), ann_{\mathbb{R}[X]}(\varphi) = \{f(x) \in \mathbb{R}[X] \mid f(x) \cdot \varphi = 0\} \Rightarrow$
$ann_{\mathbb{R}[X]}(\varphi) = \{f = \sum_{i=0}^{m} f_i \frac{d^i}{dt^i} \mid f \cdot \varphi = 0\}$.

Nota: Estamos viendo $f(x) \in \mathbb{R}[X]$ *como un operador diferencial.*

En consecuencia, $ann_{\mathbb{R}[X]}(\varphi) \neq < 0 > \iff$ φ satisface una ecuación no trivial diferencial lineal, homogénea y con coeficientes constantes. Por el teorema de isomorfía, tenemos $\frac{\mathbb{R}[X]}{ann_{\mathbb{R}[X]}(\varphi)} \cong R[X]\varphi$ y, siguiendo el análisis del ejemplo anterior, tenemos $dim_{\mathbb{R}}\mathbb{R}[X]\varphi < \infty \iff ann_{\mathbb{R}[X]}(\varphi) \neq < 0 > \iff$ φ satisface una ecuación diferencial del tipo anterior.

Llamamos a este tipo de funciones "linealmnete diferenciables". Análogamente al ejemplo anterior, puede obtenerse el polinomio máximo de φ.

Caso particular: $\varphi'' - \varphi' - \varphi = 0 \Rightarrow \varphi(t) = e^{\alpha t}$, con $\alpha = \frac{1+\sqrt{5}}{2} \rightarrow$ análogo a la sucesión de Fibonacci.

Definición 3.7 (Suma directa externa)
Sean ${}_AM_1, ..., {}_AM_t$. El producto cartesiano $M_1 \times ... \times M_t$ es un $A-$módulo con $(m_1, ..., m_t) + (m'_1, ..., m'_t) = (m_1 + m'_1, ..., m_t + m'_t)$ (grupo producto) y $a(m_1, ..., m_t) = (am_1, ..., am_t)$.

Dicho módulo se llama suma directa externa de $M_1, ..., M_t$. Si $M_1 = M_2 = ... = M_t$, se emplea la notación $M^t = M \times \overset{(t)}{\dots} \times M$.
En concreto, se puede formar el $A-$módulo A^t.

Ejercicio 3.8
Sea ${}_AM$, y $N_1 + ... + N_t \in \mathcal{L}({}_AM)$.
Demostrar que existe un homomorfismo sobreyectivo de $A-$módulos $f : N_1 \oplus ... \oplus N_t \rightarrow N_1 + ... + N_t$, tal que f es isomorfismo si, y sólo si la suma $N_1 + ... + N_t$ es directa.

Notación: $N_1 \oplus ... \oplus N_t \rightarrow N_1 + ... + N_t$ denota la suma directa externa de $A-$módulo.

Nota: Consideramos $A^n = A \oplus \overset{(n)}{\dots} \oplus A$, y para cada $i \in \{1, ..., n\}$ definimos $e_i = (0, ..., 0, \overset{(i)}{1}, 0, ..., 0)$. Entonces $\{e_i \mid i \in \{1, ..., n\}\}$ es un sistema de generadores de $a = (a_1, ..., a_n) = \sum_{i=1}^n a_i e_i$, y la expresión es única.

Proposición 3.9
Sea ${}_AM$ un módulo y $m_1, ..., m_n \in M$. Entones existe un único homomorfismo de módulos $f : A^n \rightarrow M$ tal que $f(e_i) = m_i, \forall i \in \{1, ..., n\}$. Como consecuencia, si M es finitamente generado con generadores $\{m_1, ..., m_n\}$, entonces $M \cong \frac{A^n}{L}$, donde L es cierto submódulo.

Demostración.
- Unicidad: Si existe una tal f, entonces para cada $a \in A^n$, se tiene $f(a) = f(\sum_i a_i e_i) = \sum_i^n a_i f(e_i) = \sum_{i=1}^n a_i m_i$.
- Existencia: Si definimos $f(a) = \sum_{i=1}^n a_i m_i$, lo cual podemos hacer por ser la expresión $a = \sum_{i=1}^n a_i e_i$ única, entonces f verifica el enunciado.
- Consecuencia: Si $M = Am_1 + ... + Am_n \Rightarrow f$ sobreyectiva $\Rightarrow$ tomando $L = Kerf$, el teorema nos garantiza que $M \cong \frac{A^n}{L}$.

□

Definición 3.10 (SEC)
Consideremos la sucesión:

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

Esta sucesión es exacta en $L \iff Ker\alpha = \{0\} \iff \alpha$ *inyectivo en* $M \iff Ker\beta = Im\alpha$*; y en* $N \iff N = Im\beta \iff \beta$ *sobreyectiva.*

Se dice que esta sucesión es una sucesión exacta corta (SEC, o SES en inglés) si es exacta en L, M *y* N*.*

Ejemplo 3.11
Si $f : M \to N$ *es un homomorfismo de módulos, la sucesión* $\{0\} \to Kerf \xrightarrow{f} Imf \to \{0\}$ *es una SEC.*

Proposición 3.12
Sea $0 \to L \xrightarrow{\psi} M \xrightarrow{\varphi} N \to 0$ *una SEC de* $A-$*módulo. Entonces:*

1. *Si* M *es finamente generado (fg)* $\Rightarrow N$ *es fg.*
2. *Si* L *y* N *son fg* $\Rightarrow M$ *es fg.*

Demostración.
1. Sea $\{m_1, ..., m_n\}$ un conjunto de generadores de M. Es claro que $\{\varphi(m_1), ..., \varphi(m_n)\}$ genera N (por ser φ sobreyectiva).
2. Sea $\{n_1, ..., n_s\}$ un conjunto de generadores de N. Tomemos $\{m_1, ..., m_s\} \subseteq M$ tales que $\varphi(m_i) = n_i, \forall i \in \{1, ..., s\}$.
   Sea ahora $\{l_1, ..., l_t\}$ un conjunto de generadores de L. Sea $m \in M$. Existe entonces una manera de expresar $\varphi(m) = \sum_{i=1} sr_i n_i$, al ser $\varphi(m) \in N$. Entonces $\varphi(m) = \sum_{i=1}^{s} r_i \varphi(m_i) = \varphi(\sum_{i=1}^{s} r_i m_i) \Rightarrow \varphi(m - \sum_{i=1}^{s} r_i m_i) = 0 \Rightarrow m - \sum_{i=1}^{s} r_i m_i \in Ker\varphi = Im\psi$.
   Existen entonces $b_1, ..., b_t \in A$ tales que $m - \sum_{i=1}^{t} r - im_i = \sum_{j=1}^{t} b_j \psi(l_j) \Rightarrow m = \sum_{i=1}^{s} r_i m_i + \sum_{j=1}^{t} b_j \psi(l_j) \Rightarrow$
   $\{m_1, ..., m_s, \psi(l_1), ..., \psi(l_t)\}$ es un sistema de generadores de M.

□

Ejemplo 3.13
Sea I *conjunto infinito y* K *cuerpo. Consideramos* $K^I = \{(\alpha_i)_{i \in I} \mid \alpha_i \in K, \forall i\}$*, que es un anillo.*

Consideramos ahora $K^{(I)} = \{(\alpha_i)_{i \in I} \mid \alpha_i \in K$ *y* $\alpha_i = 0$ *salvo para un número finito de índices*$\}$*.*
Entonces $K^{(I)}$ *es un ideal de* K^I *pero no es finitamente generado como ideal a izquierda de* K^I*.*

Nota: $\nRightarrow$ Submódulos de módulos finitamente generados no pueden ser finitamente generados.

Nota: K^I si es fintamente generado como módulo (pues es cíclico).

Nota: En la SEC $\{0\} \to L \to M \to N \to \{0\}$, se tiene

$$M \text{ fg } \nRightarrow L \text{fg}$$

4. Módulos Noetherianos y Artinianos

(Emmy Noether)

Definición 4.1 (Noetheriano)
Un módulo M se dice noetheriano si todo submódulo de M es finitamente generado.

En particular, debe ser M fg.

Ejemplo: K^I no es noetheriano.

Proposición 4.2
Para un módulo M, son equivalentes:

1. *M es noetheriano (todo submodulo es finitamente generado).*
2. *Cada cadena $L_1 \subseteq L_2 \subseteq ... \subseteq L_n \subseteq ...$ de submódulos de M se estabiliza, esto es, $\exists m \geq 1$ tal que $L_m = L_n, \forall n \geq m$ (Condición de cadena ascendente).*
3. *Cada subconjunto no vacío de $\mathcal{L}(M)$ tiene un elemento maximal respecto del orden dado por la inclusión.*

Estamos viendo $\mathcal{L}(M)$ ordenado por inclusión.

Demostración. 1. $\Rightarrow$ 2.: $L := \cup_{n\geq 1} L_n \in \mathcal{L}(M)$, luego L es finitamente generado. Si tomo un conjunto finito F de generadores L, como está en L y es finito, tiene que $\exists m \geq 1$ tal que $F \subseteq L_m \Rightarrow L \subseteq L_m \subseteq L \Rightarrow L = L_m \Rightarrow L_m = L_n, \forall n \geq m$.

2. $\Rightarrow$ 3.: Sea $\Gamma \subseteq \mathcal{L}(M)$ no vacío. Si Γ no tiene elemento maximal, y tomo $L_1 \in \Gamma$, existirá $L_2 \in \Gamma$ tal que $L_1 \subset L_2$ (inclusión estricta). Reiterando el proceso, obtengo una cadena infinita:

$$L_1 \subset L_2 \subset ... \subset L_n \subset ... \text{ (inclusiones estrictas)}$$

Hemos demostrado que (No 3. $\Rightarrow$ No 2.) $\Rightarrow$ (2. $\Rightarrow$ 3.).

3. $\Rightarrow$ 1.: Sea $N \in \mathcal{L}(M)$. Tomo Γ el conjunto de todos los submodulos finitamente generados de N, $\{0\} \in \Gamma \Rightarrow \Gamma \neq \emptyset$. Como to subconjunto no vacío de $\mathcal{L}(M)$ tiene un elemento maximal, $\exists L \in \Gamma, L$ maximal. Afirmo que $L = N$. En caso contrario, tomo $x \in N$ tal que $x \notin L$. Resulta que $L + Ax$ es un submódulo de N, y además es finitamente generado, ya que L es finitamente generado al estar en Γ. Por lo que $L + Ax \in \Gamma$ y $L \neq L + Ax \Rightarrow L$ no es maximal $\Rightarrow$ Contradicción $\Rightarrow L = N$. □

Proposición 4.3
Sea $0 \to L \xrightarrow{\psi} M \xrightarrow{\varphi} N \to 0$ un s.e.c. de módulos.

$$M \text{ es noetheriano } \iff L \text{ y } N \text{ son noetherianos.}$$

Demostración. $\circledR$ $L \cong Im\psi \underset{\text{submódulo}}{\leq} M \Rightarrow$ L es noetheriano (ya que L es noetheriano).

Tomo $N_1 \subseteq N_2 \subseteq ... \subseteq N_n \subseteq ...$ cadena en $\mathcal{L}(N)$. Tengo $\varphi^{-1}(N_1) \subseteq \varphi^{-1}(N_2) \subseteq ... \subseteq \varphi^{-1}(N_n) \subseteq ...$ cadena en $\mathcal{L}(M)$ (ya que la imagen inversa de un submódulo por un homomorfismo es un submódulo) $\Rightarrow \exists m \geq 1$ tal que $\varphi^{-1}(N_n) = \varphi^{-1}(N_m), \forall n \geq m \Rightarrow N_n = \varphi(\varphi^{-1}(N_n)) = \varphi(\varphi^{-1}(N_m)) = N_m, \forall n \geq m \Rightarrow N$ es noetheriano.

$\circledL$ Tomo una cadena en $\mathcal{L}(M)$:

$$M_1 \subseteq M_2 \subseteq ... \subseteq M_n \subseteq ... \Rightarrow \varphi(M_1) \subseteq \varphi(M_2) \subseteq ... \subseteq \varphi(M_n) \subseteq ...$$

en $\mathcal{L}(N)$.

$$M_1 \cap Im\psi \subseteq M_2 \cap Im\psi \subseteq ... \subseteq M_n \cap Im\psi \subseteq ...$$

en $\mathcal{L}(Im\psi)$.

Como $Im\psi \cong L$ y N son noetherianos, $\exists m \geq 1$ tal que $\varphi(M_n) = \varphi(M_m) \Rightarrow Im\psi \cap M_n = Im\psi \cap M_m$ para $n \geq m$.
Tomo $x \in M_n \Rightarrow \varphi(x) \in \varphi(M_n) = \varphi(M_m)$ tomo $y \in M_m$ tal que $\varphi(x) = \varphi(y) \Rightarrow x - y \in Ker\varphi = Im\psi \Rightarrow x - y \in M_n \cap Im\psi = M_m \cap Im\psi \Rightarrow x - y \in M_m \Rightarrow x \in M_m \Rightarrow M_n \subseteq M_m \subseteq M_n \Rightarrow M_n = M_m \Rightarrow M$ es noetheriano. □

Corolario 4.4
Dados dos módulos M_1, M_2, entonces:

$$M_1 \oplus M_2 \text{ noetheriano} \iff M_1, M_2 \text{ noetherianos}$$

Demostración. Tengo la SEC:

$$\begin{array}{ccccccc} 0 \to & M_1 \to & M_1 \oplus M_2 \to & M_2 \to & 0 \\ & m_1 \mapsto & (m_1, 0) & & \\ & & (m_1, m_2) \mapsto & m_2 & \end{array}$$

□

Teorema 4.5
Sea A un anillo. Cada $A-$módulo finitamente generado es noetheriano si, y sólo si, ${}_AA$ es noetheriano.

Demostración. $\circledR$ Obvio, ya que si todos los finitamente generados son noetherianos, ${}_AA$ que es finitamente generado es noetheriano.

$\circledL$ ${}_AM$ finitamente generado $\Rightarrow \exists$ un homomorfismo sobreyectivo de módulos: $0 \to Ker \to A^n \to M \to 0$ para cierto n (el número de generadores). Por la proposición anterior, si A^n es noetheriano, también lo es M.

Usando inductivamente el corolario, tengo que A^n es noetheriano. Para A es hipótesis, y para $A^n = A^{n-1} \oplus A$, por lo que, por la proposición, M es noetheriano. □

Definición 4.6
A se dice noetheriano a izquierda si ${}_AA$ es noetheriano.

Corolario 4.7
Si ${}_AA$ es noetheriano, son equivalentes para cualquier sucesión exacta corta (SEC):

$$0 \to L \to M \to N \to 0$$

1. *M finitamente generado.*
2. *L y N finitamente generado.*

Corolario 4.8
Todo DIP es noetheriano.

Lema 4.9
Para un módulo M, son equivalentes:

1. *Cada cadena $L_1 \supseteq L_2 \supseteq \cdots \supseteq L_n \supseteq \ldots$ de submódulos de M se estabiliza, esto es, $\exists m \geq 1$ tal que $L_n = L_m, \forall n \geq m$.*
2. *Cada subconjunto no vacío de $\mathcal{L}(M)$ tiene un elemento minimal.*

Demostración: Ejercicio.

Definición 4.10 (Módulos artinianos)
Un módulo M se dice artiniano si satisface (1).

Ejemplo 4.11
Sea A un dominio de integridad conmutativo. Si ${}_AA$ es artiniano $\Rightarrow$ A es un cuerpo.

Demostración: Ejercicio.

En particular, $\mathbb{Z}$ no es artiniano. $\mathbb{Z}$ si era noetheriano (por el corolario anterior). Por lo que artiniano no implica noetheriano, ni viceversa.

Ejercicio 4.12
K cuerpo de característica 0. Tomo $K[X]$ anillo de polinomios. Veo $K[X]$ como $K-$e.v. Tengo la aplicación lineal $T : K[X] \to K[X], T(f) = f'$. Eso me da una estructura de $K[X]-$módulo sobre $K[X]$ que no es la de módulo regular.

Demostrar que ese módulo es artiniano y no finitamente generado.

Consecuencia: Este no es el $K[X]-$módulo regular.

Proposición 4.13
Sea $0 \to L \to M \to N \to 0$ *una sec. Entonces* M *es artiniano* $\iff$ M *y* N *artinianos.*

Demostración. Se obtiene siguiendo los pasos de la del caso noetheriano. $\square$

Ejercicio 4.14
Sea p *un número primo.*

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

Comprobar que C_{p^∞} *es un subgrupo de* $U(1) = \{z \in \mathbb{C} \mid |z| = 1\}$ *(circunferencia unidad).*

Veo el grupo abeliano C_{p^∞} *como un* $\mathbb{Z}-$*módulo.*
Demostrar que C_{p^∞} *es artiniano, pero no finitamente generado.*

5. Módulos de Longitud Finita

Definición 5.1 (Serie de composición)
Sea M un módulo. Una seria de composición de M es una cadena de submódulos:

$$M = M_n \supset M_{n-1} \supset ... \supset M_1 \supset M_0 = \{0\}$$

(inclusiones estrictas) tal que si $M_i \supseteq N \supseteq M_{i-1}$, para N submódulo $\Rightarrow$ $N = M_i$ ó $N = M_{i-1}, \forall i \in \{1, ..., n\}$.
Es decir, entre cada dos submódulos, no cabe ninguno más.

n es la longitud de la serie.

Ejemplo 5.2
Serie de composición de $\mathbb{Z}_{12}$ (como $\mathbb{Z}-$módulo).

$$M = \mathbb{Z}_{12} = \{0, 1, ..., 11\}$$

$$\mathbb{Z}_{12} \supset \underset{\text{Orden 6}}{< 2 >} \supset \underset{\text{Orden 3}}{< 4 >} \supset < 0 > = M_3 \supset M_2 \supset M_1 \supset M_0$$

Definición 5.3 (Módulo simple)
Un módulo se dice simple si $M \supset \{0\}$ es una serie de composición.

En la definición de Serie de composición, si $M_i \supseteq N \supseteq M_{i-1}$, para N submódulo $\Rightarrow$ $N = M_i$ ó $N = M_{i-1}, \forall i \in \{1, ..., n\} \Rightarrow \frac{Mi}{M_{i-1}}$ es simple $\forall i \in \{1, ..., n\}$.

Para un módulo M, todas sus series de composición tienen los mismos factores $\frac{M_i}{M_{i-1}}$, pero pueden cambiar de orden, obteniendo series distintas.

Proposición 5.4
Un módulo no nulo admite una serie de composición si, y sólo si, es noetheriano y artiniano.

Demostración. $\Leftrightarrow$ Sea $M = M_n \supset M_{n-1} \supset ... \supset M_1 \supset M_0 = \{0\}$ s.c. (serie de composición). Razonamos por inducción sobre n.

- $n = 1 \Rightarrow M$ simple $\Rightarrow M$ noetheriano y artiniano.
- $n > 1 \Rightarrow M_{n-1}$ admite una serie de composición de longitud $n - 1$, $M_{n-1} \supset ... \supset M_1 \supset M_0 = \{0\}$, por lo que M_{n-1} es noetheriano y artiniano (hipótesis de inducción).

$$0 \to \underset{\text{noetheriano y artiniano}}{M_{n-1}} \to M_n \to \underset{\text{noetheriano y artiniano}}{\frac{M_n}{M_{n-1}}} \to 0 \text{ sec}$$

Por lo que M_n es noetheriano y artiniano.

$\Leftarrow\!\!\!\!\!\!\bigcirc$ M artiniano $\Rightarrow$ contiene al menos un submódulo simple, M_1. Hay $M_2 \supset M_1$ tal que $\frac{M_2}{M_1}$ es simple.
Reiteramos el proceso, y tenemos $\{0\} \subset M_1 \subset M_2 \subset ....$ Como M es noetheriano, esta cadena termina cuando lleguemos a M, es decir, tenemos:

$$\{0\} \subset M_1 \subset M_2 \subset ... \subset M_{n-1} \subset M_n = M$$

□

Corolario 5.5
Dada SER $0 \to L \to M \to N \to 0, L$ *y* N *admiten una serie de composición* $\iff$ M *admite serie de composición.*

Corolario 5.6
Dos módulos M_1, M_2 *admiten serie de composición* $\iff$ $M_1 \oplus M_2$ *admite serie de composición.*

Teorema 5.7 (Jordan-Hölder)
Supongamos que M *módulo admite series de composición:*

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

$$\{0\} = N_0 \subset N_1 \subset ... \subset N_k = M$$

Entonces $n = k$ *y además existe una permutación* $\sigma : \{1, ..., n\} \to \{1, ..., n\}$ *tal que* $\frac{M_i}{M_{i-1}} \cong \frac{N_{\sigma(i)}}{N_{\sigma(i)-1}}, i \in \{1, ..., n\}$.

Demostración. Por inducción sobre n.

- $n = 1 \Rightarrow M$ simple $\Rightarrow m = 1$. Sólo hay una permutación, y por tanto $\frac{M}{\{0\}} \cong \frac{M}{\{0\}}$.
- Si $n > 1 \Rightarrow M$ no es simple $\Rightarrow m > 1$. Distinguimos dos casos:

Caso a: Si $N_{m-1} = M_{n-1}$:

$$M_n = N_m \supset M_{n-1} = N_{m-1} \supset \begin{cases} M_{n-2} \supset ... \supset M_1 \\ N_{m-2} \supset ... \supset N_1 \end{cases} \supset \{0\}$$

Por inducción $m-1 = n-1$ y $\exists \sigma : \{1, ..., n-1\} \to \{1, ..., m-1\}$ tal que $\frac{M_i}{M_{i-1}} \cong \frac{N_i}{N_{i-1}}, i \in \{1, ..., n-1\} \Rightarrow n = m$ y amplio $\sigma(m) = n$.

Caso b: Si $N_{m-1} \neq M_{n-1}$:

$$M_n = N_m \supset \begin{cases} M_{n-1} \supset ... \subset M_1 \\ N_{m-1} \supset ... \supset N_1 \end{cases} \supset \{0\}$$

Entonces $M_{n-1}+N_{m-1} = M$, ya que $M_{n-1} \subset M_{n-1}+N_{m-1} \subseteq M$.

Tomo $N_{m-1} \cap M_{n-1} \subset M$, por lo que admite una serie de composición.

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

Usamos el Teorema de Isomorfía:

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

Como $\frac{M}{N_{m-1}}$ es simple, entonces $\frac{M_{n-1}}{N_{m-1} \cap M_{n-1}}$ es simple.

Podemos construir otra serie de composición:

$$M_n = N_m \supset \begin{matrix} M_{n-1} \\ N_{m-1} \end{matrix} \quad \supset L_k = M_{n-1} \cap N_{m-1} \supset L_{k-1} \supset \cdots \supset L_1 \supset \{0\}$$

Por inducción, $n-1 = k+1$ y $\exists \tau : \{1, ..., n-1\} \to \{1, ..., n-1\}$ tal que $\frac{L_i}{L_{i-1}} \cong \frac{M_{\tau(i)}}{M_{\tau(i)-1}}, i \in \{1, \ldots, n-2\}$, y $\frac{M_{n-1}}{L_{n-2}} \cong \frac{M_{\tau(n-1)}}{M_{\tau(n-1)-1}}$.

Volvemos a tener:

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

Como $\frac{M}{N_{m-1}}$ es simple, $\frac{N_{m-1}}{N_{m-1} \cap M_{n-1}}$ es simple.

Volvemos a aplicar inducción, y tenemos $m-1 = n-1$ y $\exists \rho : \{1, \ldots, n-1\} \to \{1, \ldots, n-1\}$ tal que $\frac{L_i}{L_{i-1}} \cong \frac{N_{\rho(i)}}{N_{\rho(i)-1}}$,
$i \in \{1, \ldots, n-2\}$.

$$\frac{N_{n-1}}{L_{n-2}} \cong \frac{N_{\rho(n-1)}}{N_{\rho(n-1)-1}}$$

Defino $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$ como:

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

y $\frac{M_i}{M_{i-1}} \cong \frac{N_{\sigma(i)}}{N_{\sigma(i)-1}}$.

□

Definición 5.8
Un módulo M se dice de longitud finita si admite una serie de composición o si es $\{0\}$.
La longitud de M, notación $l(M)$ es la de cualquiera de sus series de composición si $M \neq \{0\}$, ó $l(\{0\}) = 0$.

Ejercicio 5.9
Sea M de longitud finta. Demostrar:

1. *Si $0 \to L \to M \to N \to 0$ sucesión exacta corta, entonces*

$$l(M) = l(N) + l(L)$$

2. *Si $U, V \in \mathcal{L}(M)$, entonces*

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

Ejemplo 5.10
- $l(\mathbb{Z}_{12}) = 3$.
- $l(\mathbb{Z}_{13}) = 1$.
- $l(\mathbb{Z}_n) =$ *suma de los exponentes de su descomposición en primos.*

¿Cuántas series de composición distintas tienen?

- $\mathbb{Z}_{12} \to 3$.
- $\mathbb{Z}_4 \to 1$.

Si $n = p_1^{e_1} \dots p_t^{e_t}$:

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{e_1}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{e_t}}$$

Definición 5.11
Sea ${}_AM$ un módulo, y $\mathcal{L}(M)$ el conjunto de todos los submódulos de M. Dado $\Gamma_A \subseteq \mathcal{L}(M), \cap_{N \in \Gamma} N \in \mathcal{L}(M)$.

Nota: Puede ocurrir que $\cap_{N \in \Gamma} N \notin \Gamma$.

Ejemplo: $\cap_{n \in \mathbb{Z}, n \neq 0} n\mathbb{Z} = \{0\}$.

Definición 5.12 (Zócalo)
El zócalo de M es el menor submódulo de M que contiene a todos los submódulos simples de M.
Si M no contiene ningún simple, definimos su zócalo como $\{0\}$.

En ambos casos, usaremos la notación $Soc(M)$.

Ejemplo 5.13
Si V es un $K-$espacio vectorial, $Soc(V) = V$ (los simples de un e.v. son los de dimensión 1, y si tiene que contener a todas las rectas, tiene que contener a todo el espacio).

Ejemplo 5.14
$Soc(\mathbb{Z}) = \{0\}$ ($\mathbb{Z}$ no tiene submódulos simples, los submódulos de $\mathbb{Z}$ son de la forma $n\mathbb{Z}$, y $mn\mathbb{Z}$ es un submódulo de este).

Ejemplo 5.15
Si A es un DI que no es un cuerpo, $Soc(A) = \{0\}$ (los submódulos de A distintos de $\{0\}$ son ideales que contienen un elemento de 0, por lo que también contienen al cuadrado de este elemento [...]).

Ejercicio: Demostrar este último ejemplo.

Proposición 5.16
Sea M de longitud finita ($\Rightarrow$ noetheriano y artiniano). Existen submódulos simples $S_1, \ldots, S_n$ de M tal que:

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

Además, si existe otra descomposición $Soc(M) = T_1 \dot{+} \cdots \dot{+} T_m$, con $T_i \in \mathcal{L}(M)$, entonces $n = m$ y, tras reordenación, $S_i \cong T_i, i \in \{1, ..., n\}$.

Demostración. Sea Γ el conjunto de todos los submódulos de M de la forma $S_1 \dot{+} \cdots \dot{+} S_t$, con $S_i \in \mathcal{L}(M)$ simple.
Si $M \neq \{0\}$, entonces Γ es no vacío, ya que M contiene algún simple, y como es noetheriano, contiene un elemento $S_1 \dot{+} \cdots \dot{+} S_n \in \Gamma$ maximal.
$S_1 \dot{+} \cdots \dot{+} S_n \subseteq Soc(M)$, ya que todos ellos son simples y, al ser $Soc(M)$ un submódulo, la suma directa también pertenece.

Sea $S \in \mathcal{L}(M)$ simple.

$$S \cap (S_1 \dot{+} \cdots \dot{+} S_n) = \begin{cases} \{0\} \to ① \\ S \to ② \end{cases}$$

① $\Rightarrow S \dot{+} S_1 \dot{+} \cdots \dot{+} S_n \in \Gamma \Rightarrow S_1 \dot{+} \cdots \dot{+} S_n$ no es maximal.
② $\Rightarrow S \subseteq S_1 \dot{+} \cdots \dot{+} S_n$, y teníamos $S_1 \dot{+} \cdots \dot{+} S_n \subseteq Soc(M) \Rightarrow S_1 \dot{+} \cdots \dot{+} S_n = Soc(M)$.

Para la segunda parte, tenemos:

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

es una serie de composición, ya que $\frac{S_1 \dot{+} \cdots \dot{+} S_n}{S_1 \dot{+} \cdots \dot{+} S_{i-1}} \cong S_i$. Hay otra serie de composición para T_i. Aplicamos Jordan-Hölder. □

Definición 5.17
Suponemos M de longitud finita. Decimos que M es semi-simple si:

$$M = \{0\} \text{ ó } Soc(M) = M \text{ si } M \neq \{0\}$$

Ejercicio 5.18
A DIP, I ideal de A (no cuerpo). Demostrar que:

$$\frac{A}{I} \text{ es de longitud finita } \iff I \neq <0>$$

¿Puedo deducir quién es la longitud de $\frac{A}{I}$ de un generador de I?

6. Estructura de módulos de longitud finita sobre un DIP

Durante todo el tema, A es un DIP (Dominio de Integrales Principales).

Lema 6.1
Un módulo ${}_AM$ es de longitud finita $\iff$ ${}_AM$ es finitamente generado y acotado ($Ann({}_AM) \neq 0$).

Demostración. Suponemos $M \neq \{0\}$.

$\circledR$ ${}_AM$ longitud finita $\Rightarrow_A$ M finitamente generado (Longitud finita $\Rightarrow$ Noetheriano + Artiniano, Noetheriano $\Rightarrow$ finitamente generado) $\Rightarrow M = Am_1 + \cdots + Am_n, m_i \in M$.

$$< \mu >= Ann_A(M) = \bigcap_{i=1}^{n} ann_A(m_i)^{\bigstar} \text{ (A conmutativo).}$$

$$ann_A(m_i) =< f_i >, f_i \in A$$

$$\bigstar = \bigcap_{i=1}^{n} < f_i > \Rightarrow \mu = mcm(f_1, \ldots, f_n)$$

Queremos ver que $f_i \neq 0, \forall i \in \{0, \ldots, n\}$.

$$M \supseteq Am_i \cong \frac{A}{< f_i >} \Rightarrow l(Am_i) < \infty \overset{A \text{ no cuerpo}}{\Rightarrow} < f_i > \neq 0 \Rightarrow$$

$$\Rightarrow \mu \neq 0 \Rightarrow M \text{ acotado.}$$

$\circledL$ Como M es fintamente generado $\Rightarrow M = Am_1 + \cdots + Am_n$. Veo que cada Am_i es de longitud finita usando el mismo razonamiento que en el apartado anterior:

$$0 \neq < \mu >= \bigcap_{i=1}^{n} < f_i > \Rightarrow < f_i > \neq 0$$

$\Rightarrow Am_i \cong \frac{A}{<f_i>}$ es de longitud finita.

$$Am_1 \oplus \cdots \oplus Am_n \to Am_1 + \cdots + Am_n \text{ epimorfismo } \Rightarrow$$

$$\Rightarrow Am_1 + \ldots Am_n \text{ tiene long finita}$$

□

Nota: $l({}_AM) < \infty \Rightarrow < \mu >= Ann_A(M) \neq < 0 > \Rightarrow M = M_1 \dotplus \cdots \dotplus M_t$ descomposición primaria, $M_i =$ componente p_i-primaria que viene de $\mu = p_1^{e_1} \ldots p_t^{e_t}$ descomposición completa ($M_i = \{m \in M \mid p_i^{e_i} m = 0\}$).
M_i finitamente generado. ¿Se puede desomponer como $\dotplus$ de submodulos indescomponibles?

Corolario 6.2 (Resumen)
A DIP, ${}_AM$ *acotado,* $< \mu >= Ann_A(M), \mu \neq 0$.
$M \neq \{0\}, \mu = p_1^{e_1} \dots p_t^{e_t}, p_i \in A$ *irreducibles.*

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

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

$$q_i = \frac{\mu}{p_i^{e_i}} \qquad \sum_{i=1}^{t} a_i q_i = 1$$

Definición 6.3
${}_AM$ *p−primario si* $Ann_A(M) =< p^e >$ ($p \in A$ *irreducible).*

Queremos ver como es la estructura de módulos primarios para módulos de longitud finita.

Observación: Vamos a suponer que ${}_AM$ es $p-$primario con $l({}_AM < \infty$. Entonces $Ann_A(M) =< p^t >$ (una potencia de p). Si tomamos $m \in M, m \neq 0$, entonces $ann_A(M)$ está generado por un elemento de A, pero también sabemos que $ann_A(m) \supseteq Ann_A(M) =< p^t >$. Entonces $ann_A(m) =< p^r >$, con $r \leq t$.

Nota: $< f > \subseteq < g > \iff g \mid f$.

$M = Am_1 + \cdots + Am_n \Rightarrow < p^t >= ann_A(m_1) \cap \cdots \cap ann_A(m_n) =< p^{r_1} > \cap \cdots \cap < p^{r_n} >, r_i \leq t \Rightarrow < p^t >= ann_A(m_i)$ para algún i.

Corolario 6.4
Si un módulo es p−primario y tiene longitud finita, entonces $\exists x \in M$ *tal que* $Ann_A(M) = ann_A(x)$.

Lema 6.5
${}_AM$ *módulo con* $l(M) < \infty$, *M p−primario. Para* $m \in M, m \neq 0$*:*

$$Am \text{ simple} \iff ann_A(m) =< p >$$

Como consecuencia:

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

Demostración. $\circledcirc$ $Am \cong \frac{A}{ann_A(m)}$

Si Am es simple $\Rightarrow ann_A(m)$ es ideal maximal, y $ann_A(m) \supseteq Ann_A(M) = =< p^t > \Rightarrow ann_A(m) =< p >$.

Recordatorio: Los ideales maximales de un DIP están generados por los elementos. irreducibles del DIP.

$\Leftarrow$ Si $ann_A(m) =< p >\Rightarrow Am \cong \frac{A}{<p>}$ simple.

Por último, nos queda ver la consecuencia. Para ello, tomamos $Soc(M) = S_1 \dotplus \cdots \dotplus S_n$, con S_i simple, y $m \in Soc(M)$. Entonces:

$$ann_A(M) \supseteq Ann_A(S_1 \dotplus \cdots \dotplus S_n) = Ann_A(S_1) \cap \cdots \cap Ann_A(S_n)$$

y como S_i es simple, tenemos $Ann_A(S_i) = ann_A(s_i)$, con $s_i \in S_i$. Como S_i es simple, $S_i = AS_i \Rightarrow AS_i \cong \frac{A}{ann_A(S_i)}$, y como AS_i es simple, entonces $ann_A(S_i)$ es maximal, y por tanto $ann_A(S_i) =< p >$ y, por tanto:

$$ann_A(m) \supseteq < p > \Rightarrow p \cdot m = 0$$

Tomo ahora $m \in M, m \neq 0$ tal que $p \cdot m = 0$. Esto significa que $< p > \subseteq ann_A(m) \Rightarrow < p > \overset{\bigstar}{=} ann_A(m) \Rightarrow Am \cong \frac{A}{ann_A(m)} = \frac{A}{<p>} \Rightarrow Am$ simple $\Rightarrow Am \subseteq Soc(M) \Rightarrow m \in Soc(M)$.

$\bigstar p$ irreducible y $ann_A(m)$ es ideal y no es el total $\Rightarrow < p >= ann_A(m)$. $\square$

Proposición 6.6
Sea M módulo $p-$primario con $l(M) < \infty$. Tomamos $x \in M$ tal que $Ann_A(M) = ann_A(x)$.
Entonces el submódulo cíclico Ax es un sumando directo (interno) de M. Es decir, $M = Ax + N$ (N es otro elemento).

Demostración. Por inducción sobre $l(M)$.

- Si $l(M) = 1 \Rightarrow M$ es simple $\Rightarrow M = Ax$.
- Si $l(M) > 1$ y $Ax = M$, no hay nada que demostrar. Supongo que $Ax \neq M$.
  Vamos a demostrar que $\exists y \in M$ tal que $y \notin Ax$ y $ann_A(y) =< p >$.

  $\frac{M}{Ax}$ es un módulo finitamente generado, $l(\frac{M}{Ax}) < \infty$. Entonces contiene algún simple $S \subseteq \frac{M}{Ax}$. Tomo $s \in S$ tal que $S = As$.

  $$< p^t >= Ann_A(M) \subseteq Ann_A(\frac{M}{Ax}) \subseteq Ann_A(S) = ann_A(s)$$

  $$\Rightarrow ann_A(s) =< p >$$

  Tomo $z \in M$ tal que $s = z + Ax \Rightarrow pz \in Ax \Rightarrow pz = ax$ para cierto $a \in A$. Afirmo que $p \mid a$. De lo contrario, por Bezout tenemos $1 = ua + vp$ para ciertos $u, v \in A$. Así, $x = uax + vpx = upz + vpx = p(uz + vx)$. Tenemos $uz + vx \in M$, y M es un módulo primario, por lo que $ann_A(uz + vx) =< p^{t'} >$, para algún $t' \leq t$. Deduzco que $p^{t'-1}x = 0$, ya que $x = p(uz + vx)$. Por tanto, $p^{t-1}x = 0$, pero

$ann_A(x) =< p^t >$. Acabamos de encontrar un exponente más pequeño que anula a x (contradicción). Por tanto, $p \mid a$.

Otra forma de ver que $p \mid a$ es: $p^{t-1}ax = p^t z = 0 \Rightarrow p^{t-1}a \in ann_A(x) =< p^t > \Rightarrow a = pa'$.
Así tengo $pz = pa'x \Rightarrow p(z - a'x) = 0$. Llamo $y = z - a'x \neq 0$ y $py = 0 \Rightarrow ann_A(y) =< p >$.

Ay es simple, e $y \notin Ax \Rightarrow Ay \cap Ax = \{0\}$. Entonces $Ax \cong \frac{Ax}{Ay \cap Ax} \cong \frac{Ax+Ay}{Ay} = A(x + Ay) \subseteq \frac{M}{Ay}$.

$$< p^t >= ann_A(x) = Ann_A(A(x + Ay)) \supseteq Ann_A(\frac{M}{Ay}) \supseteq Ann_A(M) =< p^t >$$

$\frac{M}{Ay}$ y $x + Ay$ satisfacen $Ann_A(\frac{M}{Ay}) =< p^t >= ann_A(x + Ay)$. Entonces $l(\frac{M}{Ay}) < l(M) \Rightarrow$ Inducción.

$$\frac{M}{Ay} = \frac{Ax + Ay}{Ay} \stackrel{\cdot}{+}_{\star} \frac{N}{Ay} = \frac{Ax + Ay + N}{Ay}$$

para cierto $N \in \mathcal{L}(M)$ tal que $N \supseteq Ay$. Esto sólo es posible si $M = Ax + Ay + N = Ax + N$.

Sólo nos queda ver que es suma directa, es decir, que $Ax \cap N = \{0\}$. Para ello, consideramos $Ax \cap N \subseteq (Ax + Ay) \cap N = Ay$ (por $\star$). Entonces $Ax \cap N = Ax \cap N \cap Ay = Ax \cap Ay = \{0\}$.

□

Teorema 6.7
$M \neq \{0\}$ $p-$primario de longitud finita. Entonces existen $x_1, \ldots, x_n \in M$ no nulos tales que:

$$M = Ax_1 \stackrel{\cdot}{+} \cdots \stackrel{\cdot}{+} Ax_n$$

y $Ann_A(M) = ann_A(x_1) \subseteq ann_A(x_2) \subseteq \cdots \subseteq ann_A(x_n)$.

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

$$M = Ay_1 \stackrel{\cdot}{+} \cdots \stackrel{\cdot}{+} Ay_m$$

y $Ann_A(M) = ann_A(y_1) \subseteq ann_A(y_2) \subseteq \cdots \subseteq ann_A(y_m)$, entonces $n = m$ y $ann_A(y_i) = ann_A(x_i)$.

Demostración. ▪ Existencia: Tomo $x_1 \in M$ tal que $Ann_A(M) = ann_A(x_1)$. La proposición anterior me dice que $Ax_1 \stackrel{\cdot}{+} N = M$ para cierto submódulo N de M.
Es claro que $Ann_A(N) =\supseteq Ann_A(M) =< p^t >\Rightarrow Ann_A(N) =< p^{t'} >$ con $t' \leq t$, y $l(N) < l(M)$. Por inducción sobre $l(M)$, tengo

$x_2, \ldots, x_n \in N$ tales que $Ann_A(N) = ann_A(x_2) \subseteq \cdots \subseteq ann_A(x_n)$ y $N = Ax_2 \dot{+} \cdots \dot{+} Ax_n \Rightarrow M = Ax_i \dot{+} Ax_2 \dot{+} \cdots \dot{+} Ax_n$, y $Ann_A(M) = ann_A(x_1) \subseteq ann_A(x_2) \subseteq \cdots \subseteq ann_A(x_n)$.

- Unicidad: Hacemos inducción sobre $l(M)$.
  - Si $l(M) = 1 \Rightarrow M = Ax_1 = Ay_1 \Rightarrow n = 1 = m$.
  - Si $l(M) > 1$, entonces M no es simple. Tomamos $\frac{M}{pM}$ ($pM = \{pm : m \in M\}$).

$$Ann_A(\frac{M}{pM}) =< p >\Rightarrow Soc(\frac{M}{pM}) = \frac{M}{pM}$$

$\Rightarrow \frac{M}{pM}$ es semisimple.

Tenemos un homomorfismo de módulos $M \to \frac{Ax_1}{Apx_1} \oplus \cdots \oplus \frac{Ax_n}{Apx_n}$ dado por $\sum_{i=1}^{n} a_i x_i \mapsto (a_1 x_1 + Apx_1, \ldots, a_n x_n + Apx_n)$, que es sobreyectivo y cuyo núcleo es pM.

$$\frac{M}{pM} \cong \frac{A}{Apx_1} \oplus \cdots \oplus \frac{A}{Apx_n}$$

y cada $\frac{A}{Apx_i}$ es simple $\Rightarrow n = l(\frac{M}{pM})$.

Razonando de manera análoga con $y_1, \ldots, y_m \Rightarrow m = l(\frac{M}{pM}) \Rightarrow m = n$.

Si $pM = \{0\}$, entonces todos los $ann_A(x_i) =< p >= ann_A(y_i)$.

Si $pM \neq \{0\}$, entonces $pM = Apx_1 \dot{+} \cdots \dot{+} Apx_n = Apx_1 \dot{+} \cdots \dot{+} Apx_r$, para cierto $r \leq n$. Así, $ann_A(x_i) =< p > \iff i > r$.
Para cualquier $i \leq r, ann_A(px_i) =< p^{t_i - 1} >$ si $ann_A(x_i) =< p^{t_i} >$. Como consecuencia:

$$ann_A(px_1) \subseteq ann_A(px_2) \subseteq \cdots \subseteq ann_A(px_r)$$

Razonando de forma análoga para y_i, llegamos a que
$ann_A(py_i) =< p^{s_i - 1} >$ si $ann_A(y_i) =< p^{s_i} >$ con $s_i > 1$, donde $ann_A(y_i) =< p > \iff i > s$.

$$pM = Apy_1 \dot{+} \cdots \dot{+} Apy_s$$

pero $l(pM) < l(M) \overset{\text{indución}}{\Rightarrow} s = r$ y $s_i - 1 = r_i - 1$ para $i \in \{1, \ldots, r\}$.
Como sé que para $i > n, ann_A(x_i) = ann_A(y_i) =< p >$, y hemos terminado.

□

Observación: Si $A = \mathbb{Z}$, M grupo abeliano y $x \in M$, entonces $ann_{\mathbb{Z}}(x) = n\mathbb{Z}, n = \text{orden}(x)$.

Si $A = K[X], V \xrightarrow{R} > V, dim_K V < \infty, v \in V, ann_{K[X]}(v) =< f(x) >$. Si $f(x)$ tiene grado n, entonces $\{v, Tv, T^2v, \ldots, T^{n-1}v\}$ es linealmente independiente, pero $\{v, Tv, T^2v, \ldots, T^n v\}$ es linealmente dependiente.

Ejemplo 6.8
$U(\mathbb{Z}_8) = \{1, 3, 5, 7\}$.

- $ord(1) = 1$.
- $ord(3) = 2 \quad (3^2 = 9 = 1)$.
- $ord(5) = 2$.
- $ord(7) = 2$.

$U(\mathbb{Z}_8) =< 3 > \dot{+} < 5 >$. *(no son ideales, son subgrupos generados por).*

Ejercicio: Calcular para $U(\mathbb{Z}_{16})$.

Ejemplo 6.9
$dim_K V = 3, T : V \to V$, *polinomio mínimo*$(T) = (X - \lambda)^2, \lambda \in K$.
$\Rightarrow \exists v_1, v_2 \in V$ *tal que* $V = K[X]v_1 \dot{+} K[X]v_2$ *con* $ann_{K[X]}v_1 =< (X - \lambda)^2 >$, *y además,* $K[X]v_1$ *tiene dimensión 2, por lo que* $ann_{K[X]}v_1 =< (X - \lambda)^2 > \subset < X - \lambda >= ann_{K[X]}v_2$.

Si $dim_K V = 4$, *entonces tendríamos dos posibilidades: que* $annK[X]v_2 =< (X - \lambda)^2 >$ *(dim 2), o que hubiese otro* v_3 *tal que* $V = K[X]v_1 \dot{+} K[X]v_2 \dot{+} K[X]v_3$, *y* $ann_{K[X]}v_3$ *tuviese dimensión 1.*

Corolario 6.10
A DIP, A no es un cuerpo. Si M *es un* $A-$*módulo de longitud finita* $p-$*primario, entonces:*

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

con C_i *cíclico.*

Si:

$$M \cong D_i \oplus \cdots \oplus D_m$$

con D_i *cíclico, entonces* $n = m$ *y, tras reordenación,* $D_i \cong C_i$, $\forall i \in \{1, \ldots, n\}$.

Demostración. De $M \cong C_1 \oplus \cdots \oplus C_n$ obtengo que $x_1, \ldots, x_n \in M$ tal que $M = Ax_1 \dot{+} \cdots \dot{+} Ax_n$ con $ann_A(x_1) \subseteq ann_A(x_2) \subseteq \cdots \subseteq ann_A(x_n)$.

De $M \cong D_1 \oplus \cdots \oplus D_m$ obtengo $y_1, \ldots, y_m \in M$ tal que $M = Ay_1 \dot{+} \cdots \dot{+} Ay_m$ con $ann_A(y_1) \subseteq ann_A(y_2) \subseteq \cdots \subseteq ann_A(y_m)$.

$\Rightarrow n = m$ y $ann(x_i) = ann_A(y_i), i \in \{1, \ldots, n\}$, y:

$$C_i \cong Ax_i \cong \frac{A}{ann_A(x_i)} = \frac{A}{ann_A(y_i)} \cong Ay_i \cong D_i$$

□

Definición 6.11 (Indescomponible)
Un módulo M se dice indescomponible si $M \cong L \oplus N \Rightarrow L = \{0\}$ ó $N = \{0\}$.

Ejercicio 6.12
Razonar que, en el corolario, cada C_i es indescomponible.

Ejemplo 6.13
M grupo abeliano, $l(M) < \infty$ y $p-$primario (p primo)
$\overset{Corolario}{\Rightarrow}$ *$M \cong C_1 \oplus \cdots \oplus C_n, C_i$ cíclico, $l(C_i) < \infty, p$-primario.*
$\Rightarrow M \cong \mathbb{Z}_{p^{m_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{m_n}}$, *para $m_1, \ldots, m_n$ enteros positivos.*
$(\Rightarrow M$ *es finito de cardinal $p^{m_1+\cdots+m_n}$).*

Teorema 6.14 (Teorema de estructura de módulos de longitud finita sobre un DIP)
A DIP, ${}_AM \neq \{0\}, l(M) < \infty$. Existen irreducibles distintos $p_1, \ldots, p_r \in A$ y enteros positivos $n_1, \ldots, n_r; e_{i1} \geq \cdots \geq e_{in_i}, i \in \{1, \ldots, r\}$ determinados por M tal que:

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

para $x_{ij} \in M$ adecuados que verifican que:

$$ann_A(x_{ij}) =< p_i^{e_{ij}} >, i \in \{1, \ldots, r\}, j \in \{1, \ldots, n_i\}$$

Estos parámetros determinan M salvo isomorfismo.

Teorema 6.15 (Anterior)
A DIP, ${}_AM \neq \{0\}$, $l(M) < \infty, < \mu >= Ann_A(M), 0 \neq \mu \in A$.
$\mu = p_1^{e_1} \ldots p_r^{e_r}, p_i \in A$ irreducibles, $e_i \geq 1$.

$$M = M_1 \dot{+} \cdots \dot{+} M_r, M_i \; p_i - primario$$

$M_i = \dot{+}_{j=1}^{n_i} Ax_{ij}$, tal que $ann_A(x_{ij}) =< p_i^{e_{ij}} >$, donde
$e_i = e_{i1} \geq \cdots \geq e_{in_i} \geq 1$.

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

Esta descomposición es única.

Demostración. Unicidad: Si $M = N_1 \dot{+} \cdots \dot{+} N_t$ con N_i s_i-primario para $s_1, \ldots, s_t \in A$ irreducibles, entonces:

$$< \mu >= Ann_A(M) = \bigcap_{i=1}^{t} Ann(N_i) = \bigcap_{i=1}^{t} < s_i^{fi} >=< s_1^{f_1} \ldots s_t^{f_t} >$$

μ es asociado (se diferencian en multiplicar por una unidad) con $s_1^{f_1} \dots s_t^{f_t} \overset{\text{tras reordenación}}{\Rightarrow} t = r$ y $s_i = p_i, f_i = e_i, i \in \{1, \dots, r\}$.

$$N_i \subseteq \{m \in M : p_i^{e_i} m = 0\} = M_i \Rightarrow N_i = M_i, \forall i \in \{1, \dots, r\}$$

□

Definición 6.16
Descomposición cíclica primaria de M: $M = \dot{+}_{i=1}^{r}(\dot{+}_{j=1}^{n_i} Ax_{ij})$.
Divisores elementales de M: $\{p_i^{e_{ij}}\}$.

Ejemplo 6.17
$A = \mathbb{Z}, M$ grupo abeliano de longitud finita.

$$M = \dot{+}_{i=1}^{r}(\dot{+}_{j=1}^{n_i} \mathbb{Z}x_{ij}), x_{ij} \in M$$

$\mu = p_1^{e_1} \dots p_r^{e_r} \in \mathbb{Z}$.

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

$\Rightarrow M$ *finito de cardinal* $m = \prod_{i=1}^{r} \prod_{j=1}^{n_i} p_i^{e_{ij}} = p_1^{f_1} \dots p_r^{f_r}, f_i = \sum_{j=1}^{n_1} e_{ij} \Rightarrow \mu \mid m$.

Si $m = 12 \Rightarrow m = 2^2 \cdot 3 \Rightarrow M \cong \begin{cases} \mathbb{Z}_4 \oplus Z_3 \cong Z_{12} \\ \mathbb{Z}_2 \oplus Z_2 \oplus Z_3 \cong Z_2 \oplus Z_6 \end{cases}$.

Ejemplo 6.18
$A = K[X], V$ $K[X]-$módulo de longitud finita $\Rightarrow T : V \to V$ $K-$lineal y V dimensión finita.

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

$K[X]x_{ij}$ de dimensión finita $\Rightarrow V$ tiene dimensión finita.

$V_{ij} = K[X]x_{ij} \subseteq V$ y $T(V_{ij}) \subseteq V_{ij}$. Entonces $minpol(T\mid_{V_{ij}}) = p_i^{e_{ij}} \Rightarrow \exists x_{ij}$ tal que $\{x_{ij}, Tx_{ij}, \dots\}$ (hasta T elevado al grado de $p_i^{e_{ij}}$) es base de V_{ij}, ya que es cíclico.

Caso particular: $T : V \to V, dim_K V = n, minpol(T) = (x - \lambda)^n, \lambda \in K$.
$\exists v \in V$ tal que $B = \{v, (T - \lambda)v, \dots, (T - \lambda)^{n-1}v\}$ es $K-$base de V.

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

Entonces la matriz de la base es (escrita por filas):

$$M_B(T) = \begin{pmatrix} \lambda & 1 & 0 & 0 & \dots & 0 \\ 0 & \lambda & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & 0 & \dots & \lambda \end{pmatrix} = \mathcal{J}_n(\lambda) \to \text{ Bloque de Jordan}$$

Si le aplico eso al caso general, obtengo que $\mu = (x-\lambda_1)^{e_i}\dots(x-\lambda_r)^{e_r}$, *tomo en cada* $V_{ij} = K[X]x_{ij}$ *la base* $\{x_{ij}, (T-\lambda)x_{ij}, \dots, (T-\lambda)^{e_{ij}-1}x_{ij}\}$ *y obtengo "uniendo ordenadamente" las bases, obtengo una base de* V, *llámese* B, *tal que* $M_B(T)$ *es una diagonal por bloques:*

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

Ejemplo 6.19
$B \in M_n(\mathbb{R}), y = (y_1, \dots, y_n) \in C^\infty(\mathbb{R})^n = C^\infty(\mathbb{R}) \times \dots \times C^\infty(\mathbb{R})$.
① $y' = yB$.

Soluciones de ①: $M = \{y \in C^\infty(\mathbb{R})^n \mid y' = yB\}$ *es un subespacio vectorial de* $C^\infty(\mathbb{R}^n)$.
$C^\infty(\mathbb{R})^n$ *es un* $\mathbb{R}[X]-$*módulo, y* M *es un* $\mathbb{R}[X]-$*submódulo de* $C^\infty(\mathbb{R})^n$, *ya que si* $y \in M$, *entonces* $Xy = y' = yB \in M$. *Además, tenemos que* $dim_{\mathbb{R}} M < \infty \Rightarrow_{\mathbb{R}[X]} M$ *tiene una descomposición cíclica primaria.*

Si $x \in \mathbb{R}^n$, *pongo* $y = xe^{tB}, y' = xet^B B = yB$.
<u>Recordatorio</u>: $x \in M_n(\mathbb{C}), e^x = \sum\limits_{m\geq 0} \frac{x^m}{m!}$.
¿Cómo se calcula e^{tB}*? Tomo* J *la forma canónica de Jordan de* B *vista como matriz de* $M_n(\mathbb{C})$. *Entonces* $\exists P \in GL_n(\mathbb{C})$ *tal que* $P^{-1}BP = J$, *y por tanto:*

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

e^{tJ} *si se "saben" calcular.*

Ejemplo 6.20 (Subejemplo)
Vamos a ver que ocurre si $n = 2$. $B \in M_2(\mathbb{R})$.
μ = *polinomio mínimo de* B *(sobre* $\mathbb{C}$*).*

Caso 1. $\mu = (x-\lambda_1)(x-\lambda_2)$, *con* $\lambda_1, \lambda_2 \in \mathbb{R}$ *distintos ó* $\mu = x - \lambda$.
En este caso J *es una matriz diagonal:*

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

y entonces:

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

Caso 2. $\mu = (x-\lambda)^2$, *con* $\lambda \in \mathbb{R}$. *En este caso:*

$$J = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} \Rightarrow tJ = \begin{pmatrix} t\lambda & t \\ 0 & t\lambda \end{pmatrix} = \begin{pmatrix} t\lambda & 0 \\ 0 & t\lambda \end{pmatrix} + \begin{pmatrix} 0 & t \\ 0 & 0 \end{pmatrix}$$

y entonces:

$$e^{tJ} = e^{\begin{pmatrix} t\lambda & 0 \\ 0 & t\lambda \end{pmatrix} + \begin{pmatrix} 0 & t \\ 0 & 0 \end{pmatrix}} \overset{\star}{=} e^{\begin{pmatrix} t\lambda & 0 \\ 0 & t\lambda \end{pmatrix}} e^{\begin{pmatrix} 0 & t \\ 0 & 0 \end{pmatrix}} =$$

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

$\star$ *porque las matrices conmutan.*

Caso 3. $\mu = (x-z)(x-\bar{z})$, $z \in \mathbb{C} \setminus \mathbb{R}$. *En este caso:*

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

y entonces:

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

Alternativamente (si no queremos usar números complejos) $\mu = x^2 + bx + c \in \mathbb{R}[X]$ *irreducible. Llamamos* $\alpha = \sqrt{c - \frac{b^2}{4}}, \beta = -\frac{b}{2}$.
$V = \mathbb{R}^2, T : \mathbb{R}^2 \to \mathbb{R}^2, Tv = vB$.
Tomo $v \in \mathbb{R}^2$ *no nulo, y tengo la* $\mathbb{R}-$*base de* V $\{-\beta v, (T-\alpha)v\}$.
Entonces:

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

$$T(T-\alpha)v = (T^2 - \alpha T)v \overset{T^2 = -bI - cI}{=} \alpha(T-\alpha)v - \beta^2 v$$

En esta base:

$$c = M_T = \begin{pmatrix} \alpha & -\beta \\ \beta & \alpha \end{pmatrix} = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} + \begin{pmatrix} 0 & -\beta \\ \beta & 0 \end{pmatrix}$$

y estas matrices conmutan. Además, $\exists Q \in GL_2(\mathbb{R})$ *tal que*
$c = Q^{-1}BQ$, *por lo que:*

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

Ejercicio 6.21
Sucesión $c_k = \cos k\nu, \nu \in \mathbb{R}$ *fijo.*

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

Demostrar que $\cos(k+2)\nu = 2\cos(k+1)\nu\cos\nu - \cos k\nu, k \geq 0$. *Esto implica que* c_k *es linealmente recursiva.*

Nota: $\cos(k+2)\nu = \cos((k+2)\nu)$.

Pista: Buscar el polinomio mínimo de $\{c_k\}$ *en* $\mathbb{C}[X]$.

Notación: A partir de ahora, R anillo. ${}_RM$ módulo, $\mathcal{L}(M) = \{$submódulos de $M\}$. Si $\emptyset \neq \Gamma \subset \mathcal{L}(M)$; $\bigcap_{N\in\Gamma} N \in \mathcal{L}(M)$.

Definición 6.22
Si X *es un subconjunto de* M*, el menor (para la inclusión) submódulo de* M *que contiene a* X *se llama submódulo generado por* X.

Es decir, tomamos como Γ *todos los subconjuntos de* M *que contiene a* X*, y el submódulo generado por* X *es su intersección.*

Lo denotaremos por RX.

Lema 6.23
$RX = \{\sum_{x\in F} v_x x : F \subseteq X$ *finito,* $v_x \in R\} = \star$.

Demostración. $X \subseteq RX$ por definición $\Rightarrow$ Se cumple $\supseteq$.

Si veo que $\star$ es un submódulo, hemos terminado, ya que $\star$ contiene a X; y si vemos que es un submódulo (el menor) que contiene a X, tenemos la demostración.

Si X es finito, $X = \{x_1, \ldots, x_n\}$, entonces:

$$RX = Rx_1 + \cdots + Rx_n$$

La inclusión $\supseteq$ es obvia. Para la inclusión $\subseteq$, tenemos que ver que $Rx_1 + \cdots + Rx_n \supseteq \{x_1, \ldots, x_n\}$ y como RX es el menor submódulo que contiene a este conjunto, tenemos la igualdad. $\square$

7. Álgebra lineal básica sobre un anillo

Definición 7.1
I conjunto no vacío. Para cada $i \in I$, tomo un módulo M_i, y formamos el producto de todos estos módulos:

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

es un $R-$módulo: $(m_i)_{i\in I} + (m'_i)_{i\in I} = (m_i + m'_i)_{i\in I}$ y $r(m_i)_{i\in I} = (rm_i)_{i\in I}$. A diferencia del producto cartesiano, estas tuplas no tiene que estar ordenadas.

A este módulo se le llama módulo producto de $\{M_i : i \in I\}$.

Observación: Para cada $j \in I$,

$$\begin{array}{lll} M_j \overset{L_j}{\to} & \prod_{i\in I} M_i \overset{\pi_j}{\to} & M_j \\ m_j \mapsto & (0,\ldots,0,m_j,0,\ldots,0) & \\ & (m_i)_{i\in I} & \mapsto m_j \end{array}$$

L_j y π_j son homomorfismos de $R-$módulos.

Definición 7.2
Defino $\oplus_{i\in I} M_i$ como el submódulo de $\prod_{i\in I}$ que contiene a $L_j(M_j), \forall j \in I$.

$$\bigoplus_{i\in I} M_i = \{(m_i)_{i\in I} : m_i = 0 \text{ salvo un } n^o \text{ finito de } i\}$$

Si definimos $sop(m_i)_{i\in I} = \{i \in I : m_i \neq 0\}$, entonces:

$$\oplus_{i\in I} M_i = \{(m_i)_{i\in I} : sop(m_i)_{i\in I} \text{ finito}\}$$

Esto se llama suma directa externa de $\{M_i : i \in I\}$.

Definición 7.3
$\{M_i : i \in I\} \subseteq \mathcal{L}(M)$.
Puedo construir el submódulo suma $\sum_{i\in I} M_i$ como el menor submódulo que contiene a $M_i, \forall i \in I$.

$$\sum_{i\in I} M_i = \{\sum_{i\in F} m_i \mid m_i \in M_i, F \subseteq I \text{ finito}\}$$

Tomo $\theta : \oplus_{i\in I} M_i \to \sum_{i\in I} M_i$ tal que $\theta((m_i)_{i\in I}) = \sum_{i\in I} m_i$. Este θ es un homomorfismo sobreyectivo de $R-$módulos.

Proposición 7.4
Para $\{N_i : i \in I\} \subseteq \mathcal{L}(M)$ *son equivalentes:*

① $\forall j \in I, N_j \bigcap \sum_{j \neq i \in I} N_i = \{0\}$.

② $\forall F \subseteq I$ *finito,* $\forall j \in F, N_j \bigcap \sum_{j \neq i \in F} N_i = \{0\}$.

③ *La expresión de cada* $m \in \sum_{i \in I} N_i$ *como* $m = \sum_{i \in I} m_i, m_i \in N_i$ *es única.*

④ *Si* $0 = \sum_{i \in I} m_i$, *con* $m_i \in N_i, \forall i \in I \Rightarrow m_i = 0, \forall i \in I$.

⑤ θ *es inyectivo (y por tanto, isomorfismo).*

⑥ *Para cada* $J_1, J_2 \subseteq I$ *con* $J_1 \bigcap J_2 \neq 0$, *se tiene que* $(\sum_{i \in J_1} N_i) \bigcap (\sum_{j \in J_2} N_j) = \{0\}$.

Definición 7.5
En caso de satisfacerse las condiciones equivalentes anteriores, diré que $\sum_{i \in I} N_i$ *es una suma directa interna, notación* $\dot{+}_{i \in I} N_i$.

Corolario 7.6
Si $\{N_i : i \in I\} \subseteq \mathcal{L}(M)$ *verifica* ①-⑥ *y* $N \in \mathcal{M}$ *tal que* $N \bigcap \sum_{i \in I} N_i = \{0\}$, *entonces* $\{N_i : i \in I\} \bigcup \{N\}$ *satisface* ①-⑥.

Definición 7.7
Si $\{N_i : i \in I\} \subseteq \mathcal{L}(M)$ *satisface* ①-⑥ *y* $N_i \neq \{0\}, \forall i \in I$, *diremos que* $\{N_i : i \in I\}$ *es independiente.*

Caso particular: $\forall i \in I$, tomo $M_i = R \Rightarrow \oplus_{i \in I} M_i = R^{(I)}$, o sea:

$$R^{(I)} = \{(v_i)_{i \in I} \in R^I : sop((v_i)_{i \in I}) < \infty\}$$

$R^{(I)}$ módulo libre.

Ejemplo 7.8
A DIP, ${}_AM$ *módulo.* $t(M) = \{m \in M : ann_A(m) \neq < 0 >\}$ *es un submódulo de* M *que se llama submódulo de torsión de* M.

Supongamos que $t(M) \neq \{0\}$.
$\mathcal{P}$ = *conjunto de representantes de las clases de equivalencia (bajo la relación "ser asociados") de los irreducibles de* A.
Para cada $p \in \mathcal{P}$, *definimos* $M_p = \{m \in M : p^e m = 0$ *para algún* $e \geq 1\}$.

$$M_p \subseteq t(M), M_p \text{ submódulo}$$

Vamos a ver que todos los M_p *forman una familia independiente cuya suma directa interna es* $t(M)$, *es decir,* $t(M) = \dot{+}_{p \in \mathcal{P}} M_p$.

Tomo $m \in t(M)$, entonces Am es finitamente generado, y como $ann_A(m) \neq \{0\}$, entonces Am es de longitud finita. Por lo que tiene descomposición primaria:

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

con N_i p_i-primario. Esto significa que:

$$m = m_1 + \cdots + m_r$$

de manera única, con $m_i \in N_i \subseteq M_{p_i}, \forall i \in \{1, \ldots, r\}$.

$$M = \sum_{p \in \mathcal{P}} M_p$$

Es fácil ver la unicidad, por lo que:

$$M = \dot{\sum_{p \in \mathcal{P}}} M_p$$

Los $\{M_p : p \in \mathcal{P}\}$ se llaman componentes primarias de $t(M)$.

Ejemplo 7.9 (Subejemplo)
$M = C^\infty(\mathbb{R}), M$ $\mathbb{R}[X]-$módulo si $Xf = f'$.

$$t(M) = \{\textit{funciones que satisfacen una EDO con coeficinetes constantes}\}$$

$$\mathcal{P} = \{\textit{lineales, cuadráticos irreducibles}\}$$

Nota: M_p no tiene por qué tener dimensión finita.

Ejemplo 7.10
Si tomamos como M las sucesiones en $\mathbb{R}$, y como X la que nos lleva cada término en el siguiente.

$$(a_0, a_1, a_2, \ldots) \mapsto (a_1, a_2, \ldots)$$

Entonces $t(M)$ son las sucesiones recursivas.

Definición 7.11
I conjunto. $R^{(I)} =$ suma directa externa de I copia de $R = \{(r_i)_{i \in I} : r_i \in R$ y $r_i = 0$ salvo en un número finito de indices$\} = \{(r_i)_{i \in I} : r_i \in R, sop((r_i)_{i \in I})$ finito$\}$.

Lema 7.12
Si M es cualquier $R-$módulo, existe una sucesión exacta de la forma:

$$0 \to L \to R^{(I)} \xrightarrow{\varphi} M \to 0$$

para I adecuado.

Demostración. Tomo $\{m_i : i \in I\}$ tal que $M = \sum_{i \in I} Rm_i$.

Defino $\varphi : R^{(I)} \to M$ por $\varphi((r_i)_{i \in I}) = \sum_{i \in I} r_i m_i$.

Tomamos $L = Ker\varphi \hookrightarrow M$. □

Lema 7.13
Para $\{m_i : i \in I\} \subseteq M$, son equivalentes:

1. $\sum_{i \in I} r_i m_i = 0 \Rightarrow r_i = 0, \forall i \in I$.
2. *El homomorfismo de módulos $\varphi : R^{(I)} \to M, \varphi((r_i)_{i \in I}) = \sum_{i \in I} r_i m_i$ es inyectiva.*

Demostración. Trivial. □

Definición 7.14
Si se satisface 1., diré que el conjunto $\{m_i : i \in I\}$ es linealmente independiente.

Si ademas, $\{m_i : i \in I\}$ son un conjunto de generadores, diré que $\{m_i : i \in I\}$ es una base de M.

Proposición 7.15
M tiene una base $\iff$ $M \cong R^{(I)}$ para algún I.

Demostración. Para $\Rightarrow$, el isomorfismo es el de 2. del lema 7.13. □

Definición 7.16 (Módulo libre)
Un módulo es libre si tiene una base.

Advertencia: Hay, en general, muchos módulos que no son libres.

Ejemplo 7.17
Ningún grupo abeliano finito es libre como $\mathbb{Z}-$módulo, ya que si tuviera una base sería isomorfa a $\mathbb{Z}^{(I)}$, que es infinito.

Ejemplo 7.18
A DIP, ${}_AM$, $t(M)$ nunca es libre. $t(M)$ se conserva por isomorfismos.

Si A DIP, $A^{(I)}$ nunca es de torsión.

Proposición 7.19
Sea M un módulo. Existe una sucesión exacta:

$$\ldots \overset{f_{-2}}{\to} F_{-1} \overset{f_{-1}}{\to} F_0 \overset{f_0}{\to} M \to 0$$

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

Demostración. La demostración consiste en explicar como se construye.

Tomo un conjunto de generadores de M, y un homomorfismo de módulos sobreyectivo $F_0 \stackrel{p_0}{\to} M$.

$$Ker(p_0) = K_0 \stackrel{i_0}{\to} F_0 \stackrel{p_0}{\to} M \to 0$$

Como K_0 es módulo, existe F_{-1} libre y p_{-1} sobreyectivo tal que:

$$F_{-1} \stackrel{p_{-1}}{\to} K_0 \stackrel{i_0}{\to} F_0 \stackrel{p_0}{\to} M \to 0$$

Llamando f_1 a la composición de p_{-1} y i_0, tenemos:

$$F_{-1} \stackrel{f_{-1}}{\to} F_0 \stackrel{p_0}{\to} M \to 0$$

Reiterando el procedimiento, tenemos la sucesión. Nos queda ver que es exacta.

Veamos la exactitud en F_{-1} (ya que en cualquier F_{-i} es igual). Tenemos que ver que se cumple $Imf_{-2} = Kerf_{-1}$. Sabemos que Imf_2 es la composición de p_{-2} y i_{-1}, entonces $Imf_{-2} = Imp_{-2} = K_{-1} = Kerf_{-1}$. □

Definición 7.20
Si esta resolución es finita, entonces diré que es una resolución libre finita.

Hay anillos y módulos sobre anillos que no admiten ninguna resolución finita.

Definición 7.21
M módulo se dice finitamente presentado si existe una presentación finita, que no es sino una sucesión exacta de la forma:

$$F_{-1} \stackrel{f_{-1}}{\to} F_0 \stackrel{f_0}{\to} M \to 0$$

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

Ejercicio 7.22
Dar una presentación finita del $\mathbb{Z}-$módulo $\mathbb{Z}_2 \oplus \mathbb{Z}_4$.

Proposición 7.23
Una anillo R es noetheriano a izquierda si, y sólo si, todo módulo finitamente generado es finitamente presentado (admite una representación finita).

Demostración. Sólo vamos a ver una implicación: si ${}_RR$ noetheriano $\Rightarrow$ cada finitamente generado es finitamente generado.

Para ello, ${}_RM$ es finitamente generado. Entonces tenemos:

$$F_0 \stackrel{f_0}{\to} M \to 0$$

Entonces:

$$K_0 \to F_0 \overset{f_0}{\to} M \to 0$$

Y como $K_0 = Kerf_0$ es un submódulo de F_0, es fintamente generado.

$$F_{-1} \overset{p_{-1}}{\to} K_0 \to F_0 \overset{f_0}{\to} M \to 0$$

$$F_{-1} \overset{f_{-1}}{\to} F_0 \overset{f_0}{\to} M \to 0$$

□

Corolario 7.24
Todo módulo finitamente generado sobre un DIP es finitamente presentado.

Nota: Por el primer teorema de isomorfía:

$$M \cong \frac{F_0}{Imf_{-1}}$$

ya que $Imf_{-1} = Kerf_0$ por la exactitud.

Tomamos E_s, F_t módulos libres con bases finitas de cardinales s y t respectivamente. Diré que E_s tiene rango s (a pesar del problema de Invariance Number Basis, INB. Por ejemplo, es posible que $R \oplus R \cong R$, $R \oplus R$ tiene base de rango 2 y R tiene base de rango 1, aunque es poco común).

Llamamos:

$$e = \{e_1, \ldots, e_s\}$$

$$f = \{f_1, \ldots, f_t\}$$

las bases de E_s y F_t respectivamente. Sea $\psi : E_s \to F_t$ tal que $\psi(e_i) = \sum_{j=1}^{t} a_{ij} f_j, i \in \{1, \ldots, s\}, a_{ij} \in R$.

$$A_\psi = (a_{ij})_{\substack{1 \le i \le s \\ 1 \le j \le t}} \in M_{s \times t}(R)$$

donde $M_{s \times t}(R)$ son las matrices de tamaño $s \times t$ con coeficientes en R.

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

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

Resulta que $x = (x_1, \ldots, x_s) = u_e, y = (y_1, \ldots, y_t) = \psi(u)_f$:

$$y = xA_\psi$$

Hay que hacer esta operación por filas.

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

La aplicación:

$$\begin{array}{ccc} E_s & \overset{\psi}{\to} & F_t \\ ()_e \downarrow & = \searrow & ()_f \downarrow \\ R^s & \overset{A_\psi}{\to} & R^t \end{array}$$

Si tenemos tres módulos libres:

$$\begin{array}{ccccc} E_s & \overset{\psi}{\to} & F_t & \overset{\varphi}{\to} & G_r \\ ()_e \downarrow & & ()_f \downarrow & & ()_g \downarrow \\ R^s & \overset{A_\psi}{\to} & R^t & \overset{A_\varphi}{\to} & R^r \end{array}$$

Y tenemos:

$$R^s \overset{A_{\varphi o \psi}}{\to} R^r$$

donde:

$$A_{\varphi o \psi} = A_\varphi A_\phi$$

Ejemplo 7.25
Sea $T : V \to V$ homomorfismo de $K-$espacios vectoriales, $dim_K V < \infty$. Tengo que ${}_{K[X]}V$ es un módulo finitamente presentado. Queremos una presentación finita.

Tomamos una $K-$ base $\{v_1, \ldots, v_n\}$ de V (notemos que no existe base de V como $K[X]-$módulo). Entonces:

$$T(v_i) = \sum_{j=1}^{n} b_{ij} v_j, i \in \{1, \ldots, n\}, b_{ij} \in M_n(k)$$

Tomo F_n un $K[X]-$módulo libre con base $\{f_1, \ldots, f_n\}$ y defino $\phi : F_n \to V$, $\phi(f_i) = v_i, i \in \{1, \ldots, n\}, \phi$ es un homomorfismo de $K[x]-$módulos sobreyectivo.

$$F_n \overset{\phi}{\to} V \to 0$$

$$Xf_i - \sum_{j=1}^{n} b_{ij} f_j \in Ker\phi, i \in \{1, \ldots, n\}$$

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

Dado $x \in F_n, x = \sum_{i=1}^{n} p_i(x) f_i$, *con* $p_i(x) \in K[x]$. *Si* $x \neq 0$, *llamo* $w(x) = \sum_{i=1}^{n} \deg p_i \geq 0$, *donde sólo aparecen los* $p_i \neq 0$ *(quitamos los polinomios de grado 0 porque en muchos casos se les considera de grado* $-\infty$*).*

$$w(x) = 0 \Rightarrow p_i \in K, \forall i$$

Suponemos $x \in Ker\phi$. *Vamos a ver que pasa con su peso (*$w(x)$*):*

- *Si* $w(x) = 0 \Rightarrow \sum_{i=1}^{n} p_i f_i = x, p_i \in K$.

$$\sum_{i=1}^{n} p_i v_i = 0 \Rightarrow p_i = 0 \Rightarrow x = 0$$

- *Si* $x \neq 0$ *y* $x \in Ker\phi, w(x) \geq 1$. *Vamos a demostrar que el conjunto* $\{Xf_i - \sum_{j=1}^{n} b_{ij} f_j : i \in \{1, \ldots, n\}\}$ *es un sistema de generadores por inducción sobre* $w(x)$.
  - $w(x) = 1 \Rightarrow \exists$ *un único índice* $k \in \{1, \ldots, n\}$ *tal que* p_k *no es constante, y además* $p_k = aX + b$, *con* $a, b \in K$.

$$x = \sum_{i \neq k} p_i f_i + (aX + b) f_k =$$

$$= \sum_{i \neq k} p_i f_i + \underbrace{a(Xf_k - \sum_{j=1}^{n} b_{kj} f_j)}_{\in Ker\phi} + a \sum_{j=1}^{n} b_{kj} f_j + b f_k$$

$$\Rightarrow \sum_{i \neq k} p_i f_i + a \sum_{j=1}^{n} b_{kj} f_j + b f_k \in Ker\phi \Rightarrow$$

$$\Rightarrow \sum_{i \neq k} p_i f_i + a \sum_{j=1}^{n} b_{kj} f_j + b f_k = 0 \Rightarrow$$

$$\Rightarrow x = a(Xf_k - \sum_{j=1}^{n} b_{kj} f_k)$$

  - *Caso general:* $w(x) > 1$. *Entonces existe algún* $k \in \{1, \ldots, n\}$ *para el que* $\deg p_k \geq 1$. *Así,* $p_k(x) = q(x)x + b$, *con* $\deg q(x) = \deg p_k(x) - 1, (b \in K)$.

$$x = \sum_{i \neq k} p_i(x) f_i + \underbrace{q(x)(Xf_k - \sum_{j=1}^{n} b_{kj} f_j)}_{\in Ker\phi} + q(x) \sum_{j=1}^{n} b_{kj} f_j + b f_k$$

$$\Rightarrow y := \sum_{i\neq k} p_i(x)f_i + q(x)\sum_{j=1}^{n} b_{kj}f_j + bf_k \in Ker\phi \Rightarrow$$

$$\Rightarrow x = a(Xf_k - \sum_{j=1}^{n} b_{kj}f_j)$$

Entonces $w(y) \leq w(x) - 1$.

Por inducción, y se escribe como:

$$\sum polinomios(Xf_i - \sum_{j=1} b_{ij}f_j)$$

$\Rightarrow x$ *también.*

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

donde ψ *está definida por* $\psi(f_i) = Xf_i - \sum_{j=1}^{n} b_{ij}f_j, i \in \{1, \ldots, n\}$, *y esa sucesión es exacta.*

$$A_\psi = \begin{pmatrix} X - b_{11} & -b_{12} & \ldots & -b_{1n} \\ -b_{21} & X - b_{22} & \ldots & -b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -b_{n1} & -b_{n2} & \ldots & X - b_{nn} \end{pmatrix} \in M_n(K[X]), A_\psi = XI_n - B$$

con $B = (b_{ij}) \in M_n(K)$.
$A_\psi \equiv$ *Matriz característica de* T.

Lema 7.26
Sea F *un* $R-$*módulo libre y* $M \xrightarrow{\varphi} N$ *un epimorfismo (sobreyectivo) de* $R-$*módulos. Para cada homomorfimos de* $R-$*módulos* $F \xrightarrow{\alpha} N$ *existe un homomorfismo de módulos* $F \xrightarrow{\beta} M$ *tal que* $\varphi\beta = \alpha$.

$$\begin{array}{ccc} M & \xrightarrow{\varphi} & M \to 0 \\ \beta\uparrow & \nearrow \alpha & \\ F & & \end{array}$$

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

Proposición 7.27
Sean ${}_RM, {}_RN$ *finitamente presentados y* $M \xrightarrow{h} N$ *homomorfismo de* $R-$*módulo:*

$$\begin{array}{ccccccc} E_s & \xrightarrow{\psi} & F_t & \xrightarrow{\phi} & M \to & 0 \\ p\downarrow & & q\downarrow\searrow & & h\downarrow & \\ E_{s'} & \underset{\psi'}{\to} & F_{t'} & \underset{\phi'}{\to} & N \to & 0 \end{array}$$

Dado $h : M \to N$*:*
$\exists q$ *tal que* $\phi' q = h\phi$.
$\exists p$ *tal que* $\psi' p = q\psi$.
Observemos que $Im q\psi \subseteq Ker\phi' = Im\psi'$.

Dados $p : E_s \to E_{s'}$, *y* $q : F_t \to F_{t'}$, *construimos* h. *Para ello, tomo* $m \in M$ *y* $u \in F_t$ *tal que* $m = \phi(u)$. *Quiero definir* $h(m) = \phi'(q(u)) \in N$. *Veamos que* $h(m)$ *es independiente del* u *elegido.*
Para ello, tomamos $v \in F_t$ *tal que* $\phi(v) = m$. *Como* $0 = \phi(v-m) \Rightarrow v-u \in Ker\phi$ *y podemos tomar* $x \in E_s$ *tal que* $v - u = \psi(x)$.

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

Como $h(m)$ *es independiente del* u *elegido, tenemos que* h *está bien definida. Es fácil ver que* h *es un homomorfismo de módulos.*

Fijados 4 bases en módulos libres del diagrama, definir h *es dar una pareja de matrices* A_q *y* A_p *tales que:*

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

Concretamente, si $f = \{f_1, \ldots, f_t\}$ *es base de* F_t *y* $f' = \{f'_1, \ldots, f'_{t'}\}$ *es base de* $F_{t'}$ *y* $A_q = (q_{ij})$, *y tomo* $m_i = \phi(f_i), i \in \{1, \ldots, t\}; n_j = \phi'(f'_j), j \in \{1, \ldots, t'\}$, *tengo:*

1. $\{m_1, \ldots, m_t\}$ *genera* M *y* $\{n_1, \ldots, n_t\}$ *genera* N.
2. $h(m_i) = \sum_{j=1}^{t'} q_{ij} n_j$.

Proposición 7.28 (Cayley-Hamilton)
Sea $T : V \to V$ *un homomorfismo* $K-$*lineal, con* $dim_K V < \infty$. *Sea* $d(x) \in K[x]$ *el polinomio característico de* T *(tomando una base de* V*, se representa una* T *con respecto una base y determinante es el polinomio característico). Entonces el polinomio mínimo de* T *divide a* $d(x)$.

Demostración. Tomo la presentación finita de ${}_{K[x]}V$ que vimos al final del ejemplo 7.25.

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

Tomo A_ψ y P su matriz adjunta, o sea, la que hace $PA_\psi = d(x)I_n$.

Sea $\delta : F_n \to F_n$ el homomorfismo que, fijada base $f = \{f_1, \ldots, f_n\}$ de F_n, tiene como matriz $d(x)I_n$ (o sea, $\delta(f_i) = d(x)f_i$).

$$\begin{array}{ccccc} F_n & \overset{\delta}{\to} & F_n & \overset{\pi}{\to} & \frac{F_n}{Im\delta} \to 0 \\ p\downarrow & & id\downarrow & & h\downarrow \\ F_n & \underset{\psi}{\to} & F_n & \underset{\phi}{\to} & V \to 0 \end{array}$$

Por la proposición anterior, tenemos la existencia de h, y h es sobreyectivo, ya que lo es ϕ ($h_o\pi = \phi$).

$$Ann_{K[X]}(V) \supseteq Ann_{K[X]}(\frac{F_n}{Im\delta}) =< d(x) >$$

La última igualdad se debe a que:

$$\frac{F_n}{Im\delta} \cong \oplus_{i=1}^{n} \frac{K[x]f_i}{K[x]d(x)f_i} = \oplus_{i=1}^{n} \frac{K[x]}{< d(x) >}$$

Como $< d(x) > \subseteq Ann_{K[X]}(V)$, el polinomio mínimo de T divide a $d(x)$. $\square$

Definición 7.29
Una matriz $A = (a_{ij})_{ij} \in M_{s\times t}(R)$ siremos que es cuasi-diagonal si $a_{ij} = 0, \forall i \neq j$.

A no tiene que ser cuadrada, por ejemplo, $A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix}$ es casi-diagonal.

Poniendo la notación $d_i = a_{ii}, \forall i \in \{1, \ldots, m\}$ donde $m = \text{mín}\{s, t\}$, denotamos $A = diag_{s\times t}(d_1, \ldots, d_m)$.

Ejemplo 7.30

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

$$diag_{2\times 3}(2, 0) = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Definición 7.31
Denotamos por $GL_n(R)$ al grupo (bajo el producto) de las matrices invertibles, esto es,

$$GL_n(R) = \{Q \in M_n(R) \mid \exists Q^{-1} \in M_n(R) \text{ con } QQ^{-1} = Q^{-1}Q = I_n\}$$

Proposición 7.32
Sea la presentación finita de ${}_RM$

$$E_s \overset{\psi}{\to} F_t \overset{\phi}{\to} M \to 0$$

Supongamos que existen $P \in GL_s(R), Q \in GL_t(R)$ *y*
$D = diag_{s\times t}(d_1, \ldots, d_n)$, *con* $n = \min\{s,t\}$ *tales que* $PA = DQ$.

Si $\{m_1, \ldots, m_t\}$ *es el conjunto de generadores de* M *tal que* $m_i = \phi(f_i), \forall i \in \{1, \ldots, t\}$ *y* $x_1 = \sum_{j=1}^{t} q_{ij} m_j, \forall i \in \{1, \ldots, t\}$, *con* $Q = (q_{ij})_{ij}$, *entonces* $M = \dot{+}_{i=1}^{t} Rx_i, ann_R(x_i) = Rd_i, \forall i \leq m$ *y* $ann_R(x_i) = \{0\}, \forall i > m$.

Demostración. Definimos $\phi_1 = \phi \cdot q, \phi_1(f_1) = \phi(q(f_1)) \overset{(\star)}{=} \phi(\sum_{i=1}^{t} q_{ij} f_j) = \sum_{j=1}^{t} q_{ij}\phi(f_j) \overset{(\star)}{=} \sum_{j=1}^{t} q_{ij} m_j = x_i$

$(\star) Q = A_q, \phi(f_j) = m_j$

Tenemos entonces el diagrama:

$$\begin{array}{ccccccc} E_s & \overset{\psi_1}{\to} & F_t & \overset{\phi_1}{\to} & M & \to & 0 \\ p\downarrow & & q\downarrow & & id\downarrow & & \\ E_s & \underset{\psi}{\to} & F_t & \underset{\phi}{\to} & N & \to & 0 \end{array}$$

con $A_{\psi_1} = D, A_p = P, A_q = Q$.

La parte de la izquierda conmuta al ser $PA_\psi = DQ$.
Tenemos que ver entonces que la sucesión de arriba es exacta para que sea una presentación. Lo más difícil es la exactitud en F_t, que se consigue empleando que P y Q son invertibles (ejercicio):

Veamos ahora que $M = \dot{+}_{i=1}^{t} Rx_i$, para lo que empleamos que $\{x_1, \ldots, x_t\}$ es un conjunto de generadores de M ($M = Rx_1 + \cdots + Rx_t$, pues $x_i = \phi_1(f_i)$ y ϕ_1 es sobreyectiva).
Veamos que la suma es directa: tomamos $0 = r_1x_1 + \cdots + r_tx_t = \phi_1(r_1f_1 + \cdots + r_tf_t) \Rightarrow r_1f_1 + \cdots + r_tf_t \in Ker\phi_1 = Im\psi_1$.
Además $Im\psi_1 = R\psi_1(e_1) + \cdots + R\psi_1(e_s) \overset{(\star\star)}{=} Rd_1f_1 + \cdots + rd_mf_m = Rd_1f_1 \dot{+} \cdots \dot{+} Rd_mf_m$.

$(\star\star)$ por ser $A_{\psi_1} = D = diag_{s\times t}(d_1, \ldots, d_m)$.

En consecuencia, $r_1 \in Rd_1, \ldots, r_m \in Rd_m$ y si $t > m, r_i = 0, \forall i > m$. Además, para $i \leq m$, tenemos $^{(\star)} r_ix_i = \phi_1(r_if_i)$, con $r_if_i \in Im\psi_1 = Ker\phi_1 \Rightarrow \phi_1(r_if_i) = r_ix_i = 0 \Rightarrow M = \dot{+}_{i=1}^{t} Rx_i$.

$(\star)$ cada r_if_i se puede expresar como $s_id_if_i$, con $s_i \in R$, al ser $r_i \in Rd_i \Rightarrow r_if_i \in Im\psi_1 = Rd_1f_1 + \cdots + Rd_mf_m$.
Por otra parte, tenemos $M \cong \frac{F_t}{Im\psi_1} = \frac{Rf_1 \dot{+} \cdots \dot{+} Rf_t}{Rd_1f_1 \dot{+} \cdots \dot{+} Rd_mf_m} \cong \frac{Rf_1}{Rd_1f_1} \oplus \cdots \oplus \frac{Rf_m}{Rd_mf_m} \oplus \frac{R}{\{0\}} \oplus \overset{(t-m)}{\cdots} \oplus \frac{R}{\{0\}} \overset{(\star\star)}{\cong} \frac{R}{d_1} \oplus \cdots \oplus \frac{R}{Rd_m} \oplus \frac{R}{\{0\}} \oplus \overset{(t-m)}{\cdots} \oplus \frac{R}{\{0\}} \Rightarrow$
$\Rightarrow ann_R(x_i) = Rd_i$.

$(\star\star) \frac{Rf_i}{Rd_if_i} \cong \frac{R}{Rd_i}$. □

Ejemplo 7.33 (Caso particular)
$R = \mathbb{Z} \Rightarrow$ *siempre existen los* P *y* Q *de la proposición.*

Si M *es un grupo abeliano fintamente generado como* $\mathbb{Z}-$*módulo* $\Rightarrow$
$\Rightarrow \exists d_1, \ldots, d_m \in \mathbb{N}$ *tales que*

$$M \cong \underbrace{\mathbb{Z}_{d_1} \oplus \cdots \oplus Z_{d_m}}_{\text{parte finita (de torsión)}} \oplus \underbrace{\mathbb{Z}^{t-m}}_{\text{parte infinita (libre de torsión)}}$$

Proposición 7.34 (Repaso)

$$E_s \overset{\Psi}{\to} \quad F_t \overset{\phi}{\to} \quad M \to \quad 0$$

Hipótesis: $\exists P, Q$ *invertibles,* $D = diag(d_1, \ldots, d_m)$ *tal que* $PA_\Psi = DQ$.
Tesis: *Con* $m_i = \phi(f_i), i \in \{1, \ldots, t\}$

$$x_i = \sum_{j=1}^{t} q_{ij} m_j (i \in \{1, \ldots, t\}), Q = (q_{ij})$$

tengo $M = \dot{+}_{i=1}^{t} Rx_i$ *y* $ann_R(x_i) = Rd_i$ *para* $i \in \{1, \ldots, m\}$, $ann_r(x_i) = \{0\}$ *si* $i > m$.

Ejemplo 7.35 (Ejercicio típico de examen)
K *cuerpo,* $T : V \to V$, *con* $dim_K V = 3$, *base* $\{v_1, v_2, v_3\}$ *de* V.
Matriz de T *en* $\{v_1, v_2, v_3\}$ *es* $B = \begin{pmatrix} 1 & -1 & 1 \\ -1 & -1 & 1 \\ -1 & 1 & 1 \end{pmatrix}$.

Objetivo: *Obtener la descomposición cíclica primaria de* ${}_{K[X]}V$.

Tengo para $A = \begin{pmatrix} x-1 & 1 & -1 \\ 1 & x+1 & -1 \\ 1 & -1 & x-1 \end{pmatrix} \in M_3(K[X])$, *busco* P, Q *y* D.
$v_i = \phi(f_i)$.

$$PA_\Psi = DQ \Rightarrow PA_\Psi Q^{-1} = D$$

Partimos de A *y empezamos haciendo operaciones por filas:*

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

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

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

Utilizamos operaciones por columnas:

$$\begin{pmatrix} 1 & -1 & x-1 \\ 0 & 2 & x^2-3x+2 \\ 0 & 0 & x^3-x^2-2x+4 \end{pmatrix} \overset{c_2+c_1}{\sim} \begin{pmatrix} 1 & 0 & x-1 \\ 0 & 2 & x^2-3x+2 \\ 0 & 0 & x^3-x^2-2x+4 \end{pmatrix} \sim$$

$$\overset{c_3-(x-1)c_1}{\sim} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & x^2-3x+2 \\ 0 & 0 & x^3-x^2-2x+4 \end{pmatrix} \overset{c_3-(\frac{x^2-3x+2}{2})c_2}{\sim} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & x^3-x^2-2x+4 \end{pmatrix} = D$$

Para obtener Q^{-1}, tomamos la matriz $Id_{3\times 3}$, y le realizamos las operaciones por columnas que hemos realizado antes. Para obtener Q, podemos directamente realizar las operaciones en sentido opuesto (comenzamos por la última), y cambiando sumas por restas, y tenemos:

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

Quiero $x_1, x_2, x_3 \in V$ tal que ${}_{K[X]}V = K[X]x_1 \dot{+} K[X]x_2 \dot{+} K[X]x_3$ y que verifican:

- $ann_{K[X]}(x_1) = K[X] \Rightarrow x_1 = 0.$
- $ann_{K[X]}(x_2) = K[X]2 = K[X] \Rightarrow x_2 = 0.$
- $ann_{K[X]}(x_3) =< x^3 - x^2 - 2x + 4 >.$

Del elemento en la posición (3, 3) de Q (que es 1) tenemos que $x_3 = v_3$.

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

y por tanto es cíclico (generado por un único elemento).

Queremos la descomposición primaria. Para ello, tiene que ocurrir que $x^3 - x^2 - 2x + 4$ sea irreducible. Vamos a estudiarlo en tres casos particulares:

- *$K = \mathbb{Q}$. En este caso, el polinomio no tiene raíces (Álgebra I), y por tanto es irreducible.*

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

  es la descomposición cíclica primaria. Además, ${}_{\mathbb{Q}[X]}V$ es simple (${}_{\mathbb{Q}[x]}V = \mathbb{Q}[x]v_3 \cong \frac{\mathbb{Q}[x]}{<\mu>}$ $y <\mu>$ maximal $\Rightarrow {}_{\mathbb{Q}[X]}V$ simple).

  En ${}_{\mathbb{Q}[X]}V$, tomando la base $\{v_3, T(v_3), T^2(v_3)\}$, la matriz de T es:

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

  donde hemos usado $T^3(v_3) = T^2(v_3) + 2T(v_3) - 4v_3$. A esta matriz se le llama "matriz compañera de polinomio mínimo.

- *$K = \mathbb{R}$. $\mu = x^3 - x^2 - 2x + 4$ no es irreducible. Para ver las raíces, lo estudiamos como una función:*

$$\mu'(x) = 3x^2 - 2x - 2 \Rightarrow (\mu'(x) = 0 \iff x = \frac{1 \pm \sqrt{7}}{3})$$

$\mu(\frac{1+\sqrt{7}}{3}) > 0 \Rightarrow \mu(x)$ tiene una única raíz en $\mathbb{R} \Rightarrow$
$\Rightarrow \mu(x) = (x-\alpha)(x-z)(x-\bar{z})$ para $\alpha \in \mathbb{R}, z \in \mathbb{C} \setminus \mathbb{R}$.
$(\mu(x) = (x-\alpha)(x^2 - 2Rezx + |z|^2)$ en $\mathbb{R}[X])$

Tenemos ${}_{\mathbb{R}[X]}V = \mathbb{R}[X]v_3$. Definimos $u_1 = (x-\alpha)v_3 = (T-\alpha)v_3 \Rightarrow$ $ann_{\mathbb{R}[x]}(u_1) =< x^2 - 2Re(z)x + |z|^2 >$. Definiendo $u_2 = (x^2 - 2Re(z)x + |z|^2)v_3 = (T^2 + 2Re(z)T + |z|^2)v^3$, tenemos $ann_{\mathbb{R}[X]}(u_2) =< x - \alpha >$.

En consecuencia, ${}_{\mathbb{R}[X]}V = \underbrace{\mathbb{R}[X]u_1}_{simple} \dot{+} \underbrace{\mathbb{R}[X]u_2}_{simple} \Rightarrow_{\mathbb{R}[X]} V$ es un módulo semisimple de longitud 2.
Tomamos en V la $\mathbb{R}-$base dada por $\{\mu, Tu_1, u_2\}$. La matriz de T (por filas) respecto a dicha base es:

$$\begin{pmatrix} 0 & 1 & 0 \\ -|z|^2 & 2Re(z) & 0 \\ 0 & 0 & \alpha \end{pmatrix} \rightsquigarrow \text{ diagonlaización por bloques}$$

$T^2u_1 = (2Re(z)T - |z|^2)u_1, Tu_2 = \alpha u_2$.

- *Si $K = \mathbb{C} \Rightarrow \mu = (x-\alpha)(x-z)(x-\bar{z}), \alpha \in \mathbb{R}, z \in \mathbb{C} \setminus \mathbb{R}$.*
Llamamos $w_1 = (x-z)u_1 = (T-z)u_1 \Rightarrow ann_{\mathbb{C}[X]}(w_1) =< x - \bar{z} >$.
Seguimos sabiendo que ${}_{\mathbb{C}[X]}V = \mathbb{C}[X]u_1 \dot{+} \mathbb{C}[X]u_2$, pero ahora $\mathbb{C}[X]u_1$ puede descomponerse más.

Llamamos $w_2 = (x-\bar{z})u_1 = (T-\bar{z})u_1 \Rightarrow ann_{\mathbb{C}[X]}(w_2) =< x - z > \Rightarrow_{\mathbb{C}[X]} V = \mathbb{C}[X]w_1 \dot{+} \mathbb{C}[X]w_2 \dot{+} \mathbb{C}[X]u_2$, y como todos son de dimensión 1 $\Rightarrow$ no puede descomponerse más.

En la base $\{w_1, w_2, u_2\}$, la matriz de T es:

$$\begin{pmatrix} z & 0 & 0 \\ 0 & \bar{z} & 0 \\ 0 & 0 & \alpha \end{pmatrix} \rightsquigarrow \text{ ahora la diagonalización es completa}$$

En un momento dado hemos empleado que $carK \neq 2$. ¿Qué pasaría si fuese $carK = 2$?
Tendríamos:

$$B = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \Rightarrow X - B = \begin{pmatrix} x+1 & 1 & 1 \\ 1 & x+1 & 1 \\ 1 & 1 & x+1 \end{pmatrix}$$

Por filas, tenemos:

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

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

Por columnas, tenemos:

$$\begin{pmatrix} 1 & 1 & x+1 \\ 0 & x & x \\ 0 & 0 & x^2+x \end{pmatrix} c_2 \overset{\sim}{+} c_1 \begin{pmatrix} 1 & 0 & x+1 \\ 0 & x & x \\ 0 & 0 & x^2+x \end{pmatrix} \sim$$

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

Sólo las entradas de la diagonal que no son unidades de $K[X]$ producen sumandos en la descomposición de ${}_{K[X]}V$. En este caso, sólo tendremos 2 sumandos (correspondientes a x y a x^2+x) $\Rightarrow_{K[X]} V = K[X]x_2 + K[X]x_3$. Calculamos Q (sólo nos interesan las 2 últimas filas):

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & x+1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & x+1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = Q$$

$$\Rightarrow \begin{cases} ann_{K[X]}(x_2) =< x > \rightsquigarrow x_2 = v_2 + v_3 \\ ann_{K[X]}(x_3) =< x^2 + x > \rightsquigarrow x^3 = v_3 \end{cases}$$

Llamamos $y_1 = (x+1)x_3 = (T+1)x_3 \Rightarrow ann_{K[X]}(y_1) =< x >$.
Llamamos $y_2 = xx_3 = Tx_3 \Rightarrow ann_{K[X]}(y_2) =< x+1 >$.
$\Rightarrow_{K[X]} V = K[X]x_2 \dot{+} K[X]y_1 \dot{+} K[X]y_2$.
(recordando que $carK = 2$).

En la base $\{x_2, y_1, y_2\}$ la matriz de T es (por filas):

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

Esto es una ilustración básica de la teoría que sustenta las técnicas de diagonalización de endormorfismos. El procedimiento no tiene por qué ser el mejor (más rápido). Si por ejemplo sabemos que la matriz es diagonalizable, hay algoritmos más rápidos.

Proposición 7.36
Si A es un DE con función eucídea 0 y B es una matriz con coeficientes en A, existen P, Q invertibles (de tamaños adecuados) y D cuasi-diagonal tales que $PB = DQ$.

Demostración. Necesitamos demostrar que $PBQ^{-1} = D$.
Supongamos que $B \neq 0$ (en caso contrario, el resultado es trivial). Veamos que, mediante operaciones elementales por filas u columnas, podemos reducir B a una matriz del tipo

$$\begin{pmatrix} b & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & B' & \\ 0 & & & \end{pmatrix}$$

Llamamos $0(B) = \text{mín}(b_{ij} \mid b_{ij} \neq 0) \neq 0$ por ser $B \neq 0$. Intercambiando filas y columnas, colocamos $0(B)$ en la esquina superior izquierda. Tenemos dos casos:

- Si $b_{11} \mid b_{i1}$ y $b_{11} \mid b_{ij}, \forall i, j \Rightarrow$ hemos acabado (esto pasa siempre que b_{11} es una unidad).
- Si $b_{11} \nmid b_{i1}$(ó $b_{11} \nmid b_{1j}$) para algún i, j, consideramos $b_{i1} = qb_{11} + r$, con $0(r) < 0(b_{11})$.
  Haciendo operaciones por filas (columnas si $b_{11} \nmid b_{1j}$) hacemos que en la posición $(i, 1)$ haya un r. Colocamos r en la esquina superior izquierda. Reiterando, tenemos el resultado.

□

8. Módulos semisimples de cualquier longitud

Proposición 8.1
Sea $\{M_i : i \in I\}$ una familia no vacía de submódulos simples de un módulo M. Pongo $M' = \sum_{i\in I} M_i$, y tomo $N \subseteq M'$ un submódulo con $N \neq M'$.

Existe $J \subseteq I$ tal que $\{M_i : i \in J\}$ es independiente, $N \cap (\dot{+}_{i\in J} M_i) = \{0\}$ y $M' = N \dot{+} (\dot{+}_{i\in J} M_i)$.

Demostración. Sea Γ el conjunto de los subconjuntos J de I tales que $\{M_j : j \in J\}$ es independiente y $N \cap (\dot{+}_{j\in J} M_j) = \{0\}$.

Veamos que $\Gamma \neq \emptyset$.

1. Si $N = \{0\}$, tomo $i \in I$ cualquiera, y tengo que $\{i\} \in \Gamma$.
2. Si $N \neq \{0\}$, pero $N \cap M_i = \{0\}$ para algún i, entonces $\{i\} \in \Gamma$.
3. Si $N \neq \{0\}$ y $N \cap M_i \neq \{0\}, \forall i \in I$. Entonces, como cada M_i es simple, $N \cap M_i = M_i, \forall i \in I \Rightarrow N = M'$.

   Ordeno Γ por inclusión. Tomo una cadena χ en Γ. Pongo:

   $$J = \bigcup_{C\in\chi} C$$

   Quiero ver que $J \in \Gamma$. Veamos que $\{M_i : i \in J\}$ es independiente. Para ello, basta con comprobar que $\{M_i : i \in F\}$ es independiente para cualquier $F \subseteq J$ finito. Pero $\exists C \in \chi$ tal que $F \subseteq C$, y $C \in \Gamma$, luego $\{M_i : i \in C\}$ es independiente y, por tanto, $\{M_i : i \in F\}$ es independiente.

   Tomo $m \in N \cap (\dot{+}_{j\in J} M_j) \Rightarrow \exists F \subseteq J$ finito tal que $m \in N \cap (\dot{+}_{j\in F} M_j)$ $\Rightarrow \exists C \in \chi$ tal que $F \subseteq C \Rightarrow m \in N \cap (\dot{+}_{j\in C} M_j) = \{0\}$.

   El Lema de Zorn nos dice que $\exists J \in \Gamma$ maximal. Veamos que $M' = N \dot{+} (\dot{+}_{j\in J} M_j)$ (sólo queda ver eso).
   Para $i \notin J \Rightarrow M_i \cap (N + \dot{+}_{j\in J} M_j) \neq \{0\}$. De lo contrario, $J \cup \{i\} \in \Gamma$ y J no es maximal. Como M_i es simple $\Rightarrow M_i \subseteq (N + \dot{+}_{j\in J} M_j)$
   $\Rightarrow M_i \subseteq (N + \dot{+}_{j\in J} M_j), \forall i \in I \Rightarrow M' = N \dot{+} (\dot{+}_{j\in J} M_j)$.

□

Corolario 8.2
Sea D un anillo de división ($\forall d \in D, d \neq 0, \exists d^{-1} \in D$ tal que $dd^{-1} = d^{-1}d = 1$), y ${}_DV$ 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 ${}_DV$.

Demostración. Tomo la familia $\{Dv_i : i \in I\}$. Cada $Dv_i \cong \frac{D}{ann_D(v_i)} \cong$ $\cong_{ann_D(v_i)=\{0\}} .D$. $V = \sum_{i\in I} Dv_i$. Tomo $N = \{0\}$ en la proposición $\Rightarrow \exists J \subseteq I$ tal que $V = \dot{+}_{j\in J} Dv_j \Rightarrow \{v_j : j \in J\}$ es base de V. □

Observación: $V \cong D^{(J)}$.

Definición 8.3
Dados homomorfismos de módulos:

$$N \xrightarrow{g} M \xrightarrow{f} N$$

tales que $f_o g = id_N$, diré que f es un epimorfismo escindido (o roto) ("split" en inglés), y que g es un monomorfismo escindido (o roto).

Lema 8.4
Todo módulo f.g. no nulo contiene un submódulo propio maximal.

Demostración. Sea M el módulo. Sea Γ el conjunto de los submódulos propios de M, esto es,

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

pues $\{0\} \in \Gamma$.

Tomamos χ cadena en $\Gamma, N = \bigcap_{C\in\chi} C$.

Sean $m_1, \ldots, m_t$ generadores de M. Si $N = M \Rightarrow m_1, \ldots, m_t \in N \Rightarrow \exists c \in \chi$ tal que $m_1, \ldots, m_t \in C \Rightarrow M \subseteq C \subseteq M \Rightarrow M = C \Rightarrow C \notin \Gamma$.
Podemos aplicar Zorn $\Rightarrow \Gamma$ tiene elementos maximales. □

Observación: M f.g. $\Rightarrow \exists N \in \mathcal{L}(M) \mid \frac{M}{N}$ simple.

Teorema 8.5
Las siguientes condiciones son equivalentes para un módulo M:

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

Demostración. Si $M = \{0\}$ obvio. Supongamos $M \neq \{0\}$.

① $\Rightarrow$ ③ Sea $M \xrightarrow{\phi} N$ epimorfismo. Sea $L = ker\phi$. Por hipótesis $M = L \dotplus X$ para cierto $X \in \mathcal{L}(M)$. Tenemos $N \cong \frac{M}{L}$ por le primer teorema de isomorfia, luego

$$N \cong \frac{L \dotplus X}{L} \overset{2^o \text{ isomorfia}}{\cong} \frac{X}{L \cap X} \overset{M=L\dotplus X}{=} \frac{X}{\{0\}} \cong X$$

Consideramos entonces

$$\begin{array}{ccccc} X \cong & \dfrac{L \dotplus X}{L} & \cong & N \\ x \mapsto & x + L & \mapsto & \phi(x) \end{array}$$

$\Rightarrow \phi_{|X} : X \to N \Rightarrow (\phi_{|X})^{-1} : N \to X$ isomorfismo ($X \subseteq M$).

Considerando $\phi_o(\phi_{|X})^{-1} = id_N \Rightarrow \phi$ escindido.

③ $\Rightarrow$ ② Sea $\varphi : L \to M$ un monomorfismo. Tomamos la SEC

$$0 \to L \xrightarrow{\varphi} M \xrightarrow{K} C \to 0$$

con $C = \frac{M}{Im\varphi}$. Como K es epimorfismo $\overset{③}{\Rightarrow}$ K escinde, esto es, $\exists g : C \to M$ tal que $k_o g = id_C$. Definimos $h = id_M - g_o K : M \to M$. Entonces $K_o h = K - K_o g_o K = K - K = 0_M : M \to M$.
En consecuencia, $Imh \subseteq KerK \equiv Im\varphi \cong L$.
Tomamos entonces $f : M \to L \geq \varphi_o f = h$ (ejercicio).
En consecuencia, $\varphi_o f_o \varphi = h_o \varphi = \varphi - \underbrace{g_o K_o \varphi}_{=0} = \varphi$.
Como φ es inyectiva $\Rightarrow f_o \varphi = id_L \Rightarrow \varphi$ es escindido.

② $\Rightarrow$ ① Tomamos $X \in \mathcal{L}(M), X \subseteq M$ y la inclusión $i : X \hookrightarrow M$ es monomorfismo $\overset{②}{\Rightarrow} \exists p : M \to X \mid p_o i = p_{|X} = id_X \Rightarrow M = X \dotplus Kerp$ (ejercicio).

Nota: Ya tenemos ① $\iff$ ② $\iff$ ③ $\iff$ ①.

④ $\Rightarrow$ ⑤ Es evidente: tómese la familia de todos los submódulos simples de M.

⑤ $\Rightarrow$ ⑥ Consecuencia de una proposición anterior, con $N = \{0\}$.

⑥ $\Rightarrow$ ① Consecuencia de la proposición anterior, con $N \neq \{0\}$.

① $\Rightarrow$ ④ Emplearemos el lema. Por hipótesis, $M = Soc(M) \dotplus X$ para cierto $X \in \mathcal{L}(M)$. Veamos que $X = \{0\}$.

Si fuese $X \neq \{0\}$, tomamos $0 \neq m \in X$. Por el lema, tenemos que hay un epimorfismo $Rm \xrightarrow{p} S$ para S simple. Como $Rm \in \mathcal{L}(M) \Rightarrow M = Rm \dotplus Y$ (es sumando directo) $\Rightarrow$ existe un epimorfismo $M \overset{\pi}{\to} Rm$.

Consideramos el homorfismo $p_o\pi : m \to S$ sobreyectivo $\Rightarrow$
$\Rightarrow \exists \sim: S \to M \mid p_o\pi_o i = id_S$ ($p_o\pi$ es escindido.

De este modo, $S \overset{p \text{ sobreyectiva}}{\cong} Im(\pi_o i) \subseteq Rm \subseteq\Rightarrow X$ contiene a $Im(\pi_o i)$, que es simple, pero $Soc(M)$ contiene a todos los simple $\Rightarrow$ no puede ser $M = Soc(M) \dot{+} X$ (contradicción).

□

Definición 8.6
Si M verifica cualquiera de las condiciones anteriores, se dice que M es semisimple.

Nota: Todos los espacios vectoriales son semisimples $\Rightarrow$ todo subespacio vectorial es sumando directo.

Podemos preguntarnos para qué anillos se tiene que todos los módulos son semisimples.

Corolario 8.7
Todo cociente y todo submódulo de un módulo semisimple es semisimple.

Demostración. Sea M semisimple, $N \in \mathcal{L}(M)$ y consideramos $\frac{M}{N}$. Como M semisimple $\Rightarrow M$ es suma de módulos simples.

$$M = \sum_{i \in I} S_i \text{ con } S_i \text{ simple}$$

Consideramos la proyección canónica, $M \xrightarrow{p} \frac{M}{N}, m \mapsto m + N$ y tenemos que $\frac{M}{N} = \sum_{i \in I} p(S_i)$.

Para cada $i \in I$, se tiene o bien $p(S_i) = \{0\}$, o bien $p(S_i) \neq \{0\}$. Eliminamos de la suma los índices $i \in I$ tales que $p(S_i) = \{0\}$. Entonces los restantes sumandos son simples (pues $S_i \xrightarrow{p} p(S_i)$ es un isomorfismo) $\Rightarrow \frac{M}{N}$ es suma de simples $\Rightarrow \frac{M}{N}$ semisimple. Veamos ahora que N es semisimple. Como M semisimple, tenemos que $M = N \dot{+} X$. Consideramos $M = N \dot{+} X \xrightarrow{\pi} N, n + x \mapsto n \Rightarrow \pi$ epimorfismo $\Rightarrow N \cong \frac{M}{Ker\pi}$, que es un cociente de $M \Rightarrow N$ semisimple. □

Corolario 8.8
M es un módulo semisimple finitamente generado $\iff M = S_1 \dot{+} \cdots \dot{+} S_n$, con S_i simple.

Demostración. $\Leftarrow$ Teorema.

$\circledRightarrow$ $M = \dot{+}_{i\in I} S_i$, con S_i simple. Tenemos que ver que I es finito. Tomamos $m_1, \ldots, m_t$ conjunto de generadores de $M \Rightarrow m_j \in \dot{+}_{\text{finita}} S_i, \forall j \in \{1, \ldots, t\} \Rightarrow$ $M \subseteq \dot{+}_{\text{finita}} S_i \subseteq M \Rightarrow M = \dot{+}_{\text{finita}} S_i$. $\square$

9. Anillos semisimples

Definición 9.1
Un anillo R es semisimple si todo $R-$módulo es semisimple.

Ejemplo 9.2
Todo anillo de división es semisimple (hay muchos anillos de división).

Teorema 9.3
R es semisimple $\iff$ ${}_RR$ es semisimple.

Demostración. $\circledRightarrow$ Se sigue de la definición. $\circledLeftarrow$ Sea ${}_RR$ módulo. Escribimos $M = \sum_{m \in M} Rm$. Veremos que cada sumando no nulo es semisimple $\overset{\text{teorema}}{\Rightarrow}$ cada sumando es suma de simples $\Rightarrow$ M es suma de semisimples $\overset{\text{teorema}}{\Rightarrow}$ M es semisimple. Tenemos que $Rm \cong \frac{R}{ann_R(m)}$ que es un cociente $\Rightarrow$ Rm semisimple. $\square$

Nota: Esta es otra forma de ver que todo anillo de división es semisimple, pues ${}_RR$ es simple, y por tanto semisimple.

Definición 9.4
Sea ${}_RM$. Definimos:

$$End_R(M) = \{f : M \to M \mid f \text{ homomorfismo de } R-\text{módulos}\} \subseteq End(M)$$

Puede verse que $End_R(M)$ es subanillo de $End(M)$.

Llamo $S = End_R(M)$. Tenemos $i : S \hookrightarrow End(M)$ homomorfismo de anillos $\Rightarrow$ M es también un $S-$módulo.

Se llama a $End_R(M)$ "anillo de endomorfismos de M".

Nota: Nosotros hablamos de módulos, y no de módulos "a izquierda" o "a derecha".

Como el homomorfismo es la inclusión, si $f \in S, m \in M \Rightarrow fm = f(m)$.
Nos preguntamos ahora quién es $End_S(M) = End_{End_R(M)}(M)$.
Obviamente, $End_S(M) \subseteq End(M)$ subanillo.
Dado $g \in End(M)$

$$g \in End_S(M) \iff g(fm) = fg(m), \forall f \in S, m \in M \iff$$

Los "escalares" (que ahora son endomorfismos $f \in End_R(M)$) salen fuera.

$$\iff g(f(m)) = f(g(m)), \forall f \in End_R(M), \forall m \in M \iff$$

$$\iff f_o g = g_o f, \forall f \in S \Rightarrow$$

$$\Rightarrow End_S(M) = \{g \in End(M) \mid g_o f = f_o g, \forall f \in End_R(M)\} \subseteq End(M)$$

Esto se suele llamara "centralizador de $End_R(M)$".

Lema 9.5
$R \xrightarrow{\lambda} End_S(M)$ dado por $\lambda(r) : M \to M, m \mapsto rm, \forall r \in R$ es un homormofismo de anillos.

Demostración.

$$\begin{array}{lll} R \xrightarrow{\lambda} & End(M) & \\ r \mapsto & \lambda(r) : M \to M & \text{homomorfismo de anillos} \\ & m \mapsto rm & \end{array}$$

Basta probar que $Im(\lambda) \subseteq End_S(M)$, esto es, que $\forall r \in R$ se tiene $\lambda(r)_o f = f_o \lambda(r), \forall f \in End_R(M)$, lo cual es cierto pues

$$(\lambda(r)_o f)(m) = \lambda(r)(fm) = r(fm) \overset{f \in End_R(M)}{=}$$

$$= f(rm) = f(\lambda(r)(m)) = (f_o \lambda(r))(m) \Rightarrow$$

$$\Rightarrow \lambda(r)_o f = f_o \lambda(r)$$

Se suele llamar también anillo de biendomorfismos.

Denotamos $T = End_S(M)$. Podríamos considerar $End_T(M)$ pero hay un teorema que dice que en algún momento volvemos al inicio (como $E \to E^* \to E^{**} \cong E \dots$) □

Proposición 9.6
Los $R-$ sumandos directos de M son los mismos que los $T-$sumandos directos de M. Como consecuencia, si ${}_RM$ es semisimple $\Rightarrow {}_TM$ es semisimple.

Demostración. Tenemos el homomorfismo de anillos $\lambda : R \to T$. Si N es un $T-$sumando directo de $M \Rightarrow M = N \dot{+} X$, con $X \in \mathcal{L}({}_TM) \Rightarrow M = N \dot{+} X$, con $X \in \mathcal{L}({}_RM)$.

Recíprocamente, si tenemos ${}_RM = X \dot{+} Y, X, Y \in \mathcal{L}({}_RM)$, debemos demostrar que $X, Y \in \mathcal{L}({}_TM)$. Basta probarlo para uno de ellos, por ejemplo, X. Tomamos $p : M \to M, x + y \mapsto x$ y vemos que $p \in S = End_R(M)$.

Además, $X = Imp$. Tomamos $g \in T$ y tenemos que, $\forall x \in X$

$$g(x) = gx = g(p(x)) = (g_o p)(x) = (p_o g)(x) = p(g(x)) \in X$$

$\Rightarrow gx \in X, \forall x \in X \Rightarrow X$ es un $T-$submódulo de M. □

Observación: Como consecuencia de esta proposición:

$${}_RM \text{ semisimple} \iff {}_tM \text{ semisimple}$$

Sea $N \in \mathcal{L}({}_TM)$. Entonces $N \in \mathcal{L}({}_RM)$ (restricción escalares) $\Rightarrow$ N es $R-$sumando directo de $M \Rightarrow N$ es $T-$sumando directo de $M \Rightarrow_T M$ es semisimple.

El recíproco no puede demostrar así porque la restricción de escalares "solo va en un sentido".

Ejercicio 9.7
Demostrar que $S = End_T(M)$, donde $T = End_S(M), S = End_R(M)$.

Corolario 9.8
Si ${}_RM$ es semisimple, $l({}_RM) < \infty \Rightarrow_T M$ es semisimple y $l({}_TM) = l({}_RM)$.

Demostración. Que ${}_TM$ es semisimple ya lo sabemos.

Si ${}_RM = S_1 \dot{+} \cdots \dot{+} S_n$ con S_i $R-$submódulos simples $\Rightarrow$ Si es un $T-$submódulo de M para todo i, y S_i es $T-$simple, pues al ser T semisimple, si no fuese S_i simple $\Rightarrow S_i = X \dot{+} Y \Rightarrow S_i = X \dot{+} Y$ como $R-$módulo, lo cuál no es posible.

Dado un $R-$módulo ${}_RM$ y $n \in \mathbb{N}$, podemos considerar ${}_RM^n = M \oplus M \oplus \overset{(n)}{\dots} \oplus M$.
Teníamos $S = End_R(M)$ y consideramos $S' = End_R(M^n)$.
Tomamos, para cada $i \in \{1, \dots, n\}$ un homomorfismo de $R-$módulos dado por $L_i : M \to M^n, m \mapsto (0, 0, \dots, 0, \overset{(i)}{m}, 0, \dots, 0)$.
Recíprocamente, las proyecciones $\pi_j : M^n \to M, (m_i) \mapsto m_j$ homomorfismos de $R-$módulo.

Es claro entonces que $id_{M^n} = \sum_{i=1}^n L_i\pi_i \in S'$, pues $\forall i, L_i\pi_i \in S'$. Dado ahora $f \in T = End_S(M)$, definimos $\bar{f} = \sum_{i=1} nL_if\pi_i \in End(M^n)$.
Claramente, $\bar{f}(m_1, \dots, m_n) = (f(m_1), \dots, f(m_n))$.

Tomando $g \in S'$, tenemos

$$g\bar{f} = \sum_{i,j=1}^{n} L_i\pi_i g L_j f \pi_j \overset{\bigstar}{=} \sum_{i,j=1}^{n} L_i f \pi_i g L_j \pi_j$$

$\Rightarrow g$ conmuta con $\bar{f} \Rightarrow \bar{f} \in End_{S'}(M)$.

$\bigstar L_i, \pi_i \in S, f \in T, g \in S' \Rightarrow f$ conmuta con todos. $\square$

Teorema 9.9 (de densidad de Jacobson)
Sea ${}_RM$ semisimple, y $m_1, \dots, m_n \in M$. Para cada $f \in End_S(M)$ existe $r \in R$ tal que $f(m_i) = rm_i, \forall i \in \{1, \dots, n\}$.

Demostración. $m = (m_1, \dots, m_n) \in M^n$.
Sabemos que M^n es $R-$semisimple, luego Rm es un $R-$sumando directo de

$M^n \Rightarrow Rm$ es un $S-$sumando directo de M^n y, en particular, Rm es un $End_{S'}(M^n)-$submódulo de M^n.

Como $\bar{f} \in End_{S'}(M^n) \Rightarrow \bar{f}m \in Rm \Rightarrow (f(m_1), \ldots, f(m_n)) \in Rm \Rightarrow$
$\Rightarrow \exists r \in R \mid (f(m_1), \ldots, f(m_n)) = rm.$ □

Lema 9.10 (de Schur)
Si ${}_RN$ es simple y $f : M \to N$ es un $R-$homomorfiosmo

$$\Rightarrow \begin{cases} f = 0 \\ ó \\ f \text{ es ismomorfismo} \end{cases}$$

$\Rightarrow End_R(M)$ *es anillo de división.*

Básicamente dice que el anillo de endomorfismos de un módulo simple es un anillo de división.

Demostración. Si $f \neq 0 \Rightarrow Imf$ $R-$submódulo de $N \Rightarrow Imf = N$ (pues no puede ser $Imf = \{0\}$) $\Rightarrow Kerf \in \{M, \{0\}\}$ y no puede ser $Kerf = \{M\} \Rightarrow$ $Kerf = \{0\} \Rightarrow f$ isomorfismo. □

Proposición 9.11
${}_RM$ simple fiel. Suponemos que ${}_RR$ artiniano. Sea $D = End_R(M)$. Entonces ${}_DM$ es un D-e.v. de dimensión finita y:

$$\lambda : R \to End_D(M)$$

es un isomorfismo de anillos.

Demostración. Supongamos que ${}_DM$ no fuera de dimensión finita $\Rightarrow M$ admite una base B infinita. Tomo $\{x_i : i \in \mathbb{N}\} \subseteq B$ linealmente independiente.

Dado $i \in \mathbb{N}$, tomo $f_i : M \to M$ la aplicación $D-$lineal que vale 0 sobre todo elemento de B y $f_i(x_i) = x_i$.

Cada $f_i \in End_D(M)$. Teorema de densidad, $\exists r_i \in R$ tal que:

$$f_i(x_j) = r_i x_j \qquad \text{para } j \in \{0, \ldots, i\}$$

$r_i \in ann_R(x_0) \cap \cdots \cap ann_R(x_{i-1})$, pero $r_i \notin ann_R(x_0) \cap \cdots \cap ann_R(x_{i-1}) \cap$ $ann_R(x_i) \Rightarrow ann_R(x_0) \cap \cdots \cap ann_R(x_{i-1}) \supsetneq ann_R(x_0) \cap \cdots \cap ann_R(x_i) \Rightarrow_R R$ no es artinitano.

Tomo $\{m_1, \ldots, m_n\} D-$base de M. Dado $f \in End_D(M)$, el teorema de densidad nos dice que $\exists r \in R$ tal que $f(m_i) = rm_i, \forall i \in \{1, \ldots, n\} \Rightarrow f =$ $\lambda(r) \Rightarrow \lambda$ es sobreyectivo $\Rightarrow \lambda$ isomorfismo. □

Definición 9.12
Un elemento $e \in R$ se dice idempotente si $e^2 = e$.

Un conjunto $e_1, \ldots, e_n \in R$ de idempotentes se dice un conjunto completo de idempotentes ortogonales (CCIO) si:

1. *$e_i e_j = 0$ para $i \neq j$.*
2. *$1 = e_1 + \cdots + e_n$.*

Si $\{e_i, \ldots, e_n\}$ CCIO de $R \Rightarrow R = Re_1 \dot{+} \cdots \dot{+} Re_n$. En efecto, $r \in R \Rightarrow r = r \cdot 1 = re_1 + \cdots + re_n \Rightarrow R = Re_1 + \cdots + Re_n$.

Además, si $0 = r_1 e_1 + \cdots + r_n e_n$, para $r_i \in R \Rightarrow 0 = r_i e_i$ (multiplicando por e_i) para cada $i \in \{i, \ldots, n\}$

Teorema 9.13
Para un anillo no trivial son equivalentes:

1. *${}_R R$ semisimple y todos los $R-$módulos simples son isomorfos entre sí.*
2. *R es isomorfo, como anillo, a $End_D(M)$ con D de división y ${}_D M$ de dimensión finita.*
3. *${}_R R$ artiniano y existe un $R-$módulo simple fiel.*
4. *${}_R R$ artiniano y los únicos ideales de R son $\{0\}$ y R (un anillo que cumple esto es un anillo simple).*

Además, por 2., necesariamente, $D \cong End_R(\Sigma)$, para ${}_R\Sigma$ cualquier simple y $dim_D(M) = l({}_R R)$.

Demostración.

1. $\Rightarrow$ 4. Sabemos que ${}_R R$ tiene longitud finita. Sea I un ideal de R propio ($I \neq R$), y vamos a ver que $I = \{0\}$. $\frac{R}{I}$ es seimisimple como $R-$módulo. Como es finitamente generado $\Rightarrow \frac{R}{I}$ = suma directa finita de simples $\Rightarrow \frac{R}{I} \overset{R-\text{módulo}}{\cong} \Sigma^n$, para ${}_R\Sigma$ simple.

   Como I es ideal (no sólo a la izquierda), $I = Ann_R(\frac{R}{I}) = Ann_R(\Sigma^n) = Ann_R(\Sigma)$.

   $R \cong \Sigma^m, m = l({}_R R)$. Entonces $I = Ann_R(\Sigma) = Ann_R(\Sigma^m) =$
   $= Ann_R(R) = \{0\}$.

4. $\Rightarrow$ 3. Tomo ${}_R\Sigma$ simple. $R \neq Ann_R(\Sigma) \Rightarrow Ann_R(\Sigma) = \{0\} \Rightarrow_R \Sigma$ fiel.

3. $\Rightarrow$ 2. Proposición previa.

4. $\Rightarrow$ 1. Tomo $S = End_D(M)$. Si $m, m' \in M$ con $m \neq 0 \Rightarrow \exists f \in S$ tal que $f(m) = m'$. Así, $Sm = M \Rightarrow_S M$ simple.

Sea $\{m_1, \ldots, m_n\}D-$ base de M. Para $i \in \{i, \ldots, n\}$, defino $e_i \in S$ tal que $e_i(m_j) = \begin{cases} 0 & \text{si } j \neq i \\ m_i & \text{si } j = i \end{cases}$
$\{e_1, \ldots, e_n\}$ es CCIO de $S \Rightarrow S = Se_1 \dot{+} \cdots \dot{+} Se_n$.

Veamos que Se_i es simple. Basta con demostrar que, si $f \in S$ tal que $fe_i \neq 0 \Rightarrow Sfe_i = Se_i$.
$fe_i = f(e_i) = \sum_{j=1}^{n} a_j m_j, a_j \in D$. Tomo $k \in \{1, \ldots, k\}$ tal que $a_k \neq 0$ (tiene que haber alguno porque si no $f(e_i)$ sería 0) y defino $s : M \to M$ tal que $s(m_r) = a_k^{-1} m_i$ y $s(m_j) = 0$ si $j \neq k$.

$$sfe_i(m_i) = s(\sum_j a_j m_j) = a_k^{-1} a_k m_i = m_i$$

Entonces, $sfe_i = e_i \Rightarrow Se_i = Sfe_i$. Por tanto, ${}_SS$ semisimple.

Construimos la aplicación $Se_i \xrightarrow{F} M, f \mapsto f(m_i) = fm_i$ no nula.
Es fácil ver que F es un homomorfismo de $S-$módulos. Además, F no es nula pues $F(e_i) = e_i(m_i) = m_i \neq 0$ (pues m_i son los elementos de una base $\underset{Schur}{\Rightarrow} F \neq 0 Rightarrow F$ isomorfismo. En particular, todos los Se_i son isomorfos entre sí.

Si ${}_s\Sigma$ es simple $\Rightarrow \exists p : S \to \Sigma$ epimorfismo de $S-$módulos (teorema isomorfismo).
En consecuencia, p no se anula en todos los Se_i, esto es, $\exists i \in \{1, \ldots, n\}$ tal que $p_{|Se_i} \neq 0 \overset{Schur}{\Rightarrow} p_{|Se_i}$ isomorfismo.

Tomamos ahora $\phi : S \to R$ isomorfismo de anillos y consideramos $\{\phi(e_1, \ldots, \phi(e_n)\}$, que es un CCIO de $R \Rightarrow R = R\phi(e_1) \dot{+} \cdots \dot{+} R\phi(e_n)$.

Veamos que cada $R\phi(e_i)$ es simple (como $R-$módulo): se comprueba (mediante restricción de escalares con ϕ y ϕ^{-1}) que $\mathcal{L}({}_SX) = \mathcal{L}({}_RX)$. En consecuencia, ${}_RM$ es simple (pues lo es ${}_SM$). Vamos a comparar $\mathcal{L}(R\phi(e_i))$ con $\mathcal{L}(Se_i)$: Como ϕ isomorfismo, tenemos:

$$\begin{array}{rl} \phi(I) \to & I \\ J \leftarrow & \phi^{-1}(J) \end{array}$$

con I, J ideales, y esta aplicación es biyectiva.

En consecuencia, cada $R\phi(e_i)$ es simple como $R-$módulo y, por tanto, ${}_RR$ es semisimple.
Además, tenemos que $dim_D(M) = n = l({}_SS) = l({}_RR)$.

Sólo nos queda ver que todos los $R-$módulos simples son isomorfos entre si, y que $D \cong End_R(\Sigma)$.
Sea ${}_R\Sigma$ simple $\overset{\phi}{\Rightarrow}{}_S \Sigma$ simple $\Rightarrow {}_S \Sigma \cong_S M \overset{\phi^{-1}}{\Rightarrow}{}_R \Sigma \cong_R M$.

Por último, veamos que $D \cong End_R(\Sigma)$: por el teorema de densidad, tenemos un isomorfismo $D \xrightarrow[\cong]{\lambda} End_S(M) = End_R(M)$.

Este resultado nos va a servir para clasificar, salvo isomorfismos, todos los anillos semisimples. □

10. Componentes homogéneas

Lema 10.1
Sea R un anillo. Existe un conjunto Ω_R de $R-$módulos simples, no isomorfos entre si, tal que cualquier $R-$módulo simple es isomorfo a uno (y sólo a uno) de los de Ω_R.

Ω_R puede ser finito o infinito. Se suele llamar a Ω_R conjunto de representantes de los tipos de $R-$módulos simples.

Podríamos decir "basta con tomar Ω_R el conjunto de todos los $R-$módulos simples y quitar los isomorfos", pero si tomamos todos los $R-$módulos simples, el resultado no tiene por qué ser un conjunto (paradojas teorías conjuntos).

Demostración. Sea ${}_R\Sigma$ simple. Tomamos $s \in \Sigma$ con $s \neq 0$ y tenemos ${}_R\sigma \cong \frac{R}{ann_R(s)}$. Tomamos Σ_R un conjunto de representantes de los $R-$módulos $\frac{R}{I}$ para I ideal, representante maximal bajo la relación de equivalencia $I \sim J \iff \frac{R}{I} \cong \frac{R}{J}$.

Esto si es un conjunto, pues el cardinal debe al ser menor o igual que el conjunto de ideales de R. □

Proposición 10.2
${}_RM$ módulo. Para $\Sigma \in \Omega_R$ definimos $Soc_\Sigma(M)$ como la suma de todos los submódulos simples de M isomorfos a Σ

$$\Rightarrow Soc(M) = \dot{+}_{\Sigma \in \Omega_R} Soc_\Sigma(M)$$

El lema anterior era para poder decir "$\Sigma \in \Omega_R$" y hacer de suma.

Demostración. Sabemos que $Soc(M) = \sum_{\Sigma \in \Omega_R} Soc_\Sigma(M)$. Llamamos $N = Soc_{\Sigma'}(M) \cap \sum \Sigma \neq \Sigma' Soc_\Sigma(M)$, para $\Sigma' \in \Omega_R$ fijo.

Tomamos, suponiendo $N \neq \{0\}, m \in N$, con $m \neq 0$. Entones Rm es semisimple y finitamente generado $\Rightarrow Rm$ es de longitud finita $\Rightarrow$ existe un $R-$submódulo simple S de Rm.

Tenemos que $S \subseteq Soc_{\Sigma'}(M) \Rightarrow$ escinde: $\exists g : Soc_{\Sigma'}(M) \to S$ epimorfismo. Entonces $\exists S' \subseteq Soc_{\Sigma'}(M)$ con $S' \cong \Sigma'$ tal que $g_{|_{S'}} \neq 0 \overset{Schur}{\Rightarrow} \Sigma' \cong S' \cong S$.

Análogamente, $\exists S'' \cong \Sigma \neq \Sigma'$ tal que $S'' \cong S$ (mismo argumento) $\Rightarrow \Sigma' \cong S \cong \Sigma$.

Pero habíamos tomado $\Sigma \neq \Sigma'$ y en Ω_R sólo hay un ejemplar (representante) salvo isomorfismo $\Rightarrow$ absurdo, luego $N = \{0\}$, y la suma es directa. □

Nota: A los $Soc_\Sigma(M)$ e le llama "componentes homogéneas" del zócalo $Soc(M)$.

Observación: Sea $f \in End_R(M)$. Se tiene entonces:

$$f(Soc_\Sigma(M)) = f(\sum_{\substack{S\cong\Sigma \\ S\in\mathcal{L}(M)}} S) = \sum_{\substack{S\cong\Sigma \\ S\in\mathcal{L}(M)}} f(S)$$

Por el lema de Schur, cada sumando o bien es 0, o bien es isomorfo a Σ, luego $f(Soc_\Sigma(M)) \subseteq Soc_\Sigma(M)$. En otras palabras, $Soc_\Sigma(M)$ es invariante bajo todas las $f \in End_R(M)$.

Si $M = R$ y tomamos $f = \rho_r$ con $r \in R$ dada por $\rho_r : R \to R, r' \mapsto r'r \Rightarrow \rho_r(Soc_\Sigma(R)) \subseteq Soc_\Sigma(R) \Rightarrow Soc_\Sigma(R)$ es un ideal de $R \Rightarrow Soc(R)$ es un ideal de R.

Nota: Puede darse que el zócalo sea el 0 o el total.

Teorema 10.3
Sea R un anillo semisimple. Entonces Ω_R es finito.

Eso no es cierto si R no es semisimple. Basta tomar $R = \mathbb{Z}$ y $\Omega_\mathbb{Z}$ es infinito (hay un simple por cada primo).

Llamamos $\Omega_R = \{\Sigma_1, \dots, \Sigma_t\}$ y $D_i = End_R(\Sigma_i)$ (lo llamamos D_i porque, por Schur, es un anillo de división).
Entonces $R \cong End_{D_1}(\Sigma_1) \times \cdots \times End_{D_t}(\Sigma_t)$, y $dim_{D_i}(\Sigma_i) < \infty$.

Demostración. Ya sabemos que ${}_RR = S_1 \dotplus \cdots \dotplus S_n$, con ${}_RS_i$ simple.
Así, si ${}_R\Sigma$ es simple, tenemos un epimorfismo $R \xrightarrow{p} \Sigma \Rightarrow p_{|_{\S_i}} : S_i \to \Sigma$ es no nulo para algún $i \in \{1, \dots, n\} \overset{Schur}{\Rightarrow} S_i \cong \Sigma \Rightarrow \Omega_R$ es finito.

Si I, J ideales, se define $IJ = \{\sum_i x_i y_i \mid x_i \in I, y_i \in J\}$, que vuelve a ser un ideal y $IJ \subset I \cap J$.

Consideramos $Soc_{\Sigma_i}(R)Soc_{\Sigma_j}(R) \subseteq Soc_{\Sigma_i}(R) \cap Soc_{\Sigma_j}(R) = \{0\}$
$(i \neq j) \Rightarrow Soc_{\Sigma_i}(R) \overset{\bigstar}{\subseteq} Ann_R(\Sigma_j), \forall i \neq j.$

$\bigstar$ Se tiene que $Ann_R(\Sigma_j) = Ann_R(Soc_{\Sigma_j}(R))$. La inclusión $\supseteq$ es clara, y la otra (*subseteq*) se comprueba facilmente.

Queremos utilizar el Teorema Chino del Resto. Llamamos $I_i = \sum_{j\neq i} Soc_{\Sigma_j}(R)$, que es un ideal, $\forall i$.
Se tiene claramente que $I_i + I_j = R, \forall i \neq j$.
En consecuencia, $Ann_R(\Sigma_i) + Ann_R(\Sigma_j) = R, \forall i \neq j$.

Definimos $R \to \frac{R}{Ann_R(\Sigma_1)} \times \cdots \times \frac{R}{Ann_R(\Sigma_t)}, r \mapsto (r + Ann_R(\Sigma_1), \dots, r + Ann_R(\Sigma_t))$, que es un homomorfismo sobreyectivo. El núcleo es $Ann_R(\Sigma_1) \cap$

$\cdots \cap Ann_R(\Sigma_t) = \{0\}$ (pues $Ann_R(R) = \{0\} = Ann_R(S_1) \cap \cdots \cap Ann_R(S_n)$ y los Σ_i son isomorfos a los S_j, a lo sumo "hay $\Sigma_j' s$ repeditos") $\Rightarrow$ es un isomorfismo.

Consideramos $\frac{R}{Ann_R(\Sigma_i)}$, que es artiniano $\forall i$, y además, Σ_i es un $\frac{R}{Ann_R(\Sigma_i)}-$módulo simple fiel $\overset{\bigstar}{\Rightarrow} \frac{R}{Ann_R(\Sigma_i)} \cong End_{D_i}(\Sigma_i)$, para $D_i = End_{\frac{R}{Ann_R(\Sigma_i)}}(\Sigma_i) = End_R(\Sigma_i)$.

$\bigstar$ Teorema sobre módulos artinianos.

Nota: Podemos preguntarnos si el número t es el mismo independientemente de los representantes Σ_i escogidos. La respuesta es sí, pues es el número de tipos de isomorfía (el cardinal de Ω_R).

Nota: ¿Se pueden poner otros D_i' y Σ_i'? Sí, pero los D_i' tiene que ser isomorfos a los D_i originales y los Σ_i' tienen que tener las mismas dimensiones que los Σ_i. $\square$

Ejemplo 10.4
R, S anillos. Consideramos $T = R \times S$ y la aplicación $\pi : R \times S \to R, (r, s) \mapsto r$. Llamando $e = (1, 0) \in T$, consideramos la aplicación:

$$\begin{array}{rl} \mathcal{L}({}_T Te) \overset{\hat{\pi}}{\to} & \mathcal{L}({}_R R) \\ I \mapsto & \pi(I) \end{array}$$

Demostrar que $\hat{\pi}$ es una biyección que preserva la inclusión.

Como consecuencia, ${}_T Te$ es semisimple $\iff$ ${}_R R$ es semisimple.

Análogamente sucede con S, luego se tiene

$$ {}_T T \text{ es semisimple} \iff {}_R R \text{ y } {}_S S \text{ son semisimples}$$

(${}_T T = Te \dotplus T(1-e) \rightsquigarrow e$ es idempotente).

Ejercicio 10.5
D, E anillos de división, ${}_D M_E$, N espacio vectorial. Demostrar que

$$End_D(M) \cong End_E(N) \iff \begin{cases} D \cong E \\ dim_D(M) = dim_E(N) \end{cases}$$

Definición 10.6
R anillo, $Z(R) = \{r \in R \mid rs = sr, \forall s \in R\}$ es un subanillo conmutativo de R, que se llama centro de R.

Si $e \in Z(R)$ verifica $e^2 = e$, diremos que e es un idempotente central de R.

Si e es un ideal central, Re es un ideal de R.

Además, Re es un anillo con la suma y el producto "heredados" de R cuyo 1 es e.

Ejemplo 10.7
Dados R_1, R_2 anillos, $R = R_1 \times R_2, e = (1,0) \Rightarrow Re = R_1 \times \{0\}$ es un anillo isomorfo a R_1.

e idempotente central.

Observación: e idempotente central de $R \Rightarrow 1-e$ es idempotente central.

$\{e, 1-e\}$ CCIO (conjunto completo de idempotentes ortogonales) centrales.

$$R = Re \dotplus R(1-e) \cong Re \times R(1-e)$$

Al revés, si $R = I \dotplus J$ con I, J ideales $\Rightarrow 1 = e + (1-e), e \in I, 1-e \in J$.
$e, 1-e$ central, $I = Re, J = R(1-e)$.

Ejemplo 10.8
$R = \begin{pmatrix} k & k \\ k & k \end{pmatrix} = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in K\}, K$ *cuerpo,* $e = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ *es idempotente no central.*

$$Re = \begin{pmatrix} k & 0 \\ k & 0 \end{pmatrix} = \{\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} : a,b \in K\}, eR = \begin{pmatrix} k & k \\ 0 & 0 \end{pmatrix}$$

e NO central.

Definición 10.9
Un ideal I de R se dice indescomponible si $I = I_1 \dotplus I_2$, con I_1, I_2 ideales $\Rightarrow I_1 = \{0\}$ ó $I_2 = \{0\}$.

R indescomponible si lo es como ideal.

Con idempotentes: e idempotente central de R. e indescomponible si Re es indescomponible, equivalentemente, si $e = e' + e''$, e', e'' idempotentes centrales y ortogonales ($e'e'' = 0$), entonces $e' = 0$ ó $e'' = 0$.

$$e = e' + e''$$
$$e^2 = e'^2 + e''^2 + 2e'e'' = e' + e'' + 2e'e'' = e + 2e'e'' \Rightarrow e'e'' = 0$$

Ejercicio 10.10
R indescompible $\iff$ no es isomorfo a ningún anillo de la forma $R_1 \times R_2$ con R_1, R_2 anillos no triviales.

Proposición 10.11
Si un anillo tienen un CCIO centrales indescomponibles, entonces este es único. Si $l({}_R R) < \infty$, entonces R admite un CCIO centrales indescomponibles.

Demostración. Sean $\{e_1, \dots, e_n\}, \{f_1, \dots, f_m\}$ CCIO centrales indescomponibles. Vamos a ver que ambos conjuntos son iguales por doble inclusión.

$e_i f_j$ es un idempotente central.

$$(e_i f_j)^2 = e_i f_j e_i f_j = e_i e_i f_j f_j = e_i^2 f_j^2 = e_i f_j$$

$e_i = e_i f_j + e_i(1 - f_j)$, donde $e_1 f_j$ y $e_i(1 - f_j)$ son idempotentes centrales, y además son ortogonales.

$\Rightarrow$ como e_i es indesomponible, uno de los dos es 0.

$$\Rightarrow \begin{cases} e_i f_j = 0 \\ \text{ó} \\ e_i(1 - f_j) = 0 \end{cases}$$

Si $e_i f_j \neq 0 \Rightarrow e_i = e_i f_j$.

Análogamente, tenemos $f_j = e_i f_j$.
$\Rightarrow e_i = e_i f_j = f_j$.

Dado $e_i, 0 \neq e_i = e_i 1 = e_i(f_1 + \cdots + f_m) = e_i f_1 + \cdots + e_i f_m \Rightarrow e_i f_j \neq 0$ para algún $j \Rightarrow e_i = f_j$.

Para la segunda parte, hacemos inducción sobre $l({}_R R)$:
Si R es indescomponible $\Rightarrow$ no hay nada que demostrar.
Si no, $R = Re + R(1 - e), 0 \neq e \neq 1$ idempotente central.

$$l({}_{Re} Re) < l({}_R R) \Rightarrow \text{ aplico inducción}$$

□

[...] $\rightarrow$ 03 y 04/05/2022

Definición 10.12 (Funciones sobre un grupo)
$\mathbb{C}$ *cuerpo de los* n^o *complejos.*
G *grupo con elemento neutro* e.
$\mathbb{C}G$ $\mathbb{C}-$*espacio vectorial con base* G.

$$\mathbb{C}G \times \mathbb{C}G \xrightarrow{\mu} \mathbb{C}G$$

aplicación bilineal determinada por $\mu(g, h) = g \cdot h, \forall (g, h) \in G \times G$ *(*$\cdot$ *multiplicación de* G*).*

Si para $r, s \in \mathbb{C}G$ *denoto* $rs = \mu(r, s)$, *tengo* $r = \sum_{g \in G} r_g g, s = \sum_{g \in G} s_g g; r_g, s_g \in \mathbb{C}$.

$$rs = \mu(r, s) = \mu(\sum_{g \in G} r_g g, \sum_{h \in G} s_h h) = \sum_{g,h \in G} r_g s_h \mu(g, h) = \sum_{g,h \in G} r_g s_h gh$$

Tengo que μ *da una multiplicación en* $\mathbb{C}G$.

$$\begin{array}{rcl} \mathbb{C}G \times \mathbb{C}G \times \mathbb{C}G & \overset{\mu \times id_{\mathbb{C}G}}{\longrightarrow} & \mathbb{C}G \times \mathbb{C}G \\ id_{\mathbb{C}G} \times \mu \downarrow & & \downarrow \mu \\ \mathbb{C}G \times \mathbb{C}G & \underset{\mu}{\longrightarrow} & \mathbb{C}G \end{array}$$

conmuta, ya que lo hace:

$$\begin{array}{rcl} G \times G \times G & \overset{m \times id_G}{\longrightarrow} & G \times G \\ id_G \times m \downarrow & & \downarrow m \\ G \times G & \underset{m}{\longrightarrow} & G \end{array}$$

Además, μ *es distributiva, y el "uno" de* $\mathbb{C}G$ *es* $1e$.

La aplicación $\mathbb{C} \overset{\eta}{\to} \mathbb{C}G, z \mapsto ze$ *es homomorfismos de anillos inyectivo.*

$Im\eta$ *subanillo de* $\mathbb{C}G$ *y* $Im\eta \cong \mathbb{C}$, *y* $\mathbb{C} \subseteq Z(\mathbb{C}G)$.

$$g \in G, z \in \mathbb{C} \quad gz = g\eta(z) = gze = zge = zg$$

En la práctica, esto nos permite escribir $1e = 1 = e$.

$\mathbb{C}G$ *se llama* $\mathbb{C}-$*álgebra del grupo* G.

Tomo $\mu(G) = \{f : G \to \mathbb{C}, f \text{ aplicación}\}$, *que es un* $\mathbb{C}-$*espacio vectorial.*
$\mu(G)$ *es un* $\mathbb{C}G-$*módulo así:*
Tomado $g \in G, \phi \in \mu(G), x \in G$

$$(g\varphi)(x) = \varphi(xg)$$

$$g(h\varphi)(x) = (h\varphi)(xg) = \varphi((xg)h) = \varphi(x(gh)) = (gh \cdot \varphi)(x)$$

$\Rightarrow g \cdot (h \cdot \varphi) = (gh) \cdot \varphi$.

$$G \to End_{\mathbb{C}}(\mu(G), \mu(G))$$

$$g \mapsto \varphi \mapsto g\varphi$$

$g(z\phi) = z(g\phi)$
$g(z\phi)(x) = (z\phi)(xg) = z\phi(xg) = z(g\phi)(x)$

$$\mathbb{C}G \to End_{\mathbb{C}}(\mu(G), \mu(G))$$
$$\sum_{g\in G} r_g g \mapsto \varphi \mapsto \sum_{g\in G} r_g g\varphi$$

homomorfismo de anillos ($\mathbb{C}-$lineal).

$\Rightarrow \mu(G)$ *es un* $\mathbb{C}G-$*módulo.*

Objetivo próximo: Si G es finito $\Rightarrow \mathbb{C}G$ es semisimple.
$\Rightarrow \mu(G)$ semisimple como $\mathcal{C}G-$módulo.

Definición 10.13 (Producto Interno)
Sea V $\mathbb{C}-$*espacio de* $dim_{\mathbb{C}} < \infty$.
Un producto (interno) Hermítico es una aplicación $<,>: V \times V \to \mathbb{C}$ *tal que:*

1. $< v, w >= < \bar{w}, v >, \forall v, w \in V$.
2. $< v + v', w >=< v, w > + < v', w >, \forall v, v', w \in V$.
3. $< \alpha v, w >= \alpha < v, w >, \forall \alpha \in \mathbb{C}, \forall v, w, \in G$.
4. *Si* $v \neq 0 \Rightarrow < v, v >> 0$.

Podemos definir la norma

$$||v|| = \sqrt{< v, v >}$$

Nota:

$$\begin{array}{rl} Set \overset{L}{\to} & Vect_{\mathbb{C}} \\ X \mapsto & \mathbb{C}X \end{array}$$

$Vect_{\mathbb{C}}(\mathbb{C}X, V) \cong Set(X, V) = Set(X, U(V))$.

Si llamamos $Set \overset{U}{\leftarrow} Vect_C \Rightarrow L$ es adjunta a izquierda de U.

$$\begin{array}{rl} Set \underset{L}{\overset{U}{\leftarrow\!\!\rightarrow}} & Vect_C \\ \uparrow & \uparrow \\ Grupos \underset{L}{\longrightarrow} & Alg_{\mathbb{C}} \end{array}$$

Proposición 10.14 (Repaso)
G grupo, $\mathbb{C}G$ *álgebra compleja del grupo G.*

$\mu(G) = \{\varphi : G \to \mathbb{C}\}$ *es un* $\mathbb{C}G-$*módulo.*
$\mu(G)$ *es el espacio de representación de la representación*

$$\rho : G \to GL_{\mathbb{C}}(\mu(G))$$

dada por $\rho(g)(\varphi)(x) = (g\varphi)(x) = \varphi(xg), g, x \in G, \varphi \in \mu(G)$.

V *un* $\mathbb{C}G-$*módulo* $\overset{V \text{ restr. escalar}}{\Rightarrow}_{\mathbb{C}} V$ *espacio vectorial.*

$\mathbb{C} \subseteq \mathbb{C}G$*:*

$$\mathbb{C}G \overset{\rho}{\to} End_{\mathbb{C}}(V)$$
$$\sum_{g\in G} r_g g \mapsto \rho(\sum_{g\in G} r_g g)(v) = (\sum_{g\in G} r_g g)v = \sum_{g\in G} r_g gv$$

ρ *de anillos y de* $\mathbb{C}-$*e.e v.v.*

$$\begin{array}{ccc} \mathbb{C}G & \overset{\rho}{\to} & End_{\mathbb{C}}(V) \\ \subseteq & & \subseteq \\ G & \underset{\substack{\rho \\ \text{hom. de grupos}}}{\to} & GL_{\mathbb{C}}(V) \end{array}$$

$G \overset{\rho}{\to} GL_{\mathbb{C}}(V)$ *se llama representación lineal de* G *con espacio de representación* V.

$W \subseteq V, \mathbb{C}G-$*submódulo* $\iff W$ $\mathbb{C}-$*subespacio vectorial y* W *es* $G-$*invariante* $(w \in W, g \in G \Rightarrow gw \in W)$.

Teorema 10.15
Si G *es finito* $\Rightarrow \mathbb{C}G$ *es semisimple.*

Demostración. G finito.
V $\mathbb{C}G-$módulo de dimensión finita.
Tomo $<,>$ un producto interno en V.
Defino $<,>_G$ producto interno (se comprueba) sobre V así:

$$< v, u >_G = \sum_{g\in G} < gv, gu >$$

$$< hv, hw >_G = \sum_{g\in G} < ghv, ghw > = \sum_{g\in G} < gv, gw > = < v, w >_G$$

W es un $\mathbb{C}G-$submódulo de V.
$V = W \dotplus W^{\perp}$ (de $\mathbb{C}-$e.e. v.v.).
$W^{\perp} = \{v \in V \mid < v, w > G = 0, \forall w \in W\}$ es un $\mathbb{C}G-$submódulo.
O sea, $W^{\perp}$ es G-invariante. Es decir, he de ver que si $v \in W^{\perp}, g \in G \Rightarrow gv \in W^{\perp}$.
Dado $w \in W$,

$$< gv, w >_G = < gv, gg^{-1}w > = < v, \underbrace{g^{-1}w}_{\in W} > = 0$$

$\Rightarrow W^{\perp}$ es $G-$invariante. $\square$

Corolario 10.16
Si G es finito $\Rightarrow \mu(G)$ $\mathbb{C}G-$módulo semisimple.

Proposición 10.17
G finito.
Doto a $\mu(G)$ del producto interno:

$$< \varphi, \psi >= \frac{1}{|G|} \sum_{g \in G} \varphi(g)\bar{\psi(g)}$$

Si G fuera infinito, no podríamos realizar la suma, tendríamos que realizar una integral, y el producto interno estaría definido sólo en las funciones integrables.

Definición 10.18
G grupo.
V $\mathbb{C}G-$módulo, $dim_{\mathbb{C}} V < \infty$.
$\{v_1, v_2\}$ $\mathbb{C}-$base de V.
$x \in G, xv_i = \sum_j t_{ij}(x)v_j, t_{ij}(x) \in \mathbb{C}$.

Podemos ver como funciones $t_{ij} \in \mu(G)$, dadas por $t_{ij}(x)$, y se llaman funciones matriciales de V con respecto de la base $\{v_1, \ldots, v_n\}$.

Definimos $C(V)$ como el subespacio vectorial de $\mu(G)$ generado por $\{t_{ij} : i \leq i, j \leq n\}$. Más adelante veremos que $C(V)$ no depende de la base.

Supongo V' otro $\mathbb{C}G-$módulo con base $\{v'_1, \ldots, v'_m\}$. Sea $f : V \to V'$ homomorfismo de $\mathbb{C}G-$módulos. Las funciones matriciales de V' con respecto de $\{v'_1, \ldots, v'_m\}$ las denotamos por $\{t'_{ij} : 1 \leq i, j \leq m\}$.

$$f(v_i) = \sum_j a_{ij} v'_j, (a_{ij}) = A$$

con A matriz de f con respecto de las bases consideradas.

$$xf(v_i) = x \sum_j a_{ij} v'_j = \sum_j a_{ij} x v'_j = \sum_j a_{ij} \sum_k t'_{jk}(x) v'_k$$

$$f(xv_i) = f(\sum_j t_{ij}(x)v_j) = \sum_j t_{ij}(x) f(v_j) = \sum_j t_{ij}(x) \sum_k a_{jk} v'_k$$

Como $xf(v_i) = f(xv_i) \Rightarrow \sum_j a_{ij} \sum_k t'_{jk}(x)v'_k = \sum_j t_{ij}(x) \sum_k a_{jk} v'_k$. Por lo que:

$$A(t'_{ij}(x)) = (t_{ij}(x))A$$

$$A(t'_{ij}) = (t_{ij})A$$

Consecuencia: Si f es isomorfimo $\Rightarrow$ A es inversible $\Rightarrow$ $t'_{ij} = A^{-1}(t_{ij})A$, $t_{ij} = A(t'_{ij})A^{-1} \Rightarrow C(V)$ no depende de la base elegida $\Rightarrow C(V) = C(V')$.

Lema 10.19
$C(V)$ es un $\mathbb{C}G-$submódulo de $\mu(G)$.

Demostración. $x, y \in G$.
$xv_i = \sum_j t_{ij}(x)v_j$.

$$t_{ij}(xy) = \sum_k t_{ik}(y)t_{kj}(x) \qquad \text{(ecuación matricial)}$$

$yt_{ij}(x) = t_{ij}(xy) = \sum_k t_{ik}(y)t_{kj}(x) = (\sum_k t_{ik}(y)t_{kj})(x) \Rightarrow$
$\Rightarrow yt_{ij} = \sum_k t_{ik}(y)t_{kj} \in C(V)$ □

Lema 10.20
Sea $f : V \to \mu(G)$ homorfismo de $\mathcal{C}G-$módulos $\Rightarrow Imf \subseteq C(V)$.

Demostración.

$$f(v_i)(x) = f(v_i)(ex) = xf(v_i)(e) = f(xv_i)(e) = f(\sum_j t_{ij}(x)v_j)(e) =$$

$$= \sum_j t_{ij}(x)(e) = (\sum_j f(v_j)(e)t_{ij})(x) \Rightarrow$$

$$\Rightarrow f(v_i) = \sum_j f(v_j)(e)t_{ij} \in C(V)$$

□

Lema 10.21
G finito. Sean U, W $\mathbb{C}G-$módulos (no necesariamente de dimensión finita) y $f : U \to W$ $\mathbb{C}-$lineal. Defino la aplicación $\bar{f} : U \to W$ dada por:

$$\bar{f}(u) = \sum_{x \in G} x^{-1} f(xu), u \in U$$

es un homomorfismo de $\mathbb{C}G-$módulos.

Demostración. He de ver que $\bar{f}(yu) = y\bar{f}(u), \forall y \in G, \forall u \in U$.

$$\bar{f}(yu) = \sum_{x \in G} x^{-1} f(xyu) \overset{z=xy}{=} \sum_{z \in G} yz^{-1} f(zu) = y\bar{f}(u)$$

$z = xy \Rightarrow x = zy^{-1} \Rightarrow x^{-1} = yz^{-1}$. □

Lema 10.22
G finito, V $\mathbb{C}G-$módulo de $dim_{\mathbb{C}}V < \infty$. Existe un producto interno $<,>_G$ en V tal que $< xv, xw >_G = < v, w >_G, \forall v, w \in V, \forall x \in G$.

Esto significa que la representación $G \to U(V)$ (grupo unitario).

Demostración. Demostrado previamente. □

[...] → 17 y 18/05/2022.

$\mathbb{Z}_n = \{t^{\Sigma_j} : j \in \{0, \dots, n-1\}\}$ base ortonormal de $\mu(\mathbb{Z}_n)$.
$k \in \mathbb{Z}_n \quad t^{\Sigma_j}(k) = \omega^{jk} \quad w = e^{\frac{i2\pi}{n}}$
$t^{\Sigma_j} t^{\Sigma_{j'}} = t^{\Sigma_{j+j'}}$
$\varphi \in \mu(\mathbb{Z}_n), \qquad \varphi = \sum_{j=0}^{n-1} < \varphi, t^{\Sigma_j} > t^{\Sigma_j}$.
$\hat{\varphi}(j) = < \varphi, t^{\Sigma_j} > = \frac{1}{n} \sum_{k=0}^{n-1} \varphi(k)\omega^{-kj}$.

$$\varphi\psi = (\sum_{j=0}^{n-1} \hat{\varphi}(j)t^{\Sigma_j})(\sum_{j'=0}^{n-1} \hat{\psi}(j)t^{\Sigma_{j'}}) = \sum_{j,j'} \hat{\varphi}(j)\hat{\psi}(j')t^{\Sigma_j}t^{\Sigma_{j'}} =$$

$$= \sum_{l=0}^{n-1} (\sum_{j+j'=k} \hat{\varphi}(j)\hat{\psi}(j'))t^{\Sigma_l} = \sum_{l=0}^{n-1} (\sum_{j=0}^{n-1} \hat{\varphi}(j)\hat{\psi}(l-j))t^{\Sigma_l}$$

Ejercicio 10.23
Para $G = \mathbb{Z}_n \times \mathbb{Z}_m$, calcular $\Omega_{\mathbb{C}G}$, y deducir la correspondiente base ortonormal de $\mu(\mathbb{Z}_n \times \mathbb{Z}_m)$.

Ejemplo 10.24 (Posible examen)
D_n lo doy por generadores r, s con relaciones $r^n = s^2 = 1, sr = r^{n-1}s = r^{-1}s$.

$$D_n = \{s^a r^j : a \in \{0,1\}, j \in \{0, \dots, n-1\}\}$$

¿$\mu(D_n)$?
$\alpha \in \mathbb{C}, \alpha^n = 1$
V_α $\mathbb{C}-$ *espacio vectorial Hermitiano con base ortonormal,* $\{v_1, v_2\}$.

$$\begin{aligned} D_n \to & \quad U(V_\alpha) \\ r \mapsto & \quad \begin{pmatrix} \alpha & 0 \\ 0 & \bar{\alpha} \end{pmatrix} \\ s \mapsto & \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{aligned}$$

$$sr = r^{-1}s \Rightarrow \begin{pmatrix} \alpha & 0 \\ 0 & \bar{\alpha} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \bar{\alpha} & 0 \\ 0 & \alpha \end{pmatrix}$$

$$\begin{pmatrix}\alpha & 0\\ 0 & \bar{\alpha}\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}=\begin{pmatrix}0 & \alpha\\ \bar{\alpha} & 0\end{pmatrix}$$
$$\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}\bar{\alpha} & 0\\ 0 & \alpha\end{pmatrix}=\begin{pmatrix}0 & \alpha\\ \bar{\alpha} & 0\end{pmatrix}$$

V_α un $\mathbb{C}D_n-$módulo.
¿V_α irreducible? ¿O sea, simple?
V_α no simple $\iff \exists 0 \neq v \in V_\alpha$ *tal que* $\mathbb{C}v$ *es submódulo* $\iff$
$\iff \exists 0 \neq v \in V_\alpha \mid rv, sv \in \mathbb{C}v$.

Pongo todo en coordenadas, $v \equiv (x, y) \in \mathbb{C}^2$

$$(x,y)\begin{pmatrix}\alpha & 0\\ 0 & \bar{\alpha}\end{pmatrix}=\beta(x,y)$$

$$(x,y)\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}=\gamma(x,y)$$

para ciertos $\beta, \gamma \in \mathbb{C}$.
$\Rightarrow \alpha^2 = 1$.

$$\alpha^2 \neq 1 \Rightarrow V_\alpha \text{ simple}$$

$V_\alpha \overset{\mathbb{C}D_n-\text{módulo}}{\cong} V_{\alpha'} \Rightarrow \alpha + \bar{\alpha} = \alpha' + \bar{\alpha'}$

$$\alpha + \bar{\alpha} \neq \alpha' + \bar{\alpha'} \Rightarrow V_\alpha \ncong V_{\alpha'}$$

Funciones matriciales de V_α: $\begin{pmatrix}t_{11} & t_{12}\\ t_{21} & t_{22}\end{pmatrix}$

$$s^a r^j \mapsto \begin{pmatrix}\alpha & 0\\ 0 & \bar{\alpha}\end{pmatrix}^j \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}^a = \begin{cases}\begin{pmatrix}\alpha^j & 0\\ 0 & \bar{\alpha}^j\end{pmatrix} & si\ a=0\\ \begin{pmatrix}0 & \alpha^j\\ \bar{\alpha}^j & 0\end{pmatrix} & si\ a=1\end{cases}$$

Entonces:

$$t_{11}(s^a r^j) = \begin{cases}\alpha^j & si\ a=0\\ 0 & si\ a=1\end{cases}$$

$$t_{12}(s^a r^j) = \begin{cases}0 & si\ a=0\\ \alpha^j & si\ a=1\end{cases}$$

$$t_{21}(s^a r^j) = \begin{cases}0 & si\ a=0\\ \bar{\alpha}^j & si\ a=1\end{cases}$$

$$t_{22}(s^a r^j) = \begin{cases} \bar{\alpha}^j & si\ a = 0 \\ 0 & si\ a = 1 \end{cases}$$

Queremos calcular $\Omega_{\mathbb{C}D_n}$. *Tomo* $w = e^{\frac{i2\pi}{n}} \in \mathbb{C}$.

$$(\omega^j)^2 = 1 \iff \omega^{2j} = 1 \iff \frac{2\pi 2j}{n} = \text{ múltiplo entero de } 2\pi \iff$$

$$\iff 2j = \text{ múltiplo entero de } n$$

Si $2j$ *no es múltiplo entero de* $n \Rightarrow V_{w^j}$ *es simple.*

(n impar) Entonces $n = w\nu + 1, \nu \in \mathbb{N}$. *Para* $j \in \{1, \ldots, \nu\}$, *se tiene que* V_{w^j} *es simple.*

Si $j' \in \{1, \ldots, \nu\}$

$$\omega^j + \omega^{-j} = w^{j'} + w^{-j'}$$

$\Rightarrow \cos\frac{2\pi j}{n} = \cos\frac{2\pi j'}{n} \Rightarrow j = j'$.

V_{ω^j} *es simple, y son todos no isomorfos entre sí.*

$$\Omega_{\mathbb{C}D_n} \supset \{\Sigma_1, \ldots, \Sigma_\nu\}$$

Como $|G| = d_1^2 + \cdots + d_t$, *en este caso tenemos que* $|G| = |D_n| = 2n$ *y* $d_1^2 + \cdots + d_\nu^2 = 2^2 + \overset{\nu}{\ldots} + 2^2 = 4\nu$, *entonces*

$$2n - 4\nu = 4\nu + 2 - 4\nu = 2$$

Faltan en la lista dos módulos de $dim_{\mathbb{C}} = 1$.

Σ_0 *es el* $\mathbb{C}D_n-$*módulo cuya representación es la trivial,* $s^a r^k \mapsto 1 \in \mathbb{C}^x$.

Σ_{-1} *es* $s^a r^k \mapsto \begin{cases} 1 & si\ a = 0 \\ -1 & si\ a = -1 \end{cases}$

Por lo que:

$$\Omega_{\mathbb{C}D_n} = \{\Sigma_1, \ldots, \Sigma_\nu, \Sigma_{-1}, \Sigma_0\}$$

$\{t^{\Sigma_{-1}}, t^{\Sigma_0}, \sqrt{2}t_{bc}^{\Sigma_j} : j \in \{1, \ldots, \nu\}; b, c \in \{1, 2\}\}$ *base ortonormal.*

<u>Nota</u>*: Como* Σ_{-1} *y* Σ_0 *son de dimensión 1, no hay que normalizarlos, y* $t^{\Sigma_{-1}}$ *y* t^{Σ_0} *son escalares.*
Para los demás Σ_j, *como son de dimensión 2, normalizamos añadiendo* $\sqrt{2}$.

$$t^{\Sigma_0}(s^a r^k) = 1$$

$$t^{\Sigma_{-1}}(s^a r^k) = \begin{cases} 1 & si\ a = 0, k \in \{0, \dots, n-1\} \\ -1 & si\ a = 1, k \in \{0, \dots, n-1\} \end{cases}$$

$$t_{11}^{\Sigma_j}(s^a r^k) = \begin{cases} e^{\frac{i2\pi kj}{n}} & si\ a = 0, k \in \{0, \dots, n-1\} \\ 0 & si\ a = 1, k \in \{0, \dots, n-1\} \end{cases}$$

$$t_{12}^{\Sigma_j}(s^a r^k) = \begin{cases} 0 & si\ a = 0, k \in \{0, \dots, n-1\} \\ e^{\frac{i2\pi kj}{n}} & si\ a = 1, k \in \{0, \dots, n-1\} \end{cases}$$

$$t_{21}^{\Sigma_j}(s^a r^k) = \begin{cases} 0 & si\ a = 0, k \in \{0, \dots, n-1\} \\ e^{-\frac{i2\pi kj}{n}} & si\ a = 1, k \in \{0, \dots, n-1\} \end{cases}$$

$$t_{22}^{\Sigma_j}(s^a r^k) = \begin{cases} e^{-\frac{i2\pi kj}{n}} & si\ a = 0, k \in \{0, \dots, n-1\} \\ 0 & si\ a = 1, k \in \{0, \dots, n-1\} \end{cases}$$

Ejemplo 10.25
¿Y si G no es finito?
Lo más fácil es que sea un grupo de Lie compacto (no hemos visto nada de esto, es sólo para el ejemplo).

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

Tengo $\mathbb{C}S^1$. *Tomo* $\mathbb{C}S^1-$*módulos de dimensión compleja finita que provengan de representaciones continuas de* S^1. *Estas son los homomorfismos continuos de grupos* $\rho : S^1 \to GL(V)$, $dim_{\mathbb{C}} V < \infty$.

Dada ρ, *quiero inventarme un producto directo* $<,>_{S^1}$ *en* V *tal que*

$$< \rho(z)(v), \rho(z)(w) >_{S^1} =< v, w >_{S^1}, \forall v, w \in V, z \in S^1$$

$$\rho(z)(v) = zv$$

En efecto, tómese $<,>$ *producto interno en* V *y definimos:*

$$< v, w >_{S^1} = \int_{S^1} < zv, zw > \qquad es\ un\ producto\ interno\ en\ V$$

(Como estamos en dimensión infinita, integramos en vez de sumar. Además, por cómo hemos definido el producto interno es continuo, y S^1 *es compacto, por lo que es integrable y la integral es finita).*

Para un z' *fijo:*

$$< z'v, z'w >_{S^1} = \int_{S^1} < z'zv, z'zw > \overset{\bigstar}{=} \int_{S^1} < zv, zw > =< v, w >_{S^1}$$

$\bigstar$ *La medida que uso en* S^1 *es invariante por la acción de* z'.

Ejemplo 10.26
$x(n), y(n)$ sucesiones de números complejos ($n \in \mathbb{N}$) que verifican:

$$\begin{cases} x(n+1) = \lambda x(n) - y(n) + c \\ y(n+1) = \lambda y(n) + (1-\lambda)c \end{cases} \quad n \geq 0$$

Discutir el comportamiento de $x(n), y(n)$ en función de los parámetros λ, c y $x(0), y(0)$.

Defino $z(n) = c, \forall n \in \mathbb{N}$.

$$(x(n+1), y(n+1), z(n+1)) = (x(n), y(n), z(n)) \underbrace{\begin{pmatrix} \lambda & 0 & 0 \\ -1 & \lambda & 0 \\ 1 & 1-\lambda & 1 \end{pmatrix}}_{=B}$$

$$(x(n), y(n), z(n)) = (x(0), y(0), z(0))B^n$$

¿Cómo describo B^n? Calculamos la forma canónica de Jordan.

$$XI - B = \begin{pmatrix} X-\lambda & 0 & 0 \\ 1 & X-\lambda & 0 \\ -1 & \lambda - 1 & X-1 \end{pmatrix} \sim \begin{pmatrix} 1 & X-\lambda & 0 \\ X-\lambda & 0 & 0 \\ -1 & \lambda - 1 & X-1 \end{pmatrix} \sim$$

$$\sim \begin{pmatrix} 1 & X-\lambda & 0 \\ 0 & -(X-\lambda)^2 & 0 \\ 0 & X-1 & X-1 \end{pmatrix} \overset{c_2-(X-\lambda)c_1}{\sim} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -(X-\lambda)^2 & 0 \\ 0 & X-1 & X-1 \end{pmatrix} \sim$$

$$\overset{c_2-c_3}{\sim} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -(X-\lambda)^2 & 0 \\ 0 & 0 & X-1 \end{pmatrix}$$

Tomo V e.v. complejo con base $\{e_1, e_2, e_3\}$. La veo como $\mathbb{C}[X]-$módulo a través de B.

$$V = \mathbb{C}[X]w_1 \dot{+} \mathbb{C}[X]w_2 \dot{+} \mathbb{C}[X]w_3$$

donde

- $ann_{\mathbb{C}[X]}(w_1) =< 1 > (\Rightarrow w_1 = 0)$.
- $ann_{\mathbb{C}[X]}(w_2) =< (X-\lambda)^2 >$.
- $ann_{\mathbb{C}[X]}(w_3) =< X-1 >$.

$$Q = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \overset{c_2+c_3}{\sim} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \overset{c_2+(X-\lambda)c_1}{\sim} \begin{pmatrix} 1 & X-\lambda & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

Entonces:

- $w_1 = e_1 + (X - \lambda)e_2$.
- $w_2 = e_2$.
- $w_3 = e_2 + e_3$.

$$V = \mathbb{C}[X]w_1 \dot{+} \mathbb{C}[X]w_2 \dot{+} \mathbb{C}[X]w_3 = \mathbb{C}[X]e_2 + \mathbb{C}[X](e_2 + e_3)$$

Tomo la base de V formada por $\{e_2, (X - \lambda)e_2, e_2 + e_3\}$ con respecto de la cual el endomorfismo dado por B está representado por la matriz:

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

$$B = P^{-1}DP$$

donde P es la matriz del cambio de base. Como $(X - \lambda)e_2 = Xe_2 - \lambda e_2 = (-1, \lambda, 0) - (0, \lambda, 0) = (-1, 0, 0)$. Entonces:

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

Tenemos:

$$B^n = P^{-1}D^nP = P^{-1} \begin{pmatrix} \lambda^n & n\lambda^{n-1} & 0 \\ 0 & \lambda^n & 0 \\ 0 & 0 & 1 \end{pmatrix} P$$

Como teníamos:

$$(x(n), y(n), z(n)) = (x(0), y(0), z(0))B^n$$

con $z(n) = c$, entonces:

$$(x(n), y(n), z(n)) = (x(0), y(0), z(0))B^n = (x(0), y(0), z(0))P^{-1}D^nP \Rightarrow$$

$$\Rightarrow (x(n), y(n), z(n))P^{-1} = (x(0), y(0), z(0))P^{-1}D^n$$

Como:

$$P^{-1} = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ -1 & 0 & 1 \end{pmatrix}$$

Entonces:

$$(y(n) - c, -x(n), c) = (y(0) - c, -x(0), c) \begin{pmatrix} \lambda^n & n\lambda^{n-1} & 0 \\ 0 & \lambda^n & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Nota:

No podemos hacer $e^{A+B} = e^A e^B$ con A, B matrices porque no conmutan.

En el caso de que si conmuten, si podemos, por ejemplo:

$$\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} = \lambda I + \underbrace{\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}}_{=N}$$

Entonces:

$$e^{\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}} = e^{I\lambda} e^N = \begin{pmatrix} e^\lambda & 0 \\ 0 & e^\lambda \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

donde para e^N usamos que:

$$e^A = \sum_{m \geq 0} \frac{A^m}{m!}$$

por lo que $e^N = \frac{N^0}{0!} + \frac{N}{1!} + 0 + 0 + \cdots = I + N = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.