Álgebra Abstracta

José Antonio de la Rosa Cubero

Índice

1. Introducción

1.1. Generalidades sobre anillos

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

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

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

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

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

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

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

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

La suma de ideales es un ideal.

Definición 4 (Ideales coprimos)**.** Dos ideales $I, J \subset A$ se dirán primos entre sí o coprimos si $I + J = A$.

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

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

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

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

Demostración.

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

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

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

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

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

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

Demostración. Para $t = 2$ es trivial.

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

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

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

La otra implicación es muy sencilla. □

Hipótesis de trabajo para el teorema chino del resto:

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

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

Demostración. Veamos primero la implicación a la derecha.

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

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

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

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

Por tanto, $I_i + \bigcap I_j = A$ y entonces por el lema anterior $I_i + I_j = A$.

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

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

Para cada i, tomamos $1 = a_i + p_i$ con $a_i \in I_i$ y $p_i \in \bigcap I_j$.

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

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

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

$\square$

Observación 1. Para anillos conmutativos denotamos

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

el ideal generado por a.

Vamos a hacer un ejemplo, aplicando el teorema anterior.

1.1.1. Interpolación

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

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

$\operatorname{Im} X_i = K$ y $\xi : K[x] \longrightarrow K \times \cdots K = K^t$.

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

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

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

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

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

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

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

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

es un isomorfismo de anillos.

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

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

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

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

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

$$1 = 1 + p$$

$$x = x + p$$

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

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

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

que vale 0 en α_j para cualquier j salvo en α_i que vale 1.

Tenemos que

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

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

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

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

1.1.2. Transformada discreta de Fourier

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

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

Seguro que $\operatorname{car} K \not| n$ ya que $1, \omega, \omega^2, \ldots, \omega^{n-1}$ son las raíces de $x^n - 1$ y son distintas.

Vamos a interpolar las raíces de la unidad.

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

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

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

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

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

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

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

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

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

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

donde $\hat{y} = y \frac{1}{n} A^T_{\omega^{-1}}$.

Explicitamente, se calcula que los coeficientes quedan:

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

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

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

que es la transformada de Fourier de y.

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

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

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

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

2. Módulos

Definición 5. Sean M, N grupos aditivos:

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

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

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

Definición 6 (Anillo de endomorfismo de M)**.** Definimos directamente $\mathrm{End}(M) := \mathrm{Ad}(M,M)$.

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

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

Finalmente se ve que se cumplen las propiedades distributivas, que se siguen de que son homomorfismos. □

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

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

Definición 7 (Módulo)**.** Sea M un grupo aditivo y A un anillo. Una estructura de A-módulo sobre M es un homomorfismo de anillos $\rho : A \longrightarrow \mathrm{End}(M)$.

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

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

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

Entonces:

$$\psi : \mathrm{Map}(X \times Y, Z) \longrightarrow \mathrm{Map}(X, \mathrm{Map}(Y,Z))$$

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

Ejercicio: comprobar que ψ^{-1} es realmente la inversa de ψ.

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

$$\psi : \mathrm{Biad}(M \times N, L) \longrightarrow \mathrm{Ad}(M, \mathrm{Ad}(N,L))$$

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

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

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

Ejercicio, demostrar que la aplicación ψ es una biyección.

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

Definición 8.

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

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

1. *Homomorfismos de anillos* $\rho : A \longrightarrow \mathrm{End}(M)$
2. *Las aplicaciones $A \times M \longrightarrow M$ que satisfacen:*
   - $(a + a')m = am + a'm$
   - $a(m + m') = am + am'$
   - $(aa')m = a(a'm)$
   - $1 \cdot m = m$

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

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

Comprobamos la tercera propiedad como ejemplo:

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

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

De forma análoga se demuestran el resto de propiedades.

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

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

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

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

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

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

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

2.1. $K[x]$-módulos con K cuerpo

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

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

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

Veamos que es un endomorfismo de espacios vectoriales:

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

Así que $\rho(x)$ es K-lineal.

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

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

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

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

resulta que V es un $K[x]$-módulo.

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

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

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

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

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

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

2.2. Módulos abstractos

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

Aplicando el primer teorema de isomorfía, tenemos:

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

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

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

se le llama el anulador de M.

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

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

Definición 9. Un submódulo de un módulo ${}_AM$ es un subgrupo aditivo $N \subseteq M$ tal que $am \in N$ para cualquier $a \in A$ y $m \in N$. Los submódulos del módulo regular A se llaman ideales por la izquierda de A.

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

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

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

Tenemos que el conjunto:

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

es un ideal a izquierda de A.

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

Definición 10 (Submódulo cíclico)**.** Dado ${}_AM$, y un $m \in M$. Es claro que $Am = \{am : a \in A\}$ es un submódulo de ${}_AM$ que se llama submódulo cíclico generado por m.

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

Definición 11 (Submódulo finitamente generado)**.** Dados $m_1, \dots, m_n \in M$, el conjunto

$$Am_1 + \cdots + Am_n = \{a_1 m_1 + \cdots + a_n m_n : a_i \in A\}$$

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

2.2.1. Suma directa interna

Definición 12 (Módulo suma)**.** Dados $N_1, \dots, N_n$ submódulos de ${}_AM$, defino:

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

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

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

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

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

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

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

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

Definición 13 (Suma interna)**.** Si $M = N_1 + \cdots + N_t$ tales que satisfacen una de las condiciones equivalentes anteriores, diremos que M es la suma directa interna y usaremos la notación $M = N_1 \dot{+} \cdots \dot{+} N_t$.

Definición 14. Si $\{N_1, \dots, N_t\}$ verifican las condiciones equivalentes anteriores y $N_i \neq \{0\}$, se dice que el conjunto $\{N_1, \dots, N_t\}$ es una familia independiente.

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

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

Tomamos

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

y

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

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

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

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

2.2.2. Módulos acotados sobre un DIP

Definición 15 (Módulo acotado sobre un DIP)**.** Sea A un dominio de ideales principales, ${}_AM$ un módulo, $\mathrm{Ann}_A(M) = \langle \mu \rangle$ para cierto $\mu \in A$.

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

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

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

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

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

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

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

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

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

$$0 = q_j a_j 0 = m_j$$

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

Definición 16 (Componentes primarias)**.** Tenemos que los M_i se llaman componentes primarias.

Proposición 7.

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

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

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

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

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

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

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

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

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

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

es decir, el subespacio propio asociado al valor propio α_i.

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

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

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

2.3. Homomorfismos de módulos

Definición 17 (Módulo cociente o factor)**.** Sea ${}_AM$ y $L \in \mathcal{L}(M)$. Consideramos M/L grupo aditivo y se define la acción:

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

M/L es un módulo.

Definición 18 (Homomorfismo de módulos)**.** Se dice que $f : {}_AM \longrightarrow {}_AN$ es un homomorfismo de módulos si respeta sumas y productos.

Definición 19 (Proyección canónica)**.** Es la aplicación $\pi : M \longrightarrow M/L$ dada por $\pi(m) = m + L$ es un homomorfismo de módulos.

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

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

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

es un homomorfismo de A-módulos.

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

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

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

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

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

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

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

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

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

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

Volviendo al caso general, tenemos que

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

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

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

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

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

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

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

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

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

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

2.3.1. Suma directa externa

Definición 20. Tomando el producto cartesiano de t módulos sobre el mismo anillo y tomando la suma usual de tuplas y definiendo el siguiente producto:

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

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

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

Ejercicio: Sea ${}_AM$, $N_1, \ldots, N_t \in \mathcal{L}({}_AM)$. Se pide demostrar que existe un homomorfismo $f : N_1 \oplus \cdots \oplus N_t \longrightarrow N_1 + \cdots + N_t$ sobreyectivo de A-módulos tal que entre la suma directa externa y la suma interna, tal que f es un isomorfismo si y solo si la suma interna es directa. Podría ser interesante usar coordenadas.

Definición 21 (Base de un módulo libre)**.** Consideramos $A^n = A \oplus \cdots \oplus A$, donde la suma se repite n veces. Para cada $i = 1, \ldots, n$, tenemos que $\{e_i : e_i = (0, \ldots, 0, 1, 0, \ldots, 0)\}$ forman un sistema de generadores de A^n. Por tanto $a = \sum_i a_i e_i \in A^n$ es una expresión única.

Dicha base puede no existir.

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

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

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

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

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

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

3. Módulos Noetherianos

3.1. Álgebra homológica

Definición 22 (Sucesiones exactas)**.** Una suceión de homomorfismos de módulos $f_i : M_i \longrightarrow M_{i+1}$ se dice exacta en M_{i+1} si $\ker f_{i+1} = \operatorname{Im} f_i$.

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

A α se les llama monomorfismos de módulos y a β epimorfismos de módulos.

A esta sucesión se le llama sucesión exacta corta.

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

$$0 \longrightarrow \ker f\iota \longrightarrow Mf \longrightarrow \operatorname{Im} f \longrightarrow 0$$

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

1. *Si M es finitamente generado, lo es también N.*

2. *Si L y N son finitamente generados, lo es también M.*

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

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

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

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

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

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

y finalmente:

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

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

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

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

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

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

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

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

Definición 23 (Módulos Noetherianos)**.** Un módulo finitamente generado M se dice Noetheriano si todo submódulo de M es finitamente generado.

El ejemplo anterior no era un módulo Noetheriano.

Proposición 10. *Equivalen:*

1. *M es noetheriano.*

2. *Cualquier cadena ascendente $L_1 \subseteq L_2 \subseteq \ldots \subseteq L_n \subseteq \ldots$ se estabiliza, es decir, a partir de un cierto m las inclusiones se vuelven igualdades.*

3. *Cada subconjunto no vacío de $\mathcal{L}(M)$ tiene un elemento maximal con respecto de la inclusión.*

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

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

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

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

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

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

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

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

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

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

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

Demostración. Supongamos M noetheriano.

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

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

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

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

con lo cual N es noetheriano.

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

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

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

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

Por tanto M es noetheriano. $\square$

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

$$M_1 \oplus M_2$$

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

Demostración. Sea la sucesión exacta corta

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

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

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

Demostración. Una de las implicaciones es obvia.

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

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

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

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

$\square$

Definición 24 (Anillo noetheriano)**.** A se dice noetheriano a izquierda si el módulo regular es noetheriano. Si A es conmutativo diremos simplemente noetheriano.

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

1. M *es finitamente generado.*

2. L *y* N *son finitamente generados.*

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

3.2. Módulo Artiniano

Definición 25 (Módulo artinano)**.** Para un ${}_AM$, son equivalentes:

1. Cada cadena descendente $L_1 \supseteq L_2 \supseteq \ldots \supseteq L_n \supseteq \ldots$ de submódulos de M se estabiliza, esto es, a partir de cierto natural m se tiene $L_n = L_m$ para todo $n \geq m$.

2. Cada subconjunto de $\mathcal{L}(M)$ tiene un elemento minimal.

A un tal módulo lo llamaremos artiniano.

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

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

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

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

Proposición 12. *Sea*

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

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

Ejercicio: sea p un número primo. Definimos:

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

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

3.3. Módulos de longitud finita

Definición 26 (Serie de composición)**.** Sea M un módulo. Una serie de composición de M es una cadena de submódulos

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

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

A n le llamamos la longitud de la serie.

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

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

tiene como subgrupo maximal (argumentando por Lagrange):

$$M_2 = \langle 2 \rangle$$

que a su vez tiene como subgrupo maximal

$$M_1 = \langle 4 \rangle$$

y ya solo tiene

$$M_0 = \{0\}$$

Definición 27 (Módulo simple)**.** M se dice simple si $M \supset \{0\}$ es una serie de composición. Es decir, si no tiene submódulos propios y no es el módulo 0.

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

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

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

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

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

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

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

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

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

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

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

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

$$\{0\} = M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \dots \subsetneq M_n = M$$

$$\{0\} = N_0 \subsetneq N_1 \subsetneq N_2 \subsetneq \dots \subsetneq N_m = M$$

Entonces $n = m$ y existe una permutación σ tal que

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

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

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

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

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

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

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

y tenemos que, por el teorema de isomorfía:

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

que al ser un factor es simple.

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

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

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

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

Tenemos que, por el teorema de isomorfía:

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

que al ser un factor es simple.

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

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

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

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

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

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

□

Definición 28 (Módulo de longitud finita)**.** Un módulo se dice de longitud finita si tiene una serie de composición finita o es $\{0\}$. La longitud $\ell(M)$ es la de cualquiera de sus series de composición, o cero si $M = \{0\}$.

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

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

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

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

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

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

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

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

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

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

Definición 29 (Zócalo)**.** El zócalo de M es el menor submódulo de M que contiene a todos los submódulos simples de M.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Consideramos

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

luego

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

con lo que no sería maximal.

Luego se tiene:

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

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

Resulta que

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

es una serie de composición, ya que:

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

Aplicando Jordan-Hölder se obtiene el resultado. □

Definición 30 (Módulo semisimple)**.** Sea M de longitud finita. Decimos que M es semisimple si es $\mathrm{Soc}(M) = M$.

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

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

3.3.1. Módulos de longitud finita sobre un DIP

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

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

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

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

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

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

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

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

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

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

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

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

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

Veamos el recíproco: M acotado y finitamente generado.

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

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

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

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

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

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

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

donde

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

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

Definición 31 (Módulo p-primario)**.** ${}_AM$ se dice p-primario si $\mathrm{Ann}_A(M) = \langle p^e \rangle$, p un irreducible.

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

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

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

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

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

Corolario 7. Existe un $x ß M$, $\mathrm{Ann}_A(M) = \mathrm{ann}_A(x)$.

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

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

y como consecuencia

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

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

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

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

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

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

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

□

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

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

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

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

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

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

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

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

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

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

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

$\square$