1. Módulos

Definición. Una operación en un conjunto C es una aplicación $\theta\colon C\times C\longrightarrow C$. Dados $x,y\in C$, $\theta(x,y)$ se nota $x\theta y$.

Sea θ una operación en un conjunto C.

Definiciones. Se dice que θ es asociativa sii $(x\theta y)\theta z = x\theta(y\theta z)$ $(x,y,z\in C)$

$$(x,y,z)\rightsquigarrow\begin{cases}((x,y),z)\rightsquigarrow(x\theta y,z)\rightsquigarrow(x\theta y)\theta z\\(x,(y,z))\rightsquigarrow(x,y\theta z)\rightsquigarrow x\theta(y\theta z)\end{cases}$$

Se dice que θ es conmutativa sii $x\theta y = y\theta x$ $(x,y\in C)$.

$$\theta(x,y)=\theta(y,x):\theta \text{ es simétrica.}$$

Se dice que θ tiene elemento neutro sii $\exists\, e\in C, \forall\, x\in C\colon e\theta x = x\theta e = x$.

$$\theta(e,\ ):C\longrightarrow C \qquad \theta(\ ,e):C\longrightarrow C \qquad \exists\, e\in C:\theta(e,\ )=\theta(\ ,e)=1_C$$
$$x\mapsto\theta(e,x) \qquad x\mapsto\theta(x,e)$$

Observación. En el último caso, e es único (y se llama el elemento neutro de θ), pues más generalmente:
Si $u,v\in C$ satisfacen que $u\theta x = x$ y $x\theta v = x$, para todo $x\in C$, entonces $u=v$.
Tomando $x=u$ en $x\theta v = x$, resulta que $u\theta v = u$; y tomando $x=v$ en $u\theta x = x$, se tiene que $u\theta v = v$. Por lo tanto, $u=v$.

Definición. Un monoide es un conjunto C provisto de una operación θ asociativa. El monoide (C,θ) se dice conmutativo sii θ es conmutativa.

Ejemplo. $(\mathbb{N},+)$ es un monoide conmutativo.

Definición. Un semigrupo es un monoide cuya operación tiene elemento neutro.

Ejemplo. $(\mathbb{N},\cdot)$ es un semigrupo conmutativo; en cambio, $(\mathbb{N},+)$ no lo es, vale decir,

$$\nexists\, e\in\mathbb{N}, \forall\, n\in\mathbb{N}: n+e=n,$$

porque

$$\nexists\, e,n\in\mathbb{N}: n+e=n,$$

o sea,

$$\forall\, e,n\in\mathbb{N}: n+e\neq n.$$

Un argumento:

$$e \geq 1 \Longrightarrow n + e \geq n + 1 \Longrightarrow n + e > n.$$

Otro:

$$n + e = n \Longrightarrow (-n) + (n + e) = (-n) + n \Longrightarrow e = 0 \Longrightarrow e \notin \mathbb{N}.$$

Sea S un semigrupo, con operación θ y elemento neutro e.
Definición. Se dice que $x \in S$ es inversible sii $\exists\, y \in S : y\theta x = x\theta y = e$.

Observación. i) En tal caso, y es único (y se llama el inverso de x), porque, en general: Dado $x \in S$, si $u, v \in S$ satisfacen que $u\theta x = e$ y $x\theta v = e$, entonces $u = v$.

$$u = u\theta e = u\theta(x\theta v) = (u\theta x)\theta v = e\theta v = v.$$

ii) e es inversible, y su inverso es e: $e\theta e = e$. Además, si $x \in S$ es inversible (a izquierda o a derecha) y $x\theta x = x$, entonces $x = e$.

Definición. Un grupo es un semigrupo tal que todos sus elementos son inversibles. Lo grupos conmutativos también se llaman abelianos.

Ejemplo. $(\mathbb{U}, \cdot)$ es un grupo conmutativo.

$$\mathbb{U} = \{z \in \mathbb{C} : |z| = 1\} \qquad \mathbb{U} \times \mathbb{U} \longrightarrow \mathbb{U} \quad (z, z') \mapsto z \cdot z'$$

$i)z, z' \in \mathbb{U} \Longrightarrow z \cdot z' \in \mathbb{U}$, o sea, $|z| = |z'| = 1 \Longrightarrow |z \cdot z'| = 1$.
$ii)1 \in \mathbb{U}$, o sea, $|1| = 1$.
$iii)z \in \mathbb{U} \Longrightarrow z^{-1} \in \mathbb{U}$, o sea, $|z| = 1 \Longrightarrow |z^{-1}| = 1$.
$i')|z \cdot z'| = |z| \cdot |z'|$.
$ii')r \in \mathbb{R} \Longrightarrow |r + 0i| = |r|$.
$iii')z \neq 0 \Longrightarrow |z^{-1}| = |z|^{-1}$.

También, $|z| = 1 \Longrightarrow z^{-1} = \overline{z}$; pero $|\overline{z}| = |z|$.

En cambio, $(\mathbb{N}, \cdot)$ no es un grupo. Más aún, es un ejemplo de semigrupo S donde e es el único elemento inversible: $x\theta y = y\theta x = e \Longrightarrow x = y = e$.
En efecto,

$$\forall\, m, n \in \mathbb{N} : m \cdot n = 1 \Longrightarrow m = n = 1,$$

porque

$$n > 1 \Longrightarrow m \cdot n > m \cdot 1 = m \geq 1 \Longrightarrow m \cdot n > 1.$$

Notaciones.

	θ	e	inverso de x
aditiva*	$+$	0	$-x$
multiplicativa	$\cdot$	1	x^{-1}

*) Sólo será empleada en el caso conmutativo. La primera columna es aplicable a monoides.

Definiciones. Un anillo es un conjunto A provisto de dos operaciones, $+$ y $\cdot$ (llamadas suma y producto), tal que $(A,+)$ es un grupo abeliano, $(A,\cdot)$ es un semigrupo y se verifica:

$$i) a\cdot(b+c) = a\cdot b + a\cdot c$$
$$ii) (a+b)\cdot c = a\cdot c + b\cdot c$$

El anillo $(A,+,\cdot)$ se dice conmutativo sii $(A,\cdot)$ es conmutativo; y se llama anillo de división sii todo $x \in A$, $x \neq 0$, es inversible en $(A,\cdot)$.

Un cuerpo es un anillo de división conmutativo.

Ejemplos. i) De anillos:

	conmutativo	de división
$\mathbb{Z}$	si	no
$\mathbb{M}_n(A)$	no, para $n>1$	no, para $n>1$
$A[X]$	si	no
$\mathbb{H}$	no	si

ii) De cuerpos: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $K(X)$ (K cuerpo).

Observación. En un anillo A, son equivalentes:
i) $\forall\, a \in A : a = 0$.
ii) A tiene un solo elemento.
iii) $1 = 0$.
En tal caso, A se dice nulo.
i) $\Longrightarrow$ ii) $\Longrightarrow$ iii) son triviales. iii) $\Longrightarrow$ i) resutla de verificar que $a\cdot 0 = 0$, en cualquier anillo A (ejercicio).

Definición. Una acción de un conjunto C en un conjunto D es una aplicación $a\colon C\times D \longrightarrow D$. Dados $x \in C$ e $y \in D$ $a(x,y)$ se nota xay.

Observación. Dado un conjunto C, las nociones de "acción de C en C" y "operación en C" coinciden.

Definición. Sea A un anillo. Un A-módulo a izquierda (derecha) es un conjunto M provisto de una operación $+$, llamada suma, y una acción $\cdot$ de A, llamada producto, tal

que $(M,+)$ es un grupo abeliano y $\cdot$ satisface:

$$i)a\cdot(x+y)=a\cdot x+a\cdot y.$$
$$ii)(a+b)\cdot x=a\cdot x+b\cdot x.$$
$$iii)_s\ (a\cdot b)\cdot x=a\cdot(b\cdot x). \qquad (\ iii)_d\ (a\cdot b)\cdot x=b\cdot(a\cdot x).)$$
$$iv)1\cdot x=x.$$

Los elementos de M se llaman vectores; y los elementos de A, escalares.

Observación. i) Si M es un A-módulo a derecha, $a\cdot x$ $(a\in A, x\in M)$ suele notarse $x\cdot a$, con lo cual $iii)_d$ se escribe: $x\cdot(a\cdot b)=(x\cdot a)\cdot b$.

ii) Si A es conmutativo, las nociones de "A-módulo a izquierda" y "A-módulo a derecha" coinciden.

iii) Siendo A cualquier anillo, ambas nociones son esencialmente la misma:

Definición. Se llama anillo opuesto de A al anillo A^o que se obtiene reemplazando el producto $\cdot$ de A por el producto o dado por: $aob=b\cdot a$ $(a,b\in A)$.

$$A=(A,+,\cdot)\rightsquigarrow A^o=(A,+,o)$$

Observación. i) $A^o=A\iff A$ es conmutativo.
ii) $(A^o)^o=A$.

Definición. Si M es un A-módulo a izquierda (derecha), se llama módulo opuesto de M al A^o-módulo a derecha (izquierda) M^o que se deduce de M reemplazando A por A^o.

$$M=(A,M,+,\cdot)\rightsquigarrow M^o=(A^o,M,+,\cdot)$$

Por ejemplo, M satisface $iii)_s$ para $A\Longrightarrow M$ satisface $iii)_d$ para A^o:

$$(aob)\cdot x=(b\cdot a)\cdot x=b\cdot(a\cdot x).$$

Observación. i) Si A es conmutativo, $M^o=M$.
ii) $(M^o)^o=M$.

Notación. La clase de A-módulos a izquierda (derecha) se nota $\mathfrak{M}_s(A)$ $(\mathfrak{M}_d(A))$. Si A es conmutativo, $\mathfrak{M}_s(A)=\mathfrak{M}_d(A)$ y se escribe $\mathfrak{M}(A)$.

$$\mathfrak{M}_s(A)\longrightarrow\mathfrak{M}_d(A^o) \qquad \mathfrak{M}_d(B)\longrightarrow\mathfrak{M}_s(B^o) \qquad B=A^o\Longrightarrow\mathfrak{M}_d(A^o)\longrightarrow\mathfrak{M}_s(A)$$
$$M\mapsto M^o \qquad\qquad N\mapsto N^o$$

Las aplicaciones entre $\mathfrak{M}_s(A)$ y $\mathfrak{M}_d(A^o)$ definidas tomando módulo opuesto son recíprocas. Lo mismo sucede con las aplicaciones entre entre $\mathfrak{M}_d(A)$ y $\mathfrak{M}_s(A^o)$ (basta reemplazar A por A^o). Si A es conmutativo, todas estas aplicaciones coinciden con la aplicación identidad de $\mathfrak{M}(A)$.

Convención. Los módulos se consideran a izquierda.

Observación. En un A-módulo M, se verifica:
i) $a \cdot 0 = 0$.
ii) $0 \cdot x = 0$.
iii) $-(a \cdot x) = (-a) \cdot x = a \cdot (-x)$; en particular, $-x = (-1) \cdot x$.

Definición. Un A-módulo se dice nulo si y sólo si $\forall\, x \in M : x = 0$ (vale decir, M tiene un sólo elemento).

Observación. Si A es un anillo nulo, todo A-módulo es nulo.

Convención. Los anillos se suponen no nulos.

Ejemplos. i) Espacios vectoriales.
Dado un cuerpo K, "K-módulo" es lo mismo que "K-espacio vectorial". Si D es un anillo de división, los D-módulos serán llamados D-espacios vectoriales.
ii) Grupos abelianos y $\mathbb{Z}$-módulos.
Sea $(G, +)$ un grupo abeliano. Se construye una acción $*$ de $\mathbb{Z}$ en G definiendo $m * x$ $(m \in \mathbb{Z}, x \in G)$ en la forma: si $m \geq 0$, $m * x$ se define por inducción en m, tomando $0 * x = 0$ y $(h+1) * x = h * x + x$ $(h \in \mathbb{N}_0)$; y si $m < 0$, $m * x$ se define poniendo $m * x = (-m) * (-x)$. Se verifica que $(G, +, *)$ es un $\mathbb{Z}$-módulo (ejercicio).
Además, si $\cdot$ es una acción de $\mathbb{Z}$ en G tal que $(G, +, \cdot)$ es un $\mathbb{Z}$-módulo, entonces $\cdot = *$.
Sea $\mathcal{A}$ la clase de los grupos abelianos. Las aplicaciones de $\mathcal{A}$ en $\mathfrak{M}(\mathbb{Z})$, $(G, +) \mapsto (G, +, *)$, y de $\mathfrak{M}(\mathbb{Z})$ en $\mathcal{A}$, $(M, +, *) \mapsto (M, +)$ son recíprocas.
iii) Endomorfismos de K-espacios vectoriales y $K[X]$-módulos.
Sea $(V, +, \cdot)$ un K-espacio vectorial, y sea t un endomorfismo de la estructura de K-espacio vectorial de V. Se define una acción $*$ de $K[X]$ en V en la forma siguiente. Dado $f \in K[X]$, $f = \sum_{0 \leq i \leq n} a_i X^i$, y $v \in V$, se toma

$$f * v = \sum_{0 \leq i \leq n} a_i \cdot t^i(v)$$

(esta definición es independiente de la escritura de f). Se verifica que $(V, +, *)$ es un $K[X]$-módulo y $*$ satisface

$$kX^0 * v = k \cdot v,$$
$$X * v = t(v),$$

(ejercicio).
Recíprocamente, sea $(M, +, \cdot)$ un $K[X]$-módulo. Se definen una acción $\circ$ de K en M y una aplicación $u\colon M \longrightarrow M$ por

$$k \circ x = kX^0 \cdot x,$$
$$u(x) = X \cdot x.$$

Se verifica que $(M, +, \circ)$ es un K-espacio vectorial y u es un endomorfismo de esa estructura (ejercicio).

Sea $\mathcal{E}$ la clase de K-espacios vectoriales provistos de endomorfismos. Las aplicaciones de $\mathcal{E}$ en $\mathfrak{M}(K[X])$, $(V,+,\cdot,t)\mapsto(V,+,*)$, y de $\mathfrak{M}(K[X])$ en $\mathcal{E}$, $(M,+,\cdot)\mapsto(M,+,\cdot,u)$ son recíprocas.

iv) Estructuras izquierda y derecha de un anillo.

Sea A un anillo. A puede considerarse como A-módulo a izquierda, en cuyo caso se nota A_s (estructura izquierda de A).

También, A puede considerarse como A-módulo a derecha, con la acción $aox = x\cdot a$ $(a,x\in A)$, en cuyo caso se nota A_d (estructura derecha de A). Notar que $A_d=((A^o)_s)^o$.

Si A es un anillo tal que todo A-módulo es nulo, entonces A es nulo.

v) Potencias de un módulo.

Sea M un A-módulo, y sea I un conjunto. Se definen $+$ y $\cdot$ para $M^I=\{f\,:\,f\colon M\}$ en la forma:

$$(f+g)(i)=f(i)+_M g(i)\ \ (i\in I),$$
$$(a\cdot f)(i)=a\cdot_M f(i)\ \ (i\in I).$$

Se verifica que $(M^I,+,\cdot)$ es una A-módulo. Una aplicación $f\colon I\longrightarrow M$ también se llama familia de elementos de M con índices en I. En tal caso, $f(i)$ se nota $f_i\,(i\in I)$; y f se representa por $(f_i)_{i\in I}$. Con esta notación, las definiciones de $+$ y $\cdot$ se escriben

$$(f_i)_{i\in I}+(g_i)_{i\in I}=(f_i+_M g_i)_{i\in I},$$
$$a\cdot(f_i)_{i\in I}=(a\cdot_M f_i)_{i\in I}.$$

Casos especiales: sucesiones, uplas y matrices. Aclaración: $M^\emptyset=\{\emptyset\}$ es nulo. Ejercicio: explicitar la estructura en los casos especiales.

Sea M un monoide, notado multiplicativamente. Dada una sucesión $(x_i)_{1\le i\le n}$ de elementos de M, se define $\prod_{1\le i\le n}x_i$ inductivamente por

$$\prod_{1\le i\le 1}x_i=x_1,\qquad \prod_{1\le i\le h+1}x_i=\left(\prod_{1\le i\le h}x_i\right)\cdot x_{h+1}\ (h\in\mathbb{N})$$

Si M está notado aditivamente (en cuyo caso, M es conmutativo), se escribe $\sum_{1\le i\le n}x_i$ en lugar de $\prod_{1\le i\le n}x_i$, con lo cual la definición dada toma la forma

$$\sum_{1\le i\le 1}x_i=x_1,\qquad \sum_{1\le i\le h+1}x_i=\left(\sum_{1\le i\le h}x_i\right)+x_{h+1}\ (h\in\mathbb{N}).$$

[Comentario: $\prod_{1\le i\le 4}x_i=((x_1\cdot x_2)\cdot x_3)\cdot x_4$; pero también puede asociarse $x_1\cdot(x_2\cdot(x_3\cdot x_4))$, $(x_1\cdot x_2)\cdot(x_3\cdot x_4)$, $(x_1\cdot(x_2\cdot x_3))\cdot x_4$, $x_1\cdot((x_2\cdot x_3)\cdot x_4)$.]

Si M es un semigrupo, la definición puede extenderse a $n=0$ poniendo $\prod_{1\le i\le 0}x_i=1$ ($\sum_{1\le i\le 0}=0$, si la notación es aditiva).

Se supone que M es un semigrupo.

Proposición 1.1. *$(j,n\in\mathbb{N}_0)$. Si $j\le n$, $\prod_{1\le i\le n}x_i=\prod_{1\le i\le j}x_i\cdot\prod_{1\le i\le n-j}x_{j+i}$.*

Demostración. Por inducción en n. El caso $n = 0$ es trivial ($1 = 1 \cdot 1$). Si $n = h + 1$, con $h \in \mathbb{N}_0$, como el caso $j = n$ también es trivial ($t = t \cdot 1$), puede suponerse $j < n$, o sea $j \leq h$. Luego,

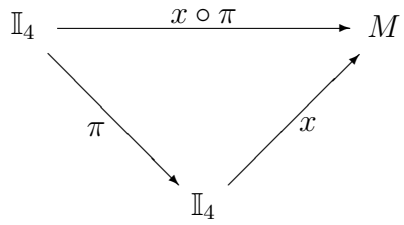
$$\prod_{1\leq i\leq h+1} x_i = \prod_{1\leq i\leq h} x_i \cdot x_{h+1} = \left(\prod_{1\leq i\leq j} x_i \cdot \prod_{1\leq i\leq h-j} x_{j+i}\right) \cdot x_{h+1}$$
$$= \prod_{1\leq i\leq j} x_i \cdot \left(\prod_{1\leq j\leq h-j} x_{j+i} \cdot x_{h+1}\right) = \prod_{1\leq i\leq j} x_i \cdot \prod_{1\leq i\leq (h-j)+1=(h+1)-j} x_{j+i}.\square$$

Se supone –además– que M es conmutativo y que está notado aditivamente.

Motivación: $x_1 + x_2 + x_3 + x_4 = x_3 + x_2 + x_4 + x_1$ se escribe $\sum_{1\leq i\leq 4} x_i = \sum_{1\leq i\leq 4}(x\pi)_i$, $x_3 + x_2 + x_4 + x_1 = x_{\pi(1)} + x_{\pi(2)} + x_{\pi(3)} + x_{\pi(4)} = (x\pi)_1 + (x\pi)_2 + (x\pi)_3 + (x\pi)_4$.

$$\begin{aligned} \pi\colon \mathbb{I}_4 &\longrightarrow \mathbb{I}_4 \\ 1 &\mapsto 3 \\ 2 &\mapsto 2 \\ 3 &\mapsto 4 \\ 4 &\mapsto 1 \end{aligned}$$

π es biyectiva



$x_{\pi(i)} = x(\pi(i)) = (x\pi)(i) = (x\pi)_i$.

Proposición 1.2. ($n \in \mathbb{N}_0$). *Si π es una permutación de grado n, $\sum_{1\leq i\leq n} x_i = \sum_{1\leq i\leq n}(x\pi)_i$.*

Demostración. Por inducción en n. El caso $n = 0$ es trivial ($0 = 0$). Suponiendo $n = h + 1$, con $h \in \mathbb{N}_0$, sea j el índice tal que $\pi(j) = n$, y sea τ la trasposición de j y n: $\tau(j) = n$, $\tau(n) = j$, $\tau(i) = i$ ($i \neq j, n$). Como $(\pi\tau)(n) = n$, $\pi\tau$ define una permutación ω de grado $n - 1 = h$: $\omega(i) = (\pi\tau)(i)$ ($1 \leq i \leq h$).

Luego, aplicando la hipótesis inductiva a ω;

$$\sum_{1\leq i\leq h+1} x_i = \sum_{1\leq i\leq h} x_i + x_{h+1} = \sum_{1\leq i\leq h} (x\omega)_i + x_{h+1} = \sum_{1\leq i\leq h} (x(\pi\tau))_i + (x(\pi\tau))_{h+1}$$
$$= \sum_{1\leq i\leq h+1} (x(\pi\tau))_i = \sum_{1\leq i\leq h+1} ((x\pi)\tau)_i = \sum_{1\leq i\leq h+1} (x\pi)_i,$$

por el siguiente

LEMA 1.3. $(j, n \in \mathbb{N})$. *si* $j \leq n$ *y* τ *es la trasposición de* j *y* n, $\sum_{1\leq i\leq n} x_i = \sum_{1\leq i\leq n}(x\tau)_i$.

Demostración. Por asociatividad,

$$\sum_{1\leq i\leq n} x_i = \sum_{1\leq i\leq j} x_i + \sum_{1\leq i\leq n-j} x_{j+i} = \left(\sum_{1\leq i\leq j-1} x_i + x_j\right) + \left(\sum_{1\leq i\leq n-j-1} x_{j+i} + x_n\right)$$
$$\overset{*)}{=} \left(\sum_{1\leq i\leq j-1} x_i + x_n\right) + \left(\sum_{1\leq i\leq n-j-1} x_{j+i} + x_j\right) = \left(\sum_{1\leq i\leq j-1} (x\tau)_i + (x\tau)_j\right)$$
$$+ \left(\sum_{1\leq i\leq n-j-1} x_{j+i} + (x\tau)_{j+(n-j)}\right) = \sum_{1\leq i\leq j} (x\tau)_i + \sum_{1\leq i\leq n-j} (x\tau)_i = \sum_{1\leq i\leq n} (x\tau)_i,$$

nuevamente por asociatividad.□

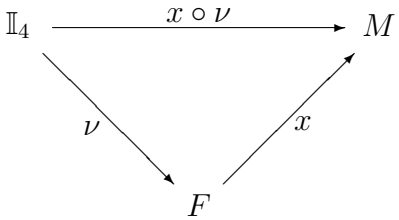
$[*)$ $(w + x) + (y + z) = w + (x + (y + z)) = w + ((y + z) + x) = w + ((z + y) + x) = w + (z + (y + x)) = (w + z) + (y + x).]$

Sea M un semigrupo conmutativo, notado aditivamente. Dada una familia finita $(x_i)_{i\in F}$ de elementos de M, se define $\sum_{i\in F} x_i = \cdots$

$[$ *Motivación*: $F = \{a, b, c, d\} \Longrightarrow \sum_{i\in F} x_i = x_c + x_b + x_d + x_a = x_{\nu(1)} + x_{\nu(2)} + x_{\nu(3)} + x_{\nu(4)} = (x\nu)_1 + (x\nu)_2 + (x\nu)_3 + (x\nu)_4 = \sum_{1\leq j\leq 4}(x\nu)_j$.

$$\begin{aligned} \pi\colon \mathbb{I}_4 &\xrightarrow{\nu} F \\ 1 &\mapsto c \\ 2 &\mapsto b \\ 3 &\mapsto d \\ 4 &\mapsto a \end{aligned}$$

ν es biyectiva



$x_{\nu(j)} = x(\nu(j)) = (x\nu)(j) = (x\nu)_j$

$\cdots \sum_{1\leq j\leq n}(x\nu)_j$, donde $\nu\colon \mathbb{I}_n \longrightarrow F$ es una numeración. ...

Motivación: $\sum_{i\in F} x_i = x_b + x_a + x_d + x_c = \sum_{1\leq j\leq 4}(x\nu')_j$.

$$\mathbb{I}_4 \xrightarrow{\nu'} F$$
$$1 \mapsto b,\ 2 \mapsto a,\ 3 \mapsto d,\ 4 \mapsto c$$

$$\pi\colon \mathbb{I}_4 \longrightarrow \mathbb{I}_4$$
$$1 \mapsto 3$$
$$2 \mapsto 2$$
$$3 \mapsto 4$$
$$4 \mapsto 1$$

π es biyectiva: $\pi = \nu^{-1} \circ \nu' \iff \nu \circ \pi = \nu'$

... Esta definición es correcta: si ν' es otra numeración de F, sea π la permutación de grado n tal que $\nu \circ \pi = \nu'$ (vale decir, $\pi = \nu^{-1} \circ \nu'$), con lo cual

$$\sum_{1\le j\le n} (x\nu)_j = \sum_{1\le j\le n} ((x\nu)\pi)_j = \sum_{1\le j\le n} (x(\nu\pi))_j = \sum_{1\le j\le n} (x\nu')_j.]$$

Aclaración: Un conjunto F se dice <u>finito</u> si y sólo si existen $n \in \mathbb{N}_0$ y una biyección $\nu\colon \mathbb{I}_n \longrightarrow F$. En tal caso, ν se llama <u>una</u> <u>numeración</u> de F; y n se dice <u>la</u> <u>cantidad</u> de elementos de F.
<u>la</u>: $\mu\colon \mathbb{I}_m \longrightarrow F$, $\nu\colon \mathbb{I}_n \longrightarrow F \rightsquigarrow \beta = \nu^{-1} \circ \mu\colon \mathbb{I}_m \longrightarrow \mathbb{I}_n$ biyección $\Longrightarrow m = n$. $\alpha\colon \mathbb{I}_m \longrightarrow \mathbb{I}_n$ inyección $\Longrightarrow m \le n$ (inducción en n).

Ahora, sea $(x_i)_{i\in I}$ una familia cualquiera de elementos de M.

Se llama <u>soporte</u> de $(x_i)_{i\in I}$ a $\operatorname*{sop}_{i\in I} x_i = \{i \in I : x_i \neq 0\}$.

Definición. Si el soporte de $(x_i)_{i\in I}$ es finito, se toma $\sum_{i\in I} x_i = \sum_{i\in F} x_i$, donde $F = \operatorname*{sop}_{i\in I} x_i$.

Ejercicio: Esta definición es consistente con la anterior: si I es finito, $\sum_{i\in I} x_i = \sum_{i\in F} x_i$.

Observación. Si J es un conjunto tal que $F \subseteq J \subseteq I$, entonces $\sum_{i\in I} x_i = \sum_{i\in J} x_i$.

$$J \subseteq I \Longrightarrow \operatorname*{sop}_{i\in J} x_i = F \cap J.\ \therefore\ F \subseteq J \Longrightarrow \operatorname*{sop}_{i\in J} x_i = F.$$

Ejemplo. Sea M un A-módulo. Si $a \in A$ y $(x_i)_{i\in I}$ es una familia de elementos de M con soporte finito, entonces $a \cdot \sum_{i\in I} x_i = \sum_{i\in I} a \cdot x_i$.

Sea $F = \operatorname{sop}_{i\in I} x_i$, de modo que $a \cdot \sum_{i\in I} x_i = a \cdot \sum_{i\in F} x_i$, por la definición. Por otra parte, $\operatorname{sop}_{i\in I} a \cdot x_i \subseteq F : a \cdot x_i \neq 0 \Longrightarrow x_i \neq 0$ (esto es equivalente a $x_i = 0 \Longrightarrow a \cdot x_i = 0$). Por lo tanto, $\operatorname{sop}_{i\in I} a \cdot x_i$ es finito, con lo cual está definida $\sum_{i\in I} a \cdot x_i$; y por la observación, $\sum_{i\in I} a \cdot x_i = \sum_{i\in F} a \cdot x_i$. Luego, lo que debe probarse es que $a \cdot \sum_{i\in F} x_i = \sum_{i\in F} a \cdot x_i$,

o sea, puede suponerse que I es un conjunto finito. En tal caso, dada una numeración $\nu\colon \mathbb{I}_n \longrightarrow I$, $a \cdot \sum_{i\in I} x_i = a \cdot \sum_{1\le j\le n}(x\nu)_j$ y $\sum_{i\in I} a\cdot x_i = \sum_{1\le j\le n} a\cdot(x\nu)_j$. Por lo tanto, lo que debe probarse es que $a \cdot \sum_{1\le j\le n}(x\nu)_j = \sum_{1\le j\le n} a\cdot(x\nu)_j$, vale decir, puede suponerse que $I = \mathbb{I}_n$, para algún $n \in \mathbb{N}_0$. En tal caso, se procede por inducción. Lo propuesto es trivial para $n = 0 : a\cdot 0 = 0$. Si $n = h+1$, con $h \in \mathbb{N}_0$,

$$a\cdot \sum_{1\le i\le h+1} x_i = a\cdot\left(\sum_{1\le i\le h} x_i + x_{h+1}\right) = a\cdot \sum_{1\le i\le h} x_i + a\cdot x_{h+1} = \sum_{1\le i\le h} a\cdot x_i + a\cdot x_{h+1} = \sum_{1\le i\le h+1} a\cdot x_i.$$

Ejercicio. En un A-módulo M, se verifica que $(\sum_{i\in I} a_i)\cdot\left(\sum_{j\in J} x_j\right) = \sum_{\substack{i\in I\\ j\in J}} a_i\cdot x_j$ (suponiendo que $\operatorname{sop}_{i\in I} a_i$ y $\operatorname{sop}_{j\in J} x_j$ son finitos).

En particular, $a\cdot\sum_{j\in J} x_j = \sum_{j\in J} a\cdot x_j$ y $(\sum_{i\in I} a_i)\cdot x = \sum_{i\in I} a_i\cdot x$. (Aclaraciones; entre ellas, $\operatorname{sop}_{\substack{i\in I\\ j\in J}} a_i\cdot x_j \subseteq \operatorname{sop}_{i\in I} a_i \times \operatorname{sop}_{j\in J} x_j$.)

2. Morfismos. Submódulos

Definición. Dados A-módulos M y N, un morfismo (también, homomorfismo o aplicación lineal) de M en N es una aplicación $f\colon M \longrightarrow N$ que verifica:

$$\begin{aligned} &i)\ f(x +_M y) = f(x) +_N f(y) \qquad (f \text{ es aditiva}).\\ &ii)\ f(a\cdot_M x) = a\cdot_N f(x) \qquad (f \text{ es activa}). \end{aligned}$$

Observación. En tal caso, f satisface:

$$\begin{aligned} &i)\ f(0) = 0.\\ &ii)\ f(-x) = -f(x).\\ &iii)\ f\left(\sum_{i\in I} a_i\cdot x_i\right) = \sum_{i\in I} a_i\cdot f(x_i),\ \text{suponiendo que } \operatorname*{sop}_{i\in I} a_i\cdot x_i \text{ es finito.} \end{aligned}$$

Ejemplos. i) Transformaciones lineales de espacios vectoriales.

Dado un cuerpo K, "morfismo de K-módulos" es lo mismo que "transformación lineal de K-espacios vectoriales".

ii) Morfismos de grupos abelianos.

Convención. Los grupos se suponen abelianos y notados aditivamente.

Definición. Dados grupos G y H, un morfismo de G en H es una aplicación $f\colon G \longrightarrow H$ que verifica:

$$f(x +_G y) = f(x) +_H f(y)$$

[Una aplicación $f\colon G \longrightarrow H$ es un morfismo de grupos si, y sólo si f es un morfissmo de $\mathbb{Z}$-módulos.

Suficiencia. Es trivial y general: dado un morfismo de A-módulos $f\colon M \longrightarrow N$, f resulta un morfismo de grupos.

Necesidad. $f(m \cdot x) = m \cdot f(x)$ $(m \in \mathbb{Z},\ x \in G)$.]

iii) Morfismos de $K[X]$-módulos (K cuerpo).

Sean V y W K-espacios vectoriales provistos de endomorfismos t y u. Una aplicación $f\colon V \longrightarrow W$ es un morfismo de $K[X]$-módulos si, y sólo si, f es una transformación lineal de K-espacios vectoriales tal que $f \circ t = u \circ f$.

iv) Morfismos nulos

$$f\colon M \longrightarrow N, \qquad f(x) = 0 \ \ (x \in M).$$

f se nota $0_{M,N}$ (morfismo nulo de M en N); $0_{M,N}$ se escribe 0_M.

v) Identidades.

$$f\colon M \longrightarrow M, \qquad f(x) = x \ \ (x \in M)$$

f se nota i_M (morfismo identidad de M).

$i_M = 0_M \Longleftrightarrow M = 0$ (abuso de notación: debería escribirse $M = \{0\}$).

vi) Homotecias

$$A \times M \longrightarrow M, \qquad (a, x) \mapsto a \cdot x.$$

Sea $c \in A$. $f\colon M \longrightarrow M$, $f(x) = c \cdot x$ $(x \in M)$. f se nota $\eta_{C,M}$ (homotecia de c en M) 0 η_c.

$\eta_{c,M}$ es aditiva.

$\eta_{c,M}$ es activa (para todo A-módulo M) si, y sólo si, $a \cdot c = c \cdot a$ $(a \in A)$.

Definición. Dado un anillo A, se llama centro de A a $C(A) = \{c \in A : a \cdot c = c \cdot a \ (a \in A)\}$.

Observación. 1) $C(A) = A \Longleftrightarrow A$ es conmutativo.

2) La suma y el producto de A definen operaciones en $C(A)$, que la convierten en un anillo (conmutativo, de modo que $C(C(A)) = C(A)$).

$\eta_{c,M}$ es un morfismo de grupos.

$\eta_{c,M}$ es un morfismo de A-módulos (para todo A-módulo M) si, y sólo si, $c \in C(A)$.

vii) Expansiones.

Sea $z \in M$. $f\colon A \longrightarrow M$, $f(a) = a \cdot z$ $(a \in A)$. f se nota ε_z (expansión de z). ε_z es un morfismo de A_s en M y $\varepsilon_z(1) = z$.

Si $f\colon A_s \longrightarrow M$ es un morfismo tal que $f(1) = z$, entonces $f = \varepsilon_z$. (Han quedado determinados todos los morfismos de A_s en M.)

Observación. Dados morfismos de A-módulos $f\colon M \longrightarrow N$ y $g\colon N \longrightarrow P$, la aplicación $g \circ f\colon M \longrightarrow P$ también es un morfismo.

Definiciones. Sean M y N A-módulos.

Un monomorfismo de M en N es un morfismo de M en N inyectivo.

Un epimorfismo de M en N es un morfismo de M en N suryectivo.

Un isomorfismo de M en N es un morfismo de M en N biyectivo.

Una sección de M en N es un morfismo $f\colon M \longrightarrow N$ tal que existe un morfismo $g\colon N \longrightarrow M$ verificando que $g \circ f = i_M$.

Una retracción de M en N es un morfismo $f\colon M \longrightarrow N$ tal que existe un morfismo $g\colon N \longrightarrow M$ verificando que $f \circ g = i_N$.

Un endomorfismo de M es un morfismo de M en M.

Un automorfismo de M es un morfismo de M en M biyectivo.

Observación. i) Toda sección (retracción) es un monomorfismo (epimorfismo). La recíproca es cierta para espacios vectoriales (en realidad, para módulos libres).

ii) La composición de dos morfismos de una misma clase es un morfismo de esa clase.

PROPOSICIÓN 2.1. *Dado un morfismo de A-módulos $f\colon M \longrightarrow N$, son equivalentes:*

i) f es un isomorfismo.

ii) Existe un morfismo $g\colon N \longrightarrow M$ verificando que $g \circ f = i_M$ y $f \circ g = i_N$.

iii) f es una sección y una retracción.

iv) f es un monomorfismo y un epimorfismo.

Además, si f es un isomorfismo, g en ii) es único; se llama el morfismo inverso de f y se nota f^{-1}.

Demostración. i) $\Longrightarrow$ ii) Repaso: que f sea biyectiva puede traducirse como

$$\forall\, y \in N, \quad \exists!\, x \in M : \ f(x) = y.$$

En tal caso, se define $g\colon N \longrightarrow M$ tomando $g(y) = x$, si $f(x) = y$; y se verifica que $g \circ f = i_M$ y $f \circ g = i_N$.

Aquí, g resulta aditiva. En efecto, dados $y, y' \in N$, sean $x, x' \in M$ tales que $f(x) = y$ y $f(x') = y'$, de modo que $g(y) = x$ y $g(y') = x'$. Como $f(x + x') = f(x) + f(x') = y + y'$, se tiene que $g(y + y') = x + x' = g(y) + g(y')$.

También g es activa. Dado $a \in A$, $f(a \cdot x) = a \cdot f(x) = a \cdot y$, con lo cual $g(a \cdot y) = a \cdot x = a \cdot g(y)$.

ii) $\Longrightarrow$ iii) $\Longrightarrow$ iv) $\Longrightarrow$ i) son triviales.$\square$

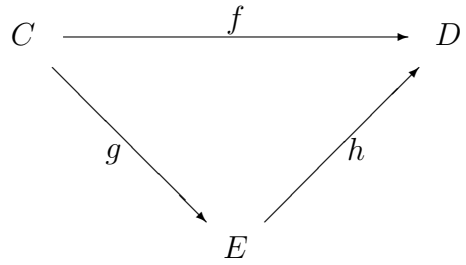
La observación final es conocida a nivel conjuntista.

Definición. Sean M y N A-módulos. Se dice que M es isomorfo a N, notado $M \simeq N$, si y sólo si existe un isomorfismo de M en N.

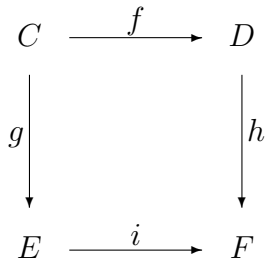
Observación. La relación así definida en $\mathfrak{M}_s(A)$ es una relación de equivalencia:

$$r)\ M \simeq M.$$
$$s)\ M \simeq N \Longrightarrow N \simeq M.$$
$$t)\ M \simeq N \ \wedge\ N \simeq P \Longrightarrow M \simeq P.$$

Diagramas conmutativos:

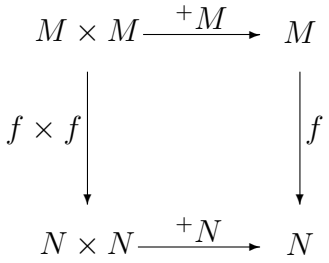


$g = h \circ f$.



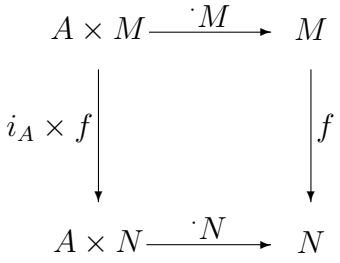
$h \circ f = i \circ g$.

Ejemplo. Dados A-módulos M y N y una aplicación $f\colon M \longrightarrow N$, se verifica:
i) f es aditiva si, y sólo si, el diagrama



es conmutativo.

ii) f es activa si, y sólo si el diagrama



es conmutativo.

Definición. Sean M y N A-módulos. Se dice que M es un submódulo de N si, y sólo si, $M \subseteq N$ y se verifica:

$$i)\, x, y \in M \Longrightarrow x +_M y = x +_N y.$$
$$ii)\, a \in A \wedge x \in M \Longrightarrow a \cdot_M x = a \cdot_N x,$$

vale decir, la inclusión $i_{M,N} \colon M \longrightarrow N$ es un morfismo de A-módulos.

Observación. Dado un morfismo de A-módulos $f \colon M \longrightarrow N$, si S es un submódulo de M, entonces $f|_S \colon S \longrightarrow M$ también es un morfismo.

Proposición 2.2. *Sea M un A-módulo. Para un subconjunto S de M, son equivalentes:*

i) S satisface:

$$1)\, S \neq \emptyset.$$
$$2)\, x, y \in S \Longrightarrow x + y \in S.$$
$$3)\, a \in A \wedge x \in S \Longrightarrow a \cdot x \in S.$$

ii) S satisface:

$$1')\, 0 \in S.$$
$$2)\, x, y \in S \Longrightarrow x + y \in S.$$
$$3)\, a \in A \wedge x \in S \Longrightarrow a \cdot x \in S.$$

iii) S "es" (esto significa: admite una estructura de A-módulo, necesariamente única, que lo convierte en) un submódulo de M.

iv) S satisface:

$$a_i \in A \wedge x_i \in S\ (i \in I) \Longrightarrow \sum_{i \in I} a_i \cdot x_i \in S$$

(suponiendo que $\operatorname{sop}_{i \in I} a_i \cdot x_i$ es finito).

Demostración. i) $\Longrightarrow$ ii). En virtud de 1'), puede tomarse $x \in S$; y aplicando 3), $0 = 0 \cdot x \in S$.

ii) $\Longrightarrow$ iii). La unicidad de la estructura es clara. En cuanto a la existencia, se definen $+_S$ y $\cdot_S$ en la forma:

$$x, y \in S \Longrightarrow x +_S y = x + y \text{ (esta definición es correcta por 2)),}$$
$$a \in A \wedge x \in S \Longrightarrow a \cdot_S x = a \cdot x \text{ (esta definición es correcta por 3)).}$$

Se verifica que $(S, +_S, \cdot_S)$ es un A-módulo:

Es claro que $+_S$ es asociativa y conmutativa. En virtud de 1'), 0 es elemento neutro de $+_S$. Todo $x \in S$ es inversible respecto de $+_S$, porque, aplicando 3), $-x = (-1) \cdot x \in S$. Finalmente, $\cdot_S$ hereda las propiedades de la definición de módulo de $\cdot$

iii) $\Longrightarrow$ iv). Si $f\colon S \longrightarrow M$ es la inclusión; $\sum_{i\in I} a_i \cdot f(x_i) = f\left(\sum_{i\in I}^{S} a_i \cdot_S x_i\right) \in \mathrm{Im} f = S$.

iv) $\Longrightarrow$ i). 1') Tomando $I = \emptyset$, $\sum_{i\in I} a_i \cdot x_i = 0$, con lo cual $0 \in S$.

2) Tomando $I = \{1, 2\}$, $a_1 = a_2 = 1$, $x_1 = x$, $x_2 = y$, $\sum_{i\in I} a_i \cdot x_i = x + y$.

3) Tomando $I = \{1\}$, $a_1 = a$, $x_1 = x$, $\sum_{i\in I} a_i \cdot x_i = a \cdot x$.

Ejemplos.

• i) Subespacios de un espacio vectorial.

Dado un K-espacio vectorial V, "submódulo de V" es lo mismo que "subespacio de V" (eventualmente, porque iii) $\Longleftrightarrow$ ii) o iii) $\Longleftrightarrow$ i), en la Proposición).

• ii) Subgrupos de un grupo abeliano.

Sean G y H grupos.

Definición. Se dice que G es un subgrupo de H si y sólo si, $G \subseteq H$ y se verifica:

$$x, y \in G \Longrightarrow x +_G y = x +_H y,$$

vale decir, $I_{G,H}\colon G \longrightarrow H$ es un morfismo de grupos.

Se tiene que G es un subgrupo de H si, y sólo si, G es un submódulo de H (porque "morfismo de grupos" es lo mismo que "morfismo de $\mathbb{Z}$-módulos").

En general, dados A-módulos M y N, si M es un submódulo de N, entonces M es subgrupo de N (porque un morfismo de A-módulos es un morfismo de grupos).

[*Ejercicio.* Sea G un grupo. Para un subconjunto S de G, son equivalentes:

i) S satisface:

$$\begin{aligned} &1)\ S \neq \emptyset.\\ &2)\ x, y \in S \Longrightarrow x + y \in S.\\ &3)\ x \in S \Longrightarrow -x \in S. \end{aligned}$$

ii) S satisface:

$$\begin{aligned} &1')\ 0 \in S.\\ &2)\ x, y \in S \Longrightarrow x + y \in S.\\ &3)\ x \in S \Longrightarrow -x \in S. \end{aligned}$$

iii) S "es" (esto significa: admite una estructura de grupo, necesariamente única, que lo convierte en) un subgrupo de G.

iv) S satisface:

$$\begin{aligned} &1)\ S \neq \emptyset.\\ &2')\ x, y \in S \Longrightarrow x - y \in S. \qquad \textit{Notación}\colon\ x - y = x + (-y). \end{aligned}$$

v) S satisface:

$$\begin{aligned} &1')\ 0 \in S.\\ &2')\ x, y \in S \Longrightarrow x - y \in S. \qquad \textit{Notación}\colon\ x - y = x + (-y).] \end{aligned}$$

• iii) Submódulos de un $K[X]$-módulo (K cuerpo).

Sea V un K-espacio vectorial provisto de un endomorfismo t. Un subconjunto S de V es un submódulo de V si, y sólo si, S es un subespacio de V que satisface: $v \in S \Longrightarrow t(v) \in S$.

• iv) Ideales de un anillo.

Sea A un anillo.

Definición. Un <u>ideal</u> a izquierda (derecha) de A es un subconjunto $\mathfrak{A}$ de A que verifica:

$$1)\, 0 \in \mathfrak{A}.$$
$$2)\, x, y \in \mathfrak{A} \Longrightarrow x + y \in \mathfrak{A}.$$
$$3)\, a \in A \wedge x \in \mathfrak{A} \Longrightarrow a \cdot x \in \mathfrak{A} \quad (x \cdot a \in \mathfrak{A}).$$

Observación. $\mathfrak{A}$ es un ideal a izquierda (derecha) de A si, y sólo si, $\mathfrak{A}$ es un submódulo de A_s (A_d).

Definición. Un ideal <u>bilátero</u> de A es un ideal a izquierda y a derecha.

Observación. 1) Todo ideal (a izquierda, a derecha o bilátero) de A es un subgrupo de A.

2) Si A es conmutativo, las tres nociones de ideal coinciden.

3) La recípreca de 1) no es cierta: dado $n \in \mathbb{N}_0$, $K[X]_n$ no es un ideal de $K[X]$ (todo ideal no nulo de $K[X]$ contiene polinomios de grado arbitrariamente grande).

Convención. Los ideales se suponen a izquierda.

Ejercicios. Sea M un A-módulo.

i) Si $\mathfrak{A}$ es un subgrupo (ideal) de A y $x \in M$, $\mathfrak{A} \cdot x = \{a \cdot x : a \in \mathfrak{A}\}$ es un subgrupo (submódulo) de M.

• v) Subgrupos de $\mathbb{Z}$.

Notar que "subgrupo de $\mathbb{Z}$" es lo mismo que "ideal de $\mathbb{Z}$".

1) Si $m \in \mathbb{Z}$, $m\mathbb{Z} = \{n \in \mathbb{Z} : m|n\}$ es un subgrupo de $\mathbb{Z}$ (por el ejercicio) $m\mathbb{Z} \subseteq n\mathbb{Z} \Longleftrightarrow m \in n\mathbb{Z} \Longleftrightarrow n|m$. $\therefore m\mathbb{Z} = n\mathbb{Z} \Longleftrightarrow |m| = |n|$.

2) Si $m, n \in \mathbb{N}_0$ y $m\mathbb{Z} = n\mathbb{Z}$, entonces $m = n$.

3) Si S es un subgrupo de $\mathbb{Z}$, existe $n \in \mathbb{N}_0$ tal que $S = n\mathbb{Z}$. Si $S = 0$, basta tomar $n = 0$. Suponiendo $S \neq 0$, se tiene que $S \cap \mathbb{N} \neq \emptyset$ (se toma $x \in S, x \neq 0$; si $x > 0$, ya está; si $x < 0, -x > 0$ y $-x \in S$). Sea, entonces, $n = min S \cap \mathbb{N}$.

$n\mathbb{Z} \subseteq S$, pues $n \in S$.

$S \subseteq n\mathbb{Z}$: Dado $x \in S$, sea $x = nq + r$, con $q, r \in \mathbb{Z}$ y $0 \leq r < n$. Como $r = x - nq \in S$, $r \neq 0$ contradice la minimalidad de n, de modo que debe ser $r = 0$.

En resumen, la aplicación de $\mathbb{N}_0$ en el conjunto de subgrupos de $\mathbb{Z}$ $n \mapsto n\mathbb{Z}$ es biyectiva, lo que se expresa diciendo que $(n\mathbb{Z})_{n \in \mathbb{N}_0}$ es una numeración de los subgrupos de $\mathbb{Z}$.

• vi) Ideales de $K[X]$ (K cuerpo).

1) Si $f \in K[X]$, $fK[X] = \{g \in K[X] : f|g\}$ es un ideal de $K[X]$. $fK[X] \subseteq gK[X] \Longleftrightarrow g|f$. $\therefore fK[X] = gK[X] \Longleftrightarrow \exists\, c \in K (c \neq 0) : c \cdot f = g$.

2) Sea $M = \{f \in K[X] : f \text{ es mónico o } f = 0\}$. Si $f, g \in M$ y $fK[X] = gK[X]$, entonces $f = g$.

3) Si $\mathfrak{A}$ es un ideal de $K[X]$, existe $f \in M$ tal que $\mathfrak{A} = fK[X]$. Por lo tanto, $(fK[X])_{f \in M}$ es una numeración de los ideales de $K[X]$.

• vii) Copotencias de un módulo.

Si M es un A-módulo e I es un conjunto, $M^{(I)} = \{x \in M^I : \operatorname{sop} x \text{ es finito}\}$ es un submódulo de M^I, llamado <u>copotencia</u> I de M.

.) $\operatorname{sop} 0 = \emptyset$.

..) $x, y \in M^I \Longrightarrow \operatorname{sop}(x + y) \subseteq \operatorname{sop} x \cup \operatorname{sop} y$.

...) $a \in A \wedge x \in M^I \ \operatorname{sop}(a \cdot x) \subseteq \operatorname{sop} x$.

• viii) Módulos simples.

Dado un A-módulo M, $\{0\}$ y M son submódulos de M.

Definición. Un A-módulo M se dice <u>simple</u> si, y sólo si, M tiene exactamente dos submódulos, vale decir, se verifica:

1) $M \neq 0$.

2) Si S es un submódulo de M y $S \neq 0$, entonces $S = M$.

Ejercicio. Un K-espacio vectorial V es simple si, y sólo si, $\dim_K V = 1$.

Observación. Un A-módulo M es simple si, y sólo si, $M \neq 0$ y para todo $x \in M$, $x \neq 0$, se verifica que $A \cdot x = M$.

Ejercicio. A_s es simple si, y sólo si, A es un anillo de división.

Definición. Sea M un A-módulo. Un submódulo S de M se dice <u>minimal</u> si, y sólo si:

1) $S \neq 0$.

2) Si T es un submódulo $\neq 0$ de M y $T \subseteq S$, entonces $T = S$.

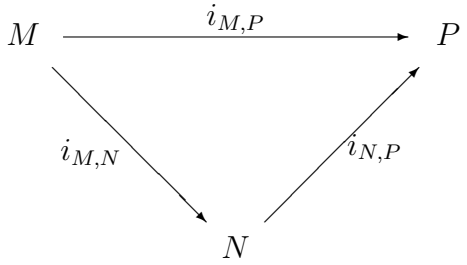
Observación. S es un submódulo minimal si, y sólo si, S es un módulo simple.

[*Necesidad.* Sea T un submódulo $\neq 0$ de S. Como T resulta un submódulo de $M^{*)}$ y $T \subseteq S$, se concluye que $T = S$.

Suficiencia. Sea T un submódulo $\neq 0$ de M tal que $T \subseteq S$. Como T resulta un submódulo de $S^{**)}$, se deduce que $T = S$.

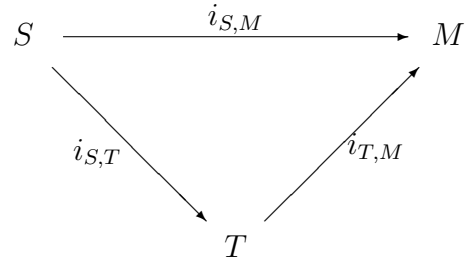
$*$) Sean M, N y P A-módulos. Si M es un submódulo de N y N es un submódulo de P, entonces M es un submódulo de P.

$$M \subseteq N \wedge N \subseteq P \Longrightarrow M \subseteq P.$$



$i_{N,P} \circ i_{M,N} = i_{M,P}$ por lo que $i_{M,P}$ sale morfismo.

$**$) Sea M un A-módulo, y sean S y T submódulos de M. Si $S \subseteq T$, entonces S es un submódulo de T



$i_{T,M} \circ i_{S,T} = i_{S,M}$.]

Definición. Dado un morfismo de A-módulos $f\colon M \longrightarrow N$, se llama <u>núcleo</u> de f a $\operatorname{Ker} f = \{x \in M : f(x) = 0\}$; y se llama <u>imagen</u> de f a $\operatorname{Im} f = \{y \in N : \exists\, x \in M : f(x) = y\}$.

Observación. i) $\operatorname{Ker} f$ e $\operatorname{Im} f$ son submódulos de M y N.

ii) Si T es un submódulo de N tal que $\operatorname{Im} f \subseteq T$, entonces $f|^T\colon M \longrightarrow T$ es un morfismo.

iii) f es un monomorfismo (epimorfismo) si, y sólo si, $\operatorname{Ker} f = 0$ ($\operatorname{Im} f = N$).

Repaso conjuntista: Sea $f\colon M \longrightarrow N$ un aplicación de conjuntos

$S \subseteq M \Longrightarrow f(S) = \{y \in N : \exists\, x \in S : f(x) = y\}$ (<u>imagen directa</u> de S por f). Por ejemplo: $f(M) = \operatorname{Im} f$.

$T \subseteq N \Longrightarrow f^{-1}(T) = \{x \in M : f(x) \in T\}$ (<u>imagen inversa</u> de T por f). Por ejemplo, si f es un morfismo de A-módulos, $f^{-1}(\{0\}) = \operatorname{Ker} f$. Si f es biyectiva y g es su aplicación inversa, entonces $f^{-1}(T) = g(T)$, de modo que la notación no es ambigua.

Nota. i) Dado un A-módulo M, $\sigma(M)$ nota el conjunto de los submódulos de M.

ii) Dado un morfismo de A-módulos $f\colon M \longrightarrow N$, $\sigma_f(M) = \{S \in \sigma(M) : S \supseteq \operatorname{Ker} f\}$.

Observación. Para un morfismo de A-módulos $f\colon M \longrightarrow N$, se verifica:

i) $S \in \sigma(M) \Longrightarrow f(S) \in \sigma(N)$.

ii) $T \in \sigma(N) \Longrightarrow f^{-1}(T) \in \sigma_f(M)$.

PROPOSICIÓN 2.2. *Dado un morfismo de A-módulos* $f\colon M \longrightarrow N$, *se consideran las aplicaciones* $f_*\colon \sigma(M) \longrightarrow \sigma(N)$, $S \mapsto f(S)$; $f^*\colon \sigma(N) \longrightarrow \sigma(M)$, $T \mapsto f^{-1}(T)$; $f_0\colon \sigma_f(M) \longrightarrow \sigma(N)$, $f_0 = f_*|_{\sigma_f(M)}$; $f^0\colon \sigma(N) \longrightarrow \sigma_f(M)$, $f^0 = f^*|^{\sigma_f(M)}$. *Entonces, se verifica:*

i) f_*, f^*, f_0 *y* f^0 *son morfismos de orden, respecto de la inclusión.*

ii) $f^0 \circ f_0 = i_{\sigma_f(M)}$.

iii) Si f *es un epimorfismo* $f_* \circ f^* = f_0 \circ f^0 = i_{\sigma(N)}$.

Demostración. i) significa para f_* y f_0:

$$S, S' \in \sigma(M) \wedge S \subseteq S' \Longrightarrow f(S) \subseteq f(S');$$

y para f^* y f^0:

$$T, T' \in \sigma(N) \wedge T \subseteq T' \Longrightarrow f^{-1}(T) \subseteq f^{-1}(T').$$

Ambas implicaciones son conjuntistas.

ii) quiere decir:

$$S \in \sigma_f(M) \Longrightarrow f^{-1}(f(S)) = S.$$

$\supseteq$ es conjuntista. Para $\subseteq$,

$$x \in f^{-1}(f(S)) \Longrightarrow f(x0 \in f(S) \Longrightarrow \exists\, y \in S : f(x) = f(y) \Longrightarrow f(x-y) = 0$$
$$\Longrightarrow x - y \in S \Longrightarrow x = (x-y) + y \in S.$$

iii) significa:

$$T \in \sigma(N) \Longrightarrow f(f^{-1}(T)) = T.$$

Esto es conjuntista: $\subseteq$ vale siempre y $\supseteq$ cuando f es suryectiva. $\square$

COROLARIO 2.3. *i) Si* f *es un epimorfismo,* f_0 *y* f^0 *son morfismos de orden recíprocos.*

ii) Si f *es un isomorfismo,* f_* *y* f^* *son morfismos de orden recíprocos.*

Demostración. i) es claro, por la Proposición.

ii) Como f es un monomorfismo, $\sigma_f(M) = \sigma(M)$, de modo que $f_0 = f_*$ y $f^0 = f_*$; y como f es un epimorfismo, se aplica i). $\square$

PROPOSICIÓN 2.4. *Dados A-módulos* M *y* N, *el conjunto* $\mathrm{Hom}_A(M,N)$ *de todos los morfismos de* M *en* N *es un submódulo de* N^M, *considerado éste como* $C(A)$*-módulo.*

Demostración. i) $0 \in \mathrm{Hom}_A(M,N)$, pues $0 = 0_{M,N}$.

ii) $f, g \in \mathrm{Hom}_A(M,N)$

$$\Longrightarrow f + g \in \mathrm{Hom}_A(M,N) : \begin{cases} (f+g)(x+y) = (f+g)(x) + (f+g)(y), \\ (f+g)(a \cdot x) = a \cdot (f+g)(x). \end{cases}$$

iii) $c \in C(A)$ y $f \in \mathrm{Hom}_A(M,N)$

$$\Longrightarrow c \cdot f \in \mathrm{Hom}_A(M,N) : \begin{cases} (c \cdot f)(x+y) = (c \cdot f)(x) + (c \cdot f)(y), \\ (c \cdot f)(a \cdot x) = a \cdot (c \cdot f)(x). \end{cases}$$

Ejemplos. i) $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q},\mathbb{Z}) = 0$. En particular, $i_{\mathbb{Z},\mathbb{Q}}$ no es una sección. Debe probarse que, dado un morfismo $f\colon \mathbb{Q} \longrightarrow \mathbb{Z}$, se tiene que $f(x) = 0$ $(x \in \mathbb{Q})$. Se usará que, dado $a \in \mathbb{Z}$,

$$m|a \ (m \in \mathbb{Z}, m \neq 0) \Longrightarrow a = 0.$$

(Suponiendo $a \neq 0$, resulta $|m| \leq |a|$ $(m \in \mathbb{Z}, m \neq 0) : \mathbb{N}$ tiene máximo). Dado $x \in \mathbb{Q}$, si $m \in \mathbb{Z}$ y $m \neq 0$, $f(x) = f(m \cdot (m^{-1} \cdot x)) = m \cdot f(m^{-1} \cdot x)$, pues la acción de $\mathbb{Z}$ en $\mathbb{Q}$ está dada por el producto de $\mathbb{Q}$, por razones de unicidad.

Si existe un morfismo $f\colon \mathbb{Q} \longrightarrow \mathbb{Z}$ tal que $f \circ i_{\mathbb{Z},\mathbb{Q}} = f|_{\mathbb{Z}} = i_{\mathbb{Z}}$, como debe ser $f = 0_{\mathbb{Q},\mathbb{Z}}$, se tiene que $0_{\mathbb{Z}} = i_{\mathbb{Z}}$, o sea $\mathbb{Z} = 0$.

ii) $\mathrm{Hom}_A(A_s, M) \simeq M$, no sólo como $C(A)$-módulos, sino como A-módulos. En particular, $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z},\mathbb{Q}) \simeq \mathbb{Q}$. $\mathrm{Hom}_A(A_s, M)$ puede considerarse como A-módulo, con la acción

$$(a \cdot f)(b) = f(b \cdot a) \ \ (b \in A),$$

que está bien definida

$$(a \cdot f) \in \mathrm{Hom}_A(A_s, M) : \begin{cases} (a \cdot f)(b+c) = (a \cdot f)(b) + (a \cdot f)(c), \\ (a \cdot f)(b \cdot c) = b \cdot (a \cdot f)(c). \end{cases}$$

y que extiende a la acción de $C(A)$

$$c \in C(A) \Longrightarrow (c \cdot f)(a) = c \cdot f(a) \ \ (a \in A).$$

Se define una aplicación $\varphi\colon \mathrm{Hom}_A(A_s, M) \longrightarrow M$ tomando $\varphi(f) = f(1)$. φ es un morfismo de A-módulos.

φ es biyectiva, pues tiene por inversa la aplicación $\varepsilon\colon M \longrightarrow \mathrm{Hom}_A(A_s, M)$, $x \mapsto \varepsilon_x$.

iii) $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q},\mathbb{Q}) \simeq \mathbb{Q}$ (ejercicio).

iv) Dual de un módulo.

Definición. Si M es un A-módulo a izquierda (derecha), se llama dual de M, que se nota M^*, al A-módulo a derecha (izquierda) que se obtiene considerando al grupo $\mathrm{Hom}_A(M, A_s)$ $(\mathrm{Hom}_A(M, A_d))$ provisto de la acción

$$(f \cdot a)(x) = f(x) \cdot a \ \ (x \in M) \qquad ((a \cdot f)(x) = a \cdot f(x) \ \ (x \in M)).$$

Notar que esta acción está bien definida

$$(f \cdot a) \in \mathrm{Hom}_A(M, A_s) : \begin{cases} (f \cdot a)(x+y) = (f \cdot a)(x) + (f \cdot a)(y), \\ (f \cdot a)(b \cdot x) = b \cdot (f \cdot a)(x). \end{cases}$$

y que extiende a la acción de $C(A)$

$$c \in C(A) \Longrightarrow (f \cdot c)(x) = c \cdot f(x) \ \ (x \in M).$$

Se define una aplicación $\gamma\colon M \longrightarrow M^{**}$ tomando $\gamma(x)(f) = f(x)$ $(x \in M, f \in M^*)$. γ está bien definida, o sea, $\gamma(x)\colon M^* \longrightarrow A_d$ es un morfismo de A-módulos a derecha. $(x \in M)$:

$$\begin{aligned} \gamma(x)(f+g) &= \gamma(x)(f) + \gamma(x)(g), \\ \gamma(x)(f \cdot a) &= \gamma(x)(f) \cdot a. \end{aligned}$$

γ es un morfismo de A-módulos a izquierda:

$$\begin{aligned} \gamma(x+y) = \gamma(x) + \gamma(y) &\Longleftrightarrow \gamma(x+y)(f) = (\gamma(x) + \gamma(y))(f) \ \ (f \in M^*), \\ \gamma(a \cdot x) = a \cdot \gamma(x) \qquad &\Longleftrightarrow \ \gamma(a \cdot x)(f) = (a \cdot \gamma(x))(f) \ \ (f \in M^*). \end{aligned}$$

$\operatorname{Ker}\gamma = \{x \in M \,:\, f(x) = 0 \ (f \in M^*)\}$.

Definición. Un A-módulo M se dice reflexivo si y sólo si, γ es un isomorfismo.

Ejemplo. Los espacios vectoriales de dimensión finita son reflexivos.

Observación. Dados A-módulos M, N y P, la aplicación de $\operatorname{Hom}_A(N,P) \times \operatorname{Hom}_A(M,N)$ en $\operatorname{Hom}_A(M,P)$; $(g,f) \mapsto g \circ f$ satisface:

i) $g \circ (f + f') = g \circ f + g \circ f'$.

ii) $(g + g') \circ f = g \circ f + g' \circ f$.

iii) $c \in C(A) \Longrightarrow c \cdot (g \circ f) = (c \cdot g) \circ f = g \circ (c \cdot f)$.

En particular, dado un A-módulo M, la composición usual de aplicaciones define una operación en el grupo $\operatorname{Hom}_A(M,M)$, que lo convierte en un anillo, notado $\operatorname{End}_A(M)$ (anillo de endomorfismos de M). M puede considerarse como módulo sobre $\operatorname{End}_A(M)$ tomando $f \cdot x = f(x)$.

Observación. Si S es un semigrupo, notado multiplicativamente, su producto define una operación en el conjunto $\operatorname{Inv}(S)$ de elementos inversibles de S, que lo convierte en un grupo.

En particular, dado un anillo A, se tiene el grupo de unidades de A, $U(A) = \operatorname{Inv}(A, \cdot)$.

Si M es un A-módulo, la composición usual de aplicaciones define una estructura de grupo en el conjunto de automorfismos de M, que se nota $\operatorname{Aut}(M)$ (grupo de automorfismos de M). En efecto, $\operatorname{Aut}_A(M) = U(\operatorname{End}_A(M))$.

3. Módulos cocientes

Repaso conjuntista:

Definición. Una relación $\sim$ en un conjunto C se dice de equivalencia si y sólo si, $\sim$ satisface:

$$r)\, x \sim x.$$
$$s)\, x \sim y \Longrightarrow y \sim x.$$
$$t)\, x \sim y \wedge y \sim z \Longrightarrow x \sim z$$

Sea $\sim$ una relación de equivalencia en un conjunto C.

Definición. Dado $x \in C$, se llama clase de equivalencia de x a $\tilde{x} = \{y \in C : y \sim x\}$.

Observación. Dados $x, y \in C$, son equivalentes:
i) $x \sim y$.
ii) $\tilde{x} = \tilde{y}$.
iii) $\tilde{x} \cap \tilde{y} \neq \emptyset$.

Definición. Se llama conjunto cociente de C por $\sim$ a $C/_\sim = \{\tilde{x} : x \in C\}$.

Observación. $C/_\sim$ es una partición de C.

Definición. Se llama proyección de C en $C/_\sim$ a la aplicación $p\colon C \longrightarrow C/_\sim$ dada por $p(x) = \tilde{x}$ $(x \in C)$.

Observación. p es suryectiva.

$\star$ Comentario sobre relaciones de equivalencia y particiones de un conjunto.

Definición. Una relación de equivalencia $\sim$ en un A-módulo M se dice compatible (con la estructura de A-módulo de M) si y sólo si $\sim$ satisface:
i) $x \sim y \wedge x' \sim y' \Longrightarrow x + x' \sim y + y'$.
ii) $a \in A \wedge x \sim y \Longrightarrow a \cdot x \sim a \cdot y$.

Ejemplos. i) Relaciones de equivalencia compatibles con la estructura de grupo. Una relación de equivalencia $\sim$ en un grupo G es compatible con la estructura de grupo de G, o sea,

$$x \sim y \wedge x' \sim y' \Longrightarrow x + x' \sim y + y',$$

si, y sólo si, $\sim$ es compatible con la estructura de $\mathbb{Z}$-módulo de G.

(Ejercicio: para la necesidad, emplear que $x \sim y \Longrightarrow -x \sim -y$.)

ii) Relaciones de equivalencia compatibles con la estructura de $K[X]$-módulo (K cuerpo).

Sea V un K-espacio vectorial provisto de un endomorfismo t. Una relación de equivalencia $\sim$ es compatible con la estructura de $K[X]$-módulo de V si, y sólo si, $\sim$ es compatible con la estructura de K-espacio vectorial de V y $\sim$ satisface: $v \sim w \Longrightarrow t(v) \sim t(w)$. (Ejercicio).

Nota. Dado un A-módulo M, $\rho(M)$ nota el conjunto de las relaciones de equivalencia en M que son compatibles.

PROPOSICIÓN 3.1. *Para un A-módulo M, se verifica:*

i) Si $\sim$ es una relación de equivalencia en M compatible, entonces $\tilde{0} = \{x \in M \mid x \sim 0\}$ es un submódulo de M.

ii) Si S es un submódulo de M, la relación $\equiv (S)$ en M dada por "$x \equiv y\,(S) \iff x - y \in S$" es una relación de equivalencia compatible.

iii) Las aplicaciones entre $\rho(M)$ y $\sigma(M)$ dadas por $\sim \mapsto \tilde{0}$ y $S \mapsto \equiv (S)$ son recíprocas.

PROPOSICIÓN 3.2. *Si $\sim$ es una relación de equivalencia en un A-módulo M compatible, existe una única estructura de A-módulo en el conjunto $M/_\sim$ tal que la proyección $p\colon M \longrightarrow M/_\sim$ es un morfismo.*

Demostración. Existencia. Se definen $+$ y $\cdot$ para $M/_\sim$ en la forma:

$$u + v = p(x + y), \text{ si } u = p(x) \text{ y } v = p(y);$$
$$a \cdot u = p(a \cdot x), \text{ si } u = p(x).$$

ante todo, $+$ y $\cdot$ están bien definidas:

$$p(x) = p(x') \wedge p(y) = p(y') \Longrightarrow p(x + y) = p(x' + y'),$$
$$p(x) = p(x') \Longrightarrow p(a \cdot x) = p(a \cdot x').$$

Se verifica que $(M/_\sim, +, \cdot)$ es un A-módulo. Por las definiciones de $+$ y $\cdot$ es claro que p es un morfismo.

Unicidad. Resulta del

LEMA 3.3. *Dados un A-módulo M, un conjunto C y una suryección $f\colon M \longrightarrow C$, si $(+_i, \cdot_i)$ $(i = 1, 2)$ son estructuras de A-módulo para las cuales f es un morfismo, entonces $(+_1, \cdot_1) = (+_2, \cdot_2)$.*. $\square$

Observación. p es un epimorfismo y $\operatorname{Ker} p = \tilde{0}$.

Ejemplos. Sea M un A-módulo.

	módulo	relación de equivalencia compatible	cociente
i)	M^I $(I \neq \emptyset)$	$x \sim y \iff x_p = y_p$ $(p \in I$ fijado$)$	$M^I/_\sim \simeq M$
ii)	M^n $(n \in \mathbb{N})$	$x \sim y \iff \sum_{1 \leq i \leq n} x_i = \sum_{1 \leq i \leq n} y_i$	$M^n/_\sim \simeq M$
iii)	$M^{n \times n}$	$x \sim y \iff dg(x) = dg(y)$	$M^{n \times n}/_\sim \simeq M^n$

Sea M un A-módulo, y sea S un submódulo de M.

Notación. El conjunto $M/_\equiv (S)$, provisto de la única estructura de A-módulo tal que la proyección de M en $M/_\equiv (S)$ es un morfismo, se nota M/S; y la proyección se escribe $\pi_{S,M}$ (también, π_S, π_M o π, según la conveniencia).

Observación. π es un epimorfismo y $\operatorname{Ker} \pi = S$. Además, $\pi(x) = x + S$ $(x \in M)$.

Notación. $\sigma_S(M)$ nota $\sigma_{\pi_{S,m}}(M) = \{T \in \sigma(M) : S \subseteq T\}$.

PROPOSICIÓN 3.4. *Las aplicaciones entre $\sigma_S(M)$ y $\sigma(M/S)$ definidas tomando imagen directa e imagen inversa por π son morfismos de orden recíprocos.*

Demostración. Se aplica la observación anterior. □

Definición. Se dice que S es un submódulo maximal de M si y sólo si:
i) $S \neq M$.
ii) Si T es un submódulo $\neq M$ de M y $S \subseteq T$, entonces $S = T$.

Ejemplo. Sea V un K-espacio vectorial de dimensión $n > 0$. Un subespacio S de V es maximal si, y sólo si, $\dim_K S = n - 1$.

(Además, como $\dim_K V = \dim_K S + \dim_K V/S$, resulta que $\dim_K S = n - 1 \iff \dim_K V/S = 1$.)

COROLARIO 3.5. *S es un submódulo maximal de M si, y sólo si, M/S es un módulo simple.*

Demostración. S es maximal $\iff \sigma_S(M)$ tiene dos elementos $\iff \sigma(M/S)$ tiene dos elementos $\iff M/S$ es simple. □

Ejemplos. i) Los grupos cocientes de $\mathbb{Z}$.

Notación. $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ $(n \in \mathbb{N}_0)$.

$$x \equiv y\ (n\mathbb{Z}) \iff x - y \in n\mathbb{Z} \iff n|x - y \iff x \equiv y\ (n).$$

$$\pi(x) = x + n\mathbb{Z} = \{x + m\ :\ n|m\}.$$

$n = 0$) $\mathbb{Z}_0 \simeq \mathbb{Z}$.

En general, $M/0 \simeq M$, porque $\pi_{M,0}$ es un isomorfismo ($\operatorname{Ker} \pi_{M,0} = 0$).

$$x \equiv y\ (0) \iff x - y = 0 \iff x = y.$$

Conjuntísticamente, $C/_= = \{\{x\}\ :\ x \in C\}$ y $p\colon C \longrightarrow C/_=$ es biyectiva.
$n = 1$) $\mathbb{Z}_1 = 0$.

En general, $M/M = 0$, porque $\pi_{M,M}$ es nula ($\operatorname{Ker} \pi_{M,M} = M$).

$$\forall\, x, y \in M : x \equiv y\ (M).$$

Conjuntísticamente, $C/_\sim = \{C\}$, si $\sim$ es la relación trivial en C, y $p\colon C \longrightarrow C/_\sim$ es constante.
$n \in \mathbb{N}$) Se sabe que

$$\forall\, x \in \mathbb{Z},\ \exists!\, r \in \mathbb{Z} : x \equiv r\ (n) \wedge 0 \leq r < n.$$

Si $C = \{r \in \mathbb{Z} : 0 \leq r < n\}$, esta propiedad puede expresarse

$$\forall\, x \in \mathbb{Z},\ \exists!\, r \in C : \pi(x) = \pi(r),$$

vale decir (π es suryectiva)

$$\forall\, u \in \mathbb{Z}_n,\ \exists!\, r \in C : \pi(r) = u,$$

o también, si $f = \pi|_C \colon C \longrightarrow \mathbb{Z}_n$,

$$\forall\, u \in \mathbb{Z}_n,\ \exists!\, r \in C : f(r) = u,$$

lo que significa:

$$f \text{ es biyectiva.}$$

(En particular, esto dice que $\mathbb{Z}_n$ es un grupo finito, de n elementos.)

LEMA 3.6.(Transporte de estructura) *Dados un conjunto C, un A-módulo M y una biyección $f \colon C \longrightarrow M$, existe una única estructura de A-módulo en C tal que f es un (iso)morfismo, a saber:*

$$x +_C y = f^{-1}(f(x) + f(y)),$$
$$a \cdot_C x = f^{-1}(a \cdot f(x)).$$

Demostración. $f^{-1}(0)$ es el elemento neutro de $+_C$; y dado $x \in C$, su inverso es $f^{-1}(-f(x))$. Aplicando f en las definiciones de $+_C$ y $\cdot_C$ se obtiene que f es un morfismo.

En cuanto, a la unicidad de la estructura, si -ahora- $(+_C, \cdot_C)$ es una estructura de A-módulo en C tal que f es un morfismo:

$$f(x +_C y) = f(x) + f(y),$$
$$f(a \cdot_C x) = a \cdot f(x),$$

aplicando f^{-1} se obtienen las definiciones dadas. También, puede aplicarse el Lema 3.3 a $f^{-1} \colon M \longrightarrow C$. □

Ejercicio. Completar la demostración.

En nuestro caso, $\mathbb{Z}_n \simeq (C.+_C)$, donde

$$r +_C s = t,$$

siendo t el resto de la división de $r + s$ por n:

$$r +_C s = f^{-1}(\pi(r) + \pi(s)) = f^{-1}(\pi(r + s)) = f^{-1}(\pi(t)) = f^{-1}(f(t)) = t.$$

Definición. Sea θ una operación en un conjunto C finito, y sea $(x_i)_{1 \le i \le n}$ una numeración de C. Se llama tabla de θ (respecto de la numeración fijada) a la matriz $(x_i \theta x_j)_{1 \le i,j \le n}$.

θ	x_1	x_2	$\cdots$	x_j	$\cdots$	x_n
x_1						
x_2						
$\cdots$						
x_i				$x_i\theta x_j$		
$\cdots$						
x_n						

Traducción en la tabla de propiedades de la operación. Tabla para $\mathbb{Z}_6$.

ii) Los módulos cocientes de $K[X]$ (K cuerpo).

Sea $M = \{f \in K[X] : f \text{ es mónico o } f = 0\}$.

Notación. $K[X]_f = K[X]/fK[X]$ ($f \in M$).

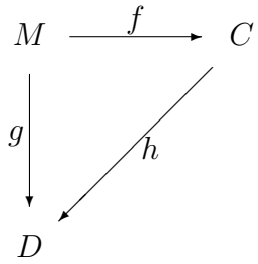
$f = 0$) $K[X]_0 \simeq K[X]$.

$f \in M$, $f \neq 0$) $K[X]_f \simeq (C, +_C, \cdot_C)$, donde

$$C = \{r \in K[X] : r = 0 \vee grr < grf\}$$
$$r +_C s = t, \text{siendo } t \text{ el resto de la división de } r + s \text{ por } f,$$
$$p \cdot_C r = u, \text{siendo } u \text{ el resto de la división de } p \cdot r \text{ por } f.$$

Ejercicio Desarrollar.

Definición. Sea M un A-módulo, y sea S un submódulo de M. Se llama módulo cociente de M por S a un objeto (C, f), donde C es un A-módulo y f es un morfismo de M en C tal que $S \subseteq \operatorname{Ker} f$, que satisface: si (D, g) es un objeto de la misma especie, existe un único morfismo $h\colon C \longrightarrow D$ que hace conmutativo el diagrama

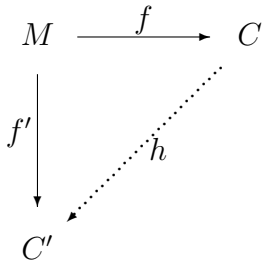


vale decir, $h \circ f = g$.

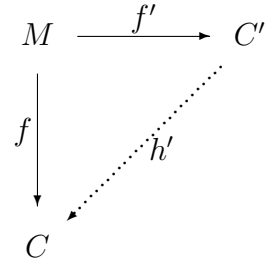
Consistencia de la definición i) Unicidad. Si (C, f) y (C', f') son módulos cocientes de M por S, existe un único isomorfismo $h\colon C \longrightarrow C'$ tal que $h \circ f = f'$.

ii) Existencia. $(M/S, \pi_{M,S})$ es un módulo cociente de M por S.

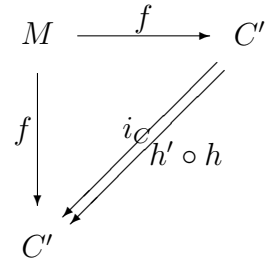
Demostración. i) Como (C, f) satisface la definición y (C', f') es un tal objeto, $\exists\, !\, h : h \circ f = f'$.



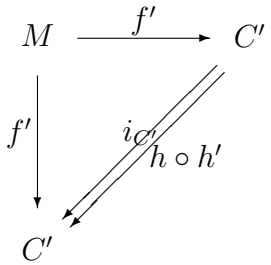
Queda por verificar que h es un isomorfismo. Como (C', f') satisface la definición y (C, f) es un tal objeto, $\exists\,!\, h' : h' \circ f' = f$.



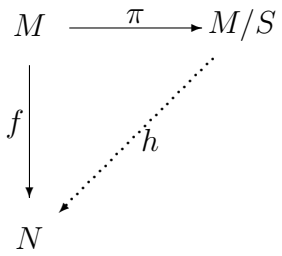
h' es el morfismo inverso de h. En efecto, como (C, f) satisface la definición, por unicidad, $(h \circ h') \circ f = f \ \wedge\ i_C \circ f = f \Longrightarrow h' \circ h = i_C$.



También, como (C', f') satisface la definición, por unicidad, $(h \circ h') \circ f' = f' \ \wedge\ i_{C'} \circ f' = f'$ $\Longrightarrow h \circ h' = i_{C'}$.



ii) Dado un morfismo de A-módulos $f\colon M \longrightarrow N$ tal que $S \subseteq \operatorname{Ker} f$, debe probarse que $\exists\,!\, h : h \circ \pi = f$.

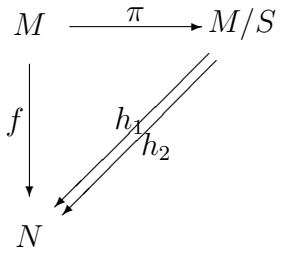


Existencia de h. *Definición.* $h(u) = f(x)$, si $u = \pi(x)$. h está bien definida:

$$\begin{array}{ccc} \pi(x) = \pi(x') & \Longrightarrow & f(x) = f(x'). \\ \Downarrow & & \Uparrow \\ x - x' \in S & \Longrightarrow & x - x \in \operatorname{Ker} f \end{array}$$

$h \circ \pi = f : h(\pi(x)) = f(x)$, por definición. h es un morfismo: $h \circ \pi (= f)$ morfismo $\Longrightarrow$ h morfismo.

Unicidad de h. Dados morfismos $h_i \colon M/S \longrightarrow N$ $(i = 1, 2)$, debe probarse que



$h_1 \circ \pi = f \ \wedge \ h_2 \circ \pi = f \Longrightarrow h_1 \circ \pi = h_2 \circ \pi \Longrightarrow *) \ h_1 = h_2$

$*$) Dadas aplicaciones de conjuntos $C \xrightarrow{f} D \underset{h}{\overset{g}{\rightrightarrows}} E$, si f es suryectiva,

$$g \circ f = h \circ f \qquad \Longrightarrow \qquad g = h$$

Proposición 3.7. *Dado un morfismo de A-módulos $f \colon M \longrightarrow N$, si S es un submódulo de M tal que $S \subseteq \operatorname{Ker} f$ y $h \colon M/S \longrightarrow N$ es el factorizador de f, se verifica:*

i) $\operatorname{Ker} h = \pi(\operatorname{Ker} f)$. *En particular, h es un monomorfismo si, y sólo si,* $\operatorname{Ker} f = S$.

ii) $\operatorname{Im} h = \operatorname{Im} f$. *En particular, h es un epimorfismo si, y sólo si, f lo es.*

Demostración. i) $\subseteq : \ u \in \operatorname{Ker} h \Longrightarrow h(u) = 0 \Longrightarrow f(x) = 0 \Longrightarrow x \in \operatorname{Ker} f \Longrightarrow u = \pi(x) \in \pi(\operatorname{Ker} f)$.

$\supseteq : \ u \in \pi(\operatorname{Ker} f) \Longrightarrow \exists\, x \in \operatorname{Ker} f : u = \pi(x) \Longrightarrow h(u) = f(x) = 0 \Longrightarrow u \in \operatorname{Ker} h$

h mono $\Longleftrightarrow \operatorname{Ker} h = 0 \Longleftrightarrow \pi(\operatorname{Ker} f) = 0 \Longleftrightarrow^{*)} \operatorname{Ker} f \subseteq \operatorname{Ker} \pi \Longleftrightarrow \operatorname{Ker} f \subseteq S$.

*) Dado un morfismo de A-módulos $f \colon M \longrightarrow N$ y un subconjunto S de M

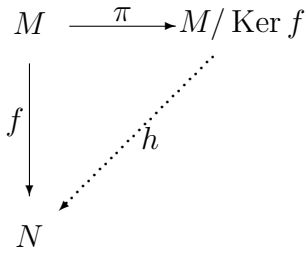
$$f(S) = 0 \Longleftrightarrow S \subseteq \operatorname{Ker} f.$$

ii) $h \circ \pi = f \Longrightarrow \mathrm{Im}(h \circ \pi) = \mathrm{Im}\, f \overset{**)}{\Longrightarrow} \mathrm{Im}\, h = \mathrm{Im}\, f$.

**) Dadas aplicaciones de conjuntos $C \xrightarrow{f} D \xrightarrow{g} E$, $\mathrm{Im}(g \circ f) = g(\mathrm{Im}\, f)$. En particular, si f es suryectiva, $\mathrm{Im}(g \circ f) = \mathrm{Im}\, g$.□

Corolario **1** (1er. Teorema de isomofismo). *Dado un morfismo de A-módulos* $f\colon M \longrightarrow N$, *se tiene que* $M/\operatorname{Ker} f \simeq \mathrm{Im}\, f$.

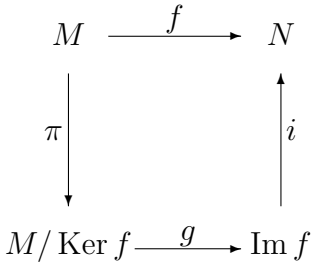
Demostración.



$\exists!\ h\colon h \circ \pi = f$.

Además, h es un monomorfismo, por i) de la Proposición anterior, e $\mathrm{Im}\, h = \mathrm{Im}\, f$, por ii) de la misma Proposición. Luego, $h|^{\mathrm{Im}\, f}\colon M/\operatorname{Ker} f \longrightarrow \mathrm{Im}\, f$ es un isomorfismo.□

Observación. Tomando $g = h|^{\mathrm{Im}\, f}$, se tiene el diagrama conmutativo



que se llama <u>análisis</u>, o <u>descomposición canónica</u> de f.

Definiciones. Dado un morfismo de A-módulos $f\colon M \longrightarrow N$, se llama <u>conúcleo</u> de f a $\mathrm{Coker} = N/\operatorname{Im} f$; y se llama <u>coimagen</u> de f a $\mathrm{Coim}\, f = M/\operatorname{Ker} f$.

Observación. i) El 1er. Teorema de isomorfismo dice que $\mathrm{Coim}\, f \simeq \mathrm{Im}\, f$.

ii) f es un epimorfismo si, y sólo si, $\mathrm{Coker}\, f = 0$. (En general, $M/S = 0 \Longleftrightarrow \pi_{M,S} = 0 \Longleftrightarrow \operatorname{Ker} \pi_{M,S} = M \Longleftrightarrow S = M$.)

iii) f es un monomorfismo si, y sólo si, $\mathrm{Coim}\, f = M$. (En general, $M/S = M \Longleftrightarrow \pi_{M,S}$ iso $\Longleftrightarrow \operatorname{Ker} \pi_{M,S} = 0 \Longleftrightarrow S = 0$.)

Ejemplos. i) $\mathbb{R}/\mathbb{Z} \simeq \mathbb{U}$. $\mathbb{Z}$ es un subgrupo de $\mathbb{R}$.

$$x \equiv y\ (\mathbb{Z}) \iff x - y \in \mathbb{Z}.$$
$$\pi(x) = x + \mathbb{Z}$$

$f\colon \mathbb{R} \longrightarrow \mathbb{U}$, $f(x) = \cos tx + \operatorname{sen} tx.i$ $(x \in \mathbb{R})$

f es un morfismo:

$f(x+y) = \cos t(x+y) + \operatorname{sen} t(x+y).i = \cos(tx+ty) + \operatorname{sen}(tx+ty).i = (\cos tx + \operatorname{sen} tx.i)(\cos ty + \operatorname{sen} ty.i) = f(x).f(y)$.

f es suryectiva, si $t \neq 0 : \forall z \in \mathbb{U}, \exists x \in \mathbb{R} : z = f(x)$. Tomar $x = \frac{arg\ z}{t}$.

$\operatorname{Ker} f = \mathbb{Z}$, para $t = 2\pi : f(x) = 1 \iff \cos tx = 1 \wedge \operatorname{sen} tx = 0 \iff tx \in 2\pi\mathbb{Z} \iff x \in \mathbb{Z}$.

ii) $\mathbb{C}^*/\mathbb{U} \simeq \mathbb{R}_{>0}$.

Notación. Si A es un anillo, A^* nota $A - \{0\}$.

Observación. A es un anillo de división si, y sólo si, $U(A) = A^*$. En particular, si K es un cuerpo, K^* resulta un grupo abeliano (grupo multiplicativo de K). $\mathbb{U}$ es un subgrupo de $\mathbb{C}^*$ (por definición).

$$x \equiv y\ (\mathbb{U}) \iff \frac{x}{y} \in \mathbb{U} \iff \left|\frac{x}{y}\right| = 1 \iff |x| = |y|.$$

$\pi(x) = x.\mathbb{U}$.

$\mathbb{R}_{>0}$ es un subgrupo de $\mathbb{R}^*$:

.) $1 > 0$.

..) $x, y > 0 \Longrightarrow x.y > 0$.

...) $x > 0 \Longrightarrow x^{-1} > 0$.

$f\colon \mathbb{C}^* \longrightarrow \mathbb{R}_{>0}$, $f(x) = |x|$ $(x \in \mathbb{C}^*)$.

f es un morfismo: $f(x.y) = f(x).f(y)$.

f es suryectiva: $\forall r \in \mathbb{R}_{>0}, \exists x \in \mathbb{C}^* : r = f(x)$. Tomar $x = r$. $\operatorname{Ker} f = \mathbb{U} : f(x) = 1 \iff |x| = 1$.

iii) $\mathbb{C}^*/\mathbb{R}_{>0} \simeq \mathbb{U}$. $\mathbb{R}_{>0}$ es un subgrupo de $\mathbb{C}^*$ (por transitividad).

$$x \equiv y\ (\mathbb{R}_{>0}) \iff \frac{x}{y} \in \mathbb{R}_{>0}.$$

$\pi(x) = x.\mathbb{R}_{>0}$.

$f\colon \mathbb{C}^* \longrightarrow \mathbb{U}$, $f(x) = \frac{x}{|x|}$ $(x \in \mathbb{C}^*)$.

f es un morfismo: $f(x.y) = f(x).f(y)$.

f es suryectiva: $\forall x \in \mathbb{U}, \exists x \in \mathbb{C}^* : z = f(x)$. Tomar $x = z$.

$\operatorname{Ker} f = \mathbb{R}_{>0} : f(x) = 1 \iff x = |x| \iff x \in \mathbb{R}_{>0}$.

iv) $\mathbb{C}^*/\mathbb{G}_n \simeq \mathbb{C}^*$.

Si $n \in \mathbb{N}$, $\mathbb{G}_n = \{z \in \mathbb{C} : z^n = 1\}$ es un subgrupo de $\mathbb{C}^*$ (grupo de raíces n-ésimas de la unidad).

$$x \equiv y\ (\mathbb{G}_n) \iff \frac{x}{y} \in \mathbb{G}_n \iff \left(\frac{x}{y}\right)^n = 1 \iff x^n = y^n.$$

$\pi(x) = x.\mathbb{G}_n$. $f\colon \mathbb{C}^* \longrightarrow \mathbb{C}^*$, $f(x) = x^n$ $(x \in \mathbb{C}^*)$.

f es un morfismo: $f = \eta_{n,\mathbb{C}^*}$.

f es suryectiva: $\forall\, y \in \mathbb{C}^*,\ \exists\, x \in \mathbb{C}^* : y = f(x)$. Tomar x como una raíz en $\mathbb{C}$ de $X^n - y$.

$\operatorname{Ker} f = \mathbb{G}_n : f(x) = 1 \iff x^n = 1$

Pero, $M/S = M \iff S = 0$. Aquí¿Qué pasa?

v) Si $m, n \in \mathbb{N}$ y $m|n$, $\mathbb{G}_n/\mathbb{G}_m \simeq \mathbb{G}_{\frac{n}{m}}$.

$$\mathbb{G}_m \subseteq \mathbb{G}_n \iff m|n \qquad \text{(ejercicio)}.$$

$f\colon \mathbb{G}_n \longrightarrow \mathbb{C}^*$, $f(x) = x^m$ $(x \in \mathbb{C}^*)$.

f es un morfismo: $f = \eta_{m,\mathbb{C}^*}|_{\mathbb{G}_n}$.

$\operatorname{Ker} f = \operatorname{Ker} \eta_{m,\mathbb{C}^*} \cap \mathbb{G}_n = \mathbb{G}_m \cap \mathbb{G}_n = \mathbb{G}_m$.

$\operatorname{Im} f = \mathbb{G}_{\frac{n}{m}}$.

$\subseteq$: $x \in \mathbb{G}_n \Longrightarrow (x^m)^{\frac{n}{m}} = x^n = 1$.

$\supseteq$: dado $y \in \mathbb{G}_{\frac{n}{m}}$, sea $x \in \mathbb{C}$ tal que $x^m = y$; pero, entonces, $x \in \mathbb{G}_n$ ya que $x^n = (x^m)^{\frac{n}{m}} = y^{\frac{n}{m}} = y^{\frac{n}{m}} = 1$.

vi) Si $m, n \in \mathbb{N}_0$ verifican que $m|n$ y $m \neq 0$, $m\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_{\frac{n}{m}}$.

Se considera $\eta_m\colon \mathbb{Z} \longrightarrow \mathbb{Z}$. $\operatorname{Im} \eta_m = m\mathbb{Z}$; y η_m es un monomorfismo, pues $m \neq 0 : m.x = 0 \Longrightarrow x = 0$. Luego, $\eta_m|^{m\mathbb{Z}}\colon \mathbb{Z} \longrightarrow m\mathbb{Z}$ es un isomorfismo. Sea $f = \left(\eta_m|^{m\mathbb{Z}}\right)^{-1} : m\mathbb{Z} \longrightarrow \mathbb{Z}$, y sea $\pi\colon \mathbb{Z} \longrightarrow \mathbb{Z}_{\frac{n}{m}}$ la proyección. Ahora, se considera $g = \pi \circ f\colon m\mathbb{Z} \longrightarrow \mathbb{Z}_{\frac{n}{m}}$. Se tiene que g es un epimorfismo, por serlo f y π. Además,

$$\operatorname{Ker} g \underset{*)}{=} f^{-1}(\operatorname{Ker} \pi) = \eta_m|^{m\mathbb{Z}}(\operatorname{Ker} \pi) = \eta_m(\operatorname{Ker} \pi) = \eta_m\left(\frac{n}{m}\mathbb{Z}\right) = n\mathbb{Z},$$

$*$) Dados morfismos de A-módulos $M \xrightarrow{f} N \xrightarrow{g} P$, $\operatorname{Ker}(g \circ f) = f^{-1}(\operatorname{Ker} g)$. En particular, si g es un morfismo, $\operatorname{Ker}(g \circ f) = \operatorname{Ker} f$.

Ejercicio. Verificar los ejemplos de cocientes dados según relaciones de equivalencia compatibles empleando el 1er. Teorema de isomorfismo.

Corolario **2** (2do. Teorema de isomorfismo). *Si M es un A-módulo y S y T son submódulos de M, entonces $\pi_S(T)$ se identifica con T/S; y con tal identificación, $(M/S)/(T/S) \simeq M/T$.*

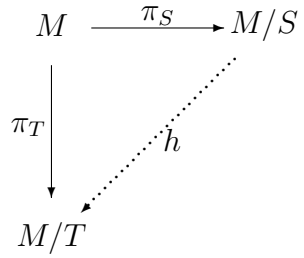
Demostración. Conjuntísticamente,

$$\pi_S(T) = \{x +_M S : x \in T\} = \{x + S \subseteq M : x \in T\},$$
$$T/S = \{x +_T S : x \in T\} = \{x + S \subseteq T : x \in T\},$$

y las estructuras de módulo coinciden.

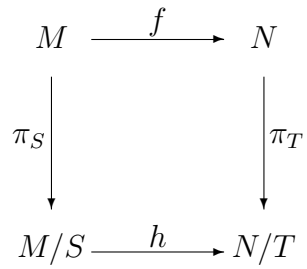
Algebraicamente, si $\pi = \pi_S$, se considera $\pi|_T\colon T \longrightarrow M/S$. Se tiene que $\operatorname{Ker} \pi|_T = \operatorname{Ker} \pi \cap T = S \cap T = S$ e $\operatorname{Im} \pi|_T = \pi(T)$, de donde $T/S \simeq \pi(T)$, por el 1er. Teorema de isomorfismo (ejercicio: identificar el isomorfismo).

Además,



$S \subseteq T = \operatorname{Ker} \pi_T \Longrightarrow \exists\, !\, h\ ;\ h \circ \pi_S = \pi_T$. Se tiene que $\operatorname{Ker} h = \pi_S(\operatorname{Ker} \pi_T) = \pi_S(T)$; y que h es un epimorfismo, por serlo π_T. Luego, $(M/S)/\pi_S(T) \simeq M/T$, por el 1er. Teorema de isomorfismo.□

PROPOSICIÓN 3.8. *Dado un morfismo de A-módulos $f\colon M \longrightarrow N$, si S y T son submódulos de M y N tales que $f(S) \subseteq T$, existe un único morfismo $h\colon M/S \longrightarrow N/T$ que hace conmutativo el diagrama*



vale decir, $h \circ \pi_S = \pi_T \circ f$. Además, se verifica:

i) $\operatorname{Ker} h = \pi_S(f^{-1}(T))$. *$h$ es un monomorfismo si, y sólo si, $S = f^{-1}(T)$.*

ii) $\operatorname{Im} h = \pi_T(\operatorname{Im} f)$. *$h$ es un epimorfismo si, y sólo si, $\pi_T \circ f$ lo es.*

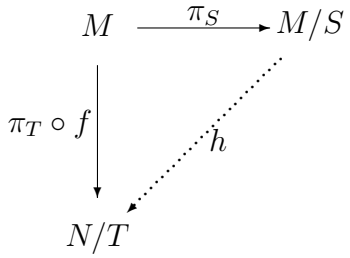
iii) Si f es un monomorfismo y $f(S) = T$, entonces h es un monomorfismo.

iv) Si f es un epimorfismo, entonces h lo es.

v) Notando h con $\overline{f}$, se tiene las fórmulas:

$$\begin{aligned} \overline{g \circ f} &= \overline{g} \circ \overline{f}, \\ \overline{i_M} &= i_{M/S}, \\ \overline{f + f'} &= \overline{f} + \overline{f'}, \\ \overline{c.f} &= c.\overline{f}\ \ (c \in C(A)). \end{aligned}$$

Demostración.



$f(S) \subseteq T \Longleftrightarrow S \subseteq f^{-1}(T) = \mathrm{Ker}(\pi_T \circ f)$. $\therefore \exists\, !h : h \circ \pi_S = \pi_T \circ f$.

i) y ii) resultan de la descomposición del factorizador, pues $\mathrm{Ker}(\pi \circ f) = f^{-1}(T)$ e $\mathrm{Im}(\pi_T \circ f) = \pi_T(\mathrm{Im}\, f)$.

iii) Siendo f monomorfismo,

$$h \text{ monomorfismo } \Longleftrightarrow f(S) = \mathrm{Im}\, f \cap T.$$

En efecto,

$$h \text{ monomorfismo } \Longleftrightarrow f^{-1}(T) \subseteq S \Longleftrightarrow \text{“}f(x) \in T \Longrightarrow x \in S\text{”} \Longrightarrow$$
$$\text{“}f(x) \in T \Longrightarrow f(x) \in f(S)\text{”} \Longleftrightarrow \mathrm{Im}\, f \cap T \subseteq f(S).$$

Por lo tanto,

$$f(S) = T \Longrightarrow \mathrm{Im}\, f \cap T = \mathrm{Im}\, f \cap f(S) = f(S).$$

iv) sigue trivialmente de ii).

v) 1ra. fórmula. Los diagramas conmutativos

$$\begin{array}{ccc} M & \xrightarrow{\ f\ } & N \\ {\scriptstyle \pi_S}\downarrow & & \downarrow{\scriptstyle \pi_T} \\ M/S & \xrightarrow{\ \overline{f}\ } & N/T \end{array}$$

$f(S) \subseteq T$

$$\begin{array}{ccc} N & \xrightarrow{\ g\ } & P \\ {\scriptstyle \pi_T}\downarrow & & \downarrow{\scriptstyle \pi_U} \\ N/T & \xrightarrow{\ \overline{g}\ } & P/U \end{array}$$

$(g(T) \subseteq U)$ suministran el diagrama conmutativo

$$\begin{array}{ccc} M & \xrightarrow{\ g \circ f\ } & P \\ {\scriptstyle \pi_S}\downarrow & & \downarrow{\scriptstyle \pi_U} \\ M/S & \xrightarrow{\ \overline{g} \circ \overline{f}\ } & P/U \end{array}$$

$((g \circ f)(S) \subseteq U)$. Luego por razones de unicidad, $\overline{g \circ f} = \overline{g} \circ \overline{f}$.

2da. fórmula. El diagrama conmutativo

$$\begin{array}{ccc} M & \xrightarrow{i_M} & M \\ {\scriptstyle \pi_S}\downarrow & & \downarrow{\scriptstyle \pi_S} \\ M/S & \xrightarrow{i_{M/S}} & M/S \end{array}$$

prueba que $\overline{i_M} = i_{M/S}$.

3ra. y 4ta. fórmulas, ejercicio.□

Corolario 3.8. *Dado un isomorfismo de A-módulos $f\colon M \longrightarrow N$, si S y T son submódulos de M y N tales que $f(S) = T$, entonces $\overline{f}\colon M/S \longrightarrow N/T$ también es un isomorfismo.*

Demostración. Sigue de iii) y iv) de la Proposición; también se obtiene de las dos primeras fórmulas de v).□

Ejercicio Si $m, n \in \mathbb{N}_0$ satisfacen que $m|n$ y $m \neq 0$, probar que $\mathbb{Z}_{\frac{m}{n}} \simeq m\mathbb{Z}/n\mathbb{Z}$ usando el corolario.

Sea p una propiedad predicable en $\mathfrak{M}_s(A)$.

Definiciones. Se dice que p es:
mórfica sii: M tiene p y $f\colon M \longrightarrow N$ morfismo $\Longrightarrow$ Im f tiene p.
epimórfica sii: M tiene p y $f\colon M \longrightarrow N$ epimorfismo $\Longrightarrow$ N tiene p.
algebraica (o isomórfica) sii: M tiene p y $f\colon M \longrightarrow N$ isomorfismo $\Longrightarrow$ N tiene p.
divisible sii: M tiene p y S submódulo de $M \Longrightarrow M/S$ tiene p.
hereditaria sii: M tiene p y S submódulo de $M \Longrightarrow S$ tiene p.

Observación. Son equivalentes:
i) p es mórfica.
ii) p es epimórfica.
iii) p es algebraica y divisible.

Ejemplo. En $\mathfrak{M}(\mathbb{Z})$, "$1 \in G$" no es una propiedad algebraica: $1 \in \mathbb{Z}$ y $1 \notin n\mathbb{Z}$

4. Generación. Módulos de tipo finito

Repaso conjuntista:

Sea C un conjunto, y sea $\mathcal{C}$ un conjunto de partes de C.

$$\bigcup\mathcal{C} = \{x \in C \,:\, \exists\, S \in \mathcal{C} \,:\, x \in S\}. \quad \bigcup\{S,T\} = S \cup T,\ \bigcup\{S\} = S,\ \bigcup\emptyset = \emptyset.$$
$$\bigcap\mathcal{C} = \{x \in C \,:\, \forall\, S \in \mathcal{C} \,:\, x \in S\}. \quad \bigcap\{S,T\} = S \cap T,\ \bigcap\{S\} = S,\ \bigcap\emptyset = \emptyset.$$

Sea $(S_i)_{i\in I}$ una familia de partes de C

$$\bigcup_{i\in I} S_i = \bigcup\{S_i \,:\, i \in I\} = \{x \in C \,:\, \exists\, i \in I \,:\, x \in S_i\}.$$
$$\bigcap_{i\in I} S_i = \bigcap\{S_i \,:\, i \in I\} = \{x \in C \,:\, \forall\, i \in I \,:\, x \in S_i\}.$$

$$\bigcup\mathcal{C} = \bigcup_{S\in\mathcal{C}} S.$$
$$\bigcap\mathcal{C} = \bigcap_{S\in\mathcal{C}} S.$$

LEMA 4.1. *Sea M un A-módulo. Si $\mathcal{C}$ es un conjunto de submódulos de M, entonces $\bigcap\mathcal{C}$ es un submódulo de M. (También, si $(S_i)_{i\in I}$ es una familia de submódulos de M, entonces $\bigcap_{i\in I} S_i$ es un submódulo de M*

Demostración. Ejercicio.□

Definición. Sea M un A-módulo, y sea C un subconjunto de M. Se llama submódulo de M generado por C a un objeto S que satisface:
i) $S \in \sigma(M) \wedge C \subseteq S$.
ii) $T \in \sigma(M) \wedge C \subseteq T \Longrightarrow S \subseteq T$.
Consistencia de la definición. *i) Unicidad. Si S y S' son submódulos de M generados por C, entonces $S = S'$.*
ii) Existencia. Si $\mathcal{C} = \{T \in \sigma(M) \,:\, C \subseteq T\}$, entonces $S = \bigcap\mathcal{C}$ es el submódulo de M generado por C.

Demostración. i)

$$\left.\begin{array}{l} S' \in \sigma(M) \wedge C \subseteq S' \Longrightarrow S \subseteq S' \\ S \in \sigma(M) \wedge C \subseteq S \Longrightarrow S' \subseteq S \end{array}\right\} \Longrightarrow S = S'.$$

ii) $S \in \sigma(M)$ por el Lema. $C \subseteq S$ por la definición de S.

$$T \in \sigma(M) \wedge C \subseteq T \Longrightarrow T \in \mathcal{C} \Longrightarrow S \subseteq T.$$

Notación. El submódulo generado por C se nota $M\langle C\rangle$ o $\langle C\rangle$.

Propiedades:
i) $\langle\emptyset\rangle = 0$.
ii) $\langle C\rangle = C \iff C$ es un submódulo.
iii) $\langle 0\rangle = 0 \wedge \langle M\rangle = M$.
iv) $\langle\langle C\rangle\rangle = \langle C\rangle$.
v) $C \subseteq C' \Longrightarrow \langle C\rangle \subseteq \langle C'\rangle$.
vi) $\langle\bigcup_{i\in I} C_i\rangle \supseteq \bigcup_{i\in I}\langle C_i\rangle$.
vii) $\langle\bigcap_{i\in I} C_i\rangle \subseteq \bigcap_{i\in I}\langle C_i\rangle$.

Ejercicio Mostrar que las inclusiones vi) y vii) pueden ser estrictas

PROPOSICIÓN 4.2. *Dado un morfismo de A-módulos $f\colon M \longrightarrow N$, si C es un subconjunto de M, entonces $f(M\langle C\rangle) = N\langle f(C)\rangle$.*

Demostración.
i) $C \subseteq \langle C\rangle \in \sigma(M) \Longrightarrow f(C) \subseteq f(\langle C\rangle) \in \sigma(N)$.
ii) $f(C) \subseteq T \in \sigma(N) \Longrightarrow C \subseteq f^{-1}(f(C)) \subseteq f^{-1}(T) \in \sigma(M) \Longrightarrow \langle C\rangle \subseteq f^{-1}(T)$ $\Longrightarrow f(\langle C\rangle) \subseteq f(f^{-1}(T)) \subseteq T$.□

Observación. Si D es un subconjunto de N, entonces $f^{-1}(N\langle D\rangle) \supseteq M\langle f^{-1}(D)\rangle$; y la inclusión puede ser estricta (ejercicio).

Definiciones. Sea M un A-módulo. Un sistema de generadores de M es un subconjunto S de M tal que $M\langle S\rangle = M$. Una familia de generadores de M es una familia $(x_i)_{i\in I}$ de elementos de M tal que $\{x_i : i \in I\}$ es un sistema de generadores de M.

COROLARIO 4.3. *Se verifica:*
i) Si S es un sistema de generadores de M, entonces $f(S)$ es un sistema de generadores de $\operatorname{Im} f$.
ii) Si $(x_i)_{i\in I}$ es una familia de generadores de M, entonces $(f(x_i))_{i\in I}$ es una familia de generadores de $\operatorname{Im} f$.

Demostración. i) S sistema de generadores de $M \Longrightarrow \langle S\rangle = M \Longrightarrow f(\langle S\rangle) = f(M) = \operatorname{Im} f \Longrightarrow \langle f(S)\rangle = \operatorname{Im} f \Longrightarrow f(S)$ sistema de generadores de $\operatorname{Im} f$.
Ojo: S sistema de generadores de $M \Longrightarrow M\langle S\rangle = M \Longrightarrow f(M\langle S\rangle) = f(M) = \operatorname{Im} f$ $\Longrightarrow N\langle f(S)\rangle^{*)} = \operatorname{Im} f \Longrightarrow f(S)$ sistema de generadores de $\operatorname{Im} f$.
$*$) Si M es un A-módulo, S es un submódulo de M y C es un subconjunto de S, entonces $M\langle C\rangle = S\langle C\rangle$.

$$C \subseteq S \in \sigma(M) \Longrightarrow M\langle C\rangle \Longrightarrow M\langle C\rangle \in \sigma(S).$$
$$C \subseteq T \in \sigma(S) \Longrightarrow C \subseteq T \in \sigma(M) \Longrightarrow M\langle C\rangle \subseteq T.$$

Ejercicio: Hacerlo al revés.
ii) $(x_i)_{i\in I}$ familia de generadores de $M \Longrightarrow \{x_i : i \in I\}$ sistema de generadores de M $\Longrightarrow f(\{x_i : i \in I\})$ sistema de generadores de $\operatorname{Im} f \Longrightarrow (f(x_i))_{i\in I}$ familia de generadores de $\operatorname{Im} f$.

Sea M un A-módulo, y sea $(x_i)_{i\in I}$ una familia de elementos de M.

Definición. Se llama submódulo de M generado por $(x_i)_{i\in I}$ a $M\langle x_i\rangle_{i\in I} = M\langle\{x_i : i \in I\}\rangle$.

Observación. $(x_i)_{i\in I}$ es una familia de generadores de M si, y sólo si, $M\langle x_i\rangle_{i\in I} = M$.

Definición. Dado $x \in M$, se dice que x es combinación lineal de $(x_i)_{i\in I}$ sii existe una familia $(a_i)_{i\in I}$ de elementos de A, con soporte finito, tal que $x = \sum_{i\in I} a_i.x_i$.
(Notar que $\operatorname{sop}_{i\in I} a_i x_i \subseteq \operatorname{sop}_{i\in I} a_i : a_i x_i \neq 0 \Longrightarrow a_i \neq 0$, o sea, $a_i = 0 \Longrightarrow a_i x_i = 0$.)

Proposición 4.4. *$M\langle x_i\rangle_{i\in I}$ es el conjunto de combinaciones lineales de $(x_i)_{i\in I}$.*

Demostración. Sea $S = \{\sum_{i\in I} a_i x_i : (a_i) \in A^{(I)}\}$. $S \in \sigma(M)$:
i) $0 = \sum_{i\in I} 0x_i$ y $(0) \in A^{(I)}$.
ii) $\sum_{i\in I} a_i x_i + \sum_{i\in I} b_i x_i = \sum_{i\in I}(a_i+b_i)x_i$ y $(a_i), (b_i) \in A^{(I)} \Longrightarrow (a_i+b_i) = (a_i)+(b_i) \in A^{(I)}$.
iii) $a\sum_{i\in I} a_i x_i = \sum_{i\in I}(aa_i)x_i$ y $(a_i) \in A^{(I)} \Longrightarrow (aa_i) = a(a_i) \in A^{(I)}$.
$x_i \in S$ $(i \in I)$: Dado $j \in I$, $x_j = \sum_{i\in I} \delta_{ij} x_i$, donde $\delta\colon I \times I \longrightarrow A$ está definida por

$$\delta_{ij} = \delta(i,j) = \begin{cases} 1, \text{ si } i = j, \\ 0, \text{ si } i \neq j. \end{cases} \quad \square$$

Sea T un submódulo de M tal que $x_i \in T$ $(i \in I)$; entonces $\sum_{i\in I} a_i x_i \in T$ $((a_i) \in A^{(I)})$, vale decir, $S \subseteq T$.

Corolario 4.5. *$(x_i)_{i\in I}$ es una familia de generadores de M si, y sólo si, todo elemento de M es combinación lineal de $(x_i)_{i\in I}$.*

Demostración. Se aplican la Observación y la Proposición.$\square$

Observación. Si $x \in M$, $M\langle x\rangle = Ax$
$T = \{(0,y) : y \in \mathbb{R}\}$, $S = \{(x,0) : x \in \mathbb{R}\}$.
$e_1, e_2 \in S \cup T$ y $e_1 + e_2 \notin S \cup T$.
Sea $(S_i)_{i\in I}$ una familia de submódulos de M.

Notación. $\sum_{i\in I} S_i$ denota $M\langle \cup_{i\in I} S_i\rangle$.
Para $I = \mathbb{I}_n$, se escribe $\sum_{1\leq i\leq n} S_i$ ó $S_1 + S_2 + \cdots + S_n$.
Si S y T son submódulos de M, (S,T) se interpreta como $(S_i)_{1\leq i\leq 2}$, donde $S_1 = S$ y $S_2 = T$, con lo cual puede considerarse $S + T$. Si $\mathcal{C}$ es un conjunto de submódulos de M, $\sum \mathcal{C}$ indica $\sum_{S\in\mathcal{C}} S$.

Proposición 4.6.

$$\sum_{i\in I} S_i = \left\{ \sum_{i\in I} x_i : (x_i)_{i\in I} \in M^{(I)} \wedge x_i \in S_i \ (i \in I) \right\}.$$

Demostración. Sea S tal conjunto. $S \in \sigma(M)$:
i) $0 = \sum_{i\in I} x_i$, con $x_i = 0 \in S_i$ $(i \in I)$
ii) $\sum_{i\in I} x_i + \sum_{i\in I} y_i = \sum_{i\in I}(x_i + y_i)$ y $x_i, y_i \in S_i$ $(i \in I) \Longrightarrow x_i + y_i \in S_i$ $(i \in I)$.
iii) $a\sum_{i\in I} x_i = \sum_{i\in I} ax_i$ y $x_i \in S_i$ $(i \in I) \Longrightarrow ax_i \in S_i$ $(i \in I)$.
Dado $\cup_{i\in I} S_i \subseteq S$: Dado $y \in I$ y $z \in S_j$, $z = \sum_{i\in I} \delta_{ij} z$ y $\delta_{ij} z \in S_i$ $(i \in I)$.
Sea T un submódulo de M tal que $\cup_{i\in I} S_i \subseteq T$. Dada $(x_i)_{i\in I} \in M^{(I)}$, con $x_i \in S_i$ $(i \in I)$, como $x_i \in T$ $(i \in I)$ resulta que $\sum_{i\in I} x_i \in T$. Luego, $S \subseteq T$.
?????: Se define

$$a_i' = \begin{cases} a_i, & \text{si } a_i x_i \neq 0, \\ 0, & \text{si } a_i x_i = 0. \end{cases}$$

i) $\operatorname{sop}_{i\in I} a_i' = \operatorname{sop}_{i\in I} a_i$ (interesa $\subseteq$).
ii) $a_i x_i = a_i' x_i$ $(i \in I)$. $\therefore \sum_{i\in I} a_i x_i = \sum_{i\in I} a_i' x_i$.

PROPOSICIÓN 4.7. *Si I es un conjunto filtrante, no vacío, y $(S_i)_{i\in I}$ es una familia creciente, entonces $\cup_{i\in I} S_i$ es un submódulo de M.*

Demostración.

$$I \text{ filtrante } : (I, \leq) \,|\, \text{f}) \; \forall\, i, j \in I, \exists\, k \in I : i \leq k \wedge j \leq k.$$
$$(S_i)_{i\in I} \text{ creciente } : i \leq j \Longrightarrow S_i \subseteq S_j.$$

Si $S = \cup_{i\in I} S_i$:
i) $0 \in S$, pues $I \neq \emptyset$.
ii) $x, y \in S \Longrightarrow \exists\, i, j \in I : x \in S_i \wedge y \in S_j \Longrightarrow \exists\, k \in I : i \leq k \wedge j \leq k \Longrightarrow S_i \subseteq S_k \wedge S_j \subseteq S_k \Longrightarrow x, y \in S_k \Longrightarrow x + y \in S_k \Longrightarrow x + y \in S$.
iii) $a \in A \wedge x \in S \Longrightarrow \exists\, i \in I : x \in S_i \Longrightarrow ax \in S_i \Longrightarrow ax \in S$.□

PROPOSICIÓN 4.8 (3er. Teorema de isomorfismo). *Si M es un A-módulo y S y T son submódulos de M, entonces $S/S \cap T \simeq S + T/T$.*

Demostración.

$$\begin{array}{ccc} S & \xrightarrow{i_{S,S+T}} & S+T \\ \downarrow & & \downarrow \\ S/S\cap T & \xrightarrow{\overline{i_{S,S+T}}} & S+T/T \end{array}$$

$(f(S) = i_{S,S+T}(S) = S \subseteq S+T)$, f es monomorfismo, porque $(i_{S,S+T})^{-1}(T) = \{x \in S \,|\, x \in T\} = S \cap T$.

f es epimorfismo, pues $\operatorname{Im} f = \pi_T(\operatorname{Im} i_{S,S+T}) = \pi_T(S) = S + T/T$. En efecto, dado $x \in S + T/T$, si $x = \pi_T(s+t)$, con $s \in S$ y $t \in T$, entonces $x = \pi_T(s)$, porque $(s+t) - s = t \in T$. (También puede aplicarse la fórmula $f(\sum_{i\in I} S_i) = \sum_{i\in I} f(S_i)$.)□

Definición. Un A-módulo se dice <u>finito</u> si, y sólo si el conjunto subyacente es finito.

Ejemplos. i) Espacios vectoriales finitos.

Si K es un cuerpo finito y V es un K-espacio vectorial de dimensión finita, entonces V es finito. La recíproca es cierta si $V \neq 0$

$$\dim_K V = n \Longrightarrow V \simeq K^n \Longrightarrow \not\in V = q^n.\ \not\in K = q.$$

$\not\in$ denota la cantidad de elementos

Recíproca. Si $v \in V$ y $v \neq 0$, $\varepsilon_v \colon K \longrightarrow V$ es monomorfismo: $k.v = 0 \Longrightarrow k = 0$. Luego, K es finito y $\not\in K \leq \not\in V$. Además, siendo V finito, cualquier sistema de generadores de V es finito.

ii) Grupos abelianos finitos.

Como se verá, pueden obtenerse a partir de grupos del tipo $\mathbb{Z}_n$, con $n \in \mathbb{N}$.

Definición. Un A-módulo M se dice de <u>tipo finito</u> (o <u>finitamente generado</u>) sii M tiene un sistema de generadores finito.

Ejemplo. Un K-espacio vectorial V es de tipo finito si, y sólo si, V tiene dimensión finita.

Proposición 4.9. *Dado un morfismo de A-módulos $f \colon M \longrightarrow N$, se verifica que M es finito si, y sólo si,* Ker f *e* Im f *son finitos. Equivalentemente, dados un A-módulo M y un submódulo S de M, se verifica que M es finito si, y sólo si, S y M/S son finitos.*

Demostración. Proposición $\Longrightarrow$ Enunciado. Aplicar la Proposición a la proyección $\pi \colon M \longrightarrow M/S$.

Enunciado $\Longrightarrow$ Proposición. Aplicar el Enunciado a M y Ker f, y usar el 1er. Teorema de isomorfismo.

Demostración del Enunciado. *Necesidad.* S es finito porque $S \subseteq M$. M/S es finito pues $M/S \subseteq \mathcal{P}(M)$.

Suficiencia. Dado $x \in M$, la aplicación de S en $x+S$, $s \mapsto x+s$ es biyectiva (tiene por inversa la aplicación de $x+S$ en S, $t \mapsto t-x$). Esto prueba que todo $u \in M/S$ es finito y que $\not\in u = \not\in S$. Luego, como $M = \cup M/S$ es unión de una cantidad finita de conjuntos finitos, resulta que M es finito; más aún, como es unión disjunta, $\not\in M = \sum_{u\in M/S} \not\in u = \not\in M/S.\not\in S$.

Este argumento vale en general: para todo A-módulo M y cualquier submódulo S de M.

Siendo F y F' conjuntos finitos, $\not\in F = \not\in F' \Longleftrightarrow$ existe una biyección de F en F'.

Sea $\mathcal{U}$ la clase universal, y sea $\sim$ la relación de equivalencia en $\mathcal{U}$ (coordinabilidad):

$$C \sim C' (C \text{ es coordinable con } C') \Longleftrightarrow \text{ existe una biyección de } C \text{ en } C'.$$

Se toma $\not{c} : \mathcal{U} \longrightarrow \mathcal{U}/\sim$ (cardinal) como la proyección, de modo que

$$\not{c}C = \not{c}C' \Longleftrightarrow C \sim C'.$$

F es finito y tiene n elementos $\Longleftrightarrow \not{c}F = \not{c}\mathbb{I}_n$.

Símbolo τ de Hilbert (Bourbaki). Universos de Sommerfeld (Grothendieck).

Siendo F y F' finitos, $F \cap F' = \emptyset \Longrightarrow \not{c}(F \cup F') = \not{c}F + \not{c}F'$.

Dada una familia $(c_i)_{i \in I}$ de cardinales, se define

$$\sum_{i \in I} c_i = \not{c}(\cup_{i \in I} C_i), \text{ si } c_i = \not{c}C_i \ (i \in I) \text{ y } C_i \cap C_j \neq \emptyset \Longrightarrow i = j \ (i, j \in I).$$

Buena definición:

i) Existencia de C_i $(i \in I)$. Tomar B_i tal que $\not{c}B_i = c_i$ y $C_i = \{i\} \times B_i$.

ii) Independencia de C_i $(i \in I)$.

Siendo F y F' finitos, $\not{c}(F \times F') = \not{c}F.\not{c}F'$.

Dados cardinales c y d, se define

$$c.d = \not{c}(C \times D), \text{ si } c = \not{c}C \text{ y } d = \not{c}D.$$

Buena definición: independencia de C y D.

Propiedad. $c_i = c \ (i \in I) \Longrightarrow \sum_{i \in I} c_i = \not{c}I.c$, pues $\cup_{i \in I} \{i\} \times C = I \times C$.

Sea M un A-módulo, y sea S un submódulo de M.

Definiciones. Se llama índice de S en M a $(M : S) = \not{c}M/S$; y se llama orden de M a $(M : 0) = \not{c}M$.

Observación. Vale la fórmula (Teorema de Lagrange):

$$(M : 0) = (M : S).(S : 0).$$

PROPOSICIÓN 4.10. *Dado un morfismo de A-módulos $f : M \longrightarrow N$, se verifica:*
i) Si M es de tipo finito, entonces $\operatorname{Im} f$ *es de tipo finito.*
ii) Si $\operatorname{Ker} f$ *e* $\operatorname{Im} f$ *son de tipo finito, entonces M es de tipo finito.*

Demostración. i) S sistema de generadores de M finito $\Longrightarrow f(S)$ sistema de generadores de $\operatorname{Im} f$ finito.

ii) Basta probar el

LEMA 4.11. *Dado un morfismo de A-módulos $f : M \longrightarrow N$, si S es un sistema de generadores de* $\operatorname{Ker} f$, *T es un sistema de generadores de* $\operatorname{Im} f$ *y U es una parte de M tal que $f(U) = T$, entonces $S \cup U$ es un sistema de generadores de M.*

Demostración. Dado $x \in M$, como $(t)_{t\in T}$ es una familia de generadores de $\operatorname{Im} f$, puede escribirse

$$f(x) = \sum_{t\in T} a_t.t, \text{ con } (a_t) \in A^{(T)}.$$

Para cada $t \in T$ se elige $u_t \in U$ tal que $f(u_t) = t$, con lo cual

$$f(x) = \sum_{t\in T} a_t f(u_t) = f\left(\sum_{t\in T} a_t u_t\right) \Longrightarrow x - \sum_{t\in T} a_t u_t \in \operatorname{Ker} f.$$

Luego, como $(s)_{s\in S}$ es una familia de generadores de $\operatorname{Ker} f$, puede escribirse

$$x - \sum_{t\in T} a_t u_t = \sum_{s\in S} b_s s, \text{ con } (b_s) \in A^{(S)};$$

y así,

$$x = \sum_{s\in S} b_s s + \sum_{t\in T} a_t u_t.$$

Dado $z \in S \cup U$, se toma

$$c_z = \begin{cases} b_z, & \text{si } z \in S \text{ y } z \neq u_t \ (t \in T), \\ a_t, & \text{si } z \notin S \text{ y } \exists\, t \in T : z = u_t \text{ (ojo: } u_t = u_{t'} \Longrightarrow t = t'), \\ b_z + a_t, & \text{si } z \in S \text{ y } \exists\, t \in T : z = u_t, \\ 0, & \text{si } z \notin S \text{ y } z \neq u_t \ (t \in T). \end{cases}$$

Luego,

$$x = \sum_{z\in S\cup U} c_z z. \square$$

Definición. Un A-módulo M se dice <u>cíclico</u> (o <u>monogénico</u>) sii M tiene un sistema de generadores de un elemento, vale decir, $M = Ax$, para algún $x \in M$.

Ejemplos. i) Los módulos nulos son cíclicos.

ii) A_s es cíclico.

iii) Sea A un anillo.

Definición. Un ideal $\mathfrak{A}$ se dice <u>principal</u> si, y sólo si, $\exists\, g \in \mathfrak{A}$, $\forall\, x \in \mathfrak{A}$, $\exists\, a \in A$: $x = a \cdot g$.

Observación. $\mathfrak{A}$ es principal, como ideal de A si, y sólo si, $\mathfrak{A}$ es cíclico, como submódulo de A_s.

iv) Un módulo simple es cíclico y no nulo; pero la recíproca no es cierta (considerar A_s, donde A es un anillo que no es de división).

v) $\mathbb{Z}$ es un grupo cíclico.

vi) $\mathbb{G}_n$ es un grupo cíclico ($n \in \mathbb{N}$).

Dado $w \in \mathbb{G}_n$,

$$w \text{ generador } \iff w^{\mathbb{Z}} = \mathbb{G}_n \iff \{w^i \mid 0 \leq i \leq n\} = \mathbb{G}_n \iff (w^i)_{0 \leq i < n}$$
$$\text{es una sucesión de elementos distintos} \underset{\text{def}}{\iff} w \text{ es primitiva}$$

Si $w_k = \cos \frac{2\pi k}{n} + \operatorname{sen} \frac{2\pi k}{n} \cdot i$ $(k \in \mathbb{Z})$, $(w_k)_{0 \leq k < n}$ es una numeración de $\mathbb{G}_n$ y se verifica:

$$w_k \text{ primitiva} \iff k \text{ y } n \text{ coprimos.}$$

Por ejemplo, w_1 es primitiva.

PROPOSICIÓN 4.12. *Dado un morfismo de A-módulos $f\colon M \longrightarrow N$, si M es cíclico, entonces* $\operatorname{Im} f$ *es cíclico.*

Demostración.

$$x \text{ generador de } M \Longrightarrow f(x) \text{ generador de } \operatorname{Im} f. \square$$

Ejemplo. $\mathbb{Z}_n$ es un grupo cíclico $(n \in \mathbb{N}_0)$. Considerar $\pi\colon \mathbb{Z} \longrightarrow \mathbb{Z}_n$.

PROPOSICIÓN 4.13. *Un A-módulo M es cíclico si, y sólo si, existe un epimorfismo de A_s en M.*

Demostración.Suficiencia. Por la proposición anterior, ya que A_s es cíclico.

Necesidad. Dado $x \in M$, se considera $\varepsilon_x\colon A_s \longrightarrow M$. Se tiene que $\operatorname{Im} \varepsilon_x = Ax = M\langle x \rangle$. Luego,

$$x \text{ generador de } M \iff \varepsilon_x \text{ epimorfismo.} \square$$

Ejemplo. Un grupo G es cíclico si, y sólo si, $G \simeq \mathbb{Z}_n$, para algún $n \in \mathbb{N}_0$. En particular, $\mathbb{G}_n \simeq \mathbb{Z}_n$ para todo $n \in \mathbb{N}$.

Suficiencia. $\mathbb{Z}_n$ es cíclico y se tiene un epimorfismo de $\mathbb{Z}_n$ en G.

Necesidad. Se tiene un epimorfismo $f\colon \mathbb{Z} \longrightarrow G$. Luego, como $\operatorname{Ker} f = n\mathbb{Z}$, para algún $n \in \mathbb{N}_0$, resulta que $G \simeq \mathbb{Z}_n$. $\mathbb{G}_n$ es cíclico $\Longrightarrow \exists\, n' \in \mathbb{N}_0 : \mathbb{G}_n \simeq \mathbb{Z}_{n'} \Longrightarrow n' \neq 0$ y $n = (\mathbb{G}_n : 1) = (\mathbb{Z}_{n'} : 0) = n'$.

COROLARIO 4.14. *Si M es un A-módulo cíclico, existe un ideal $\mathfrak{A}$ de A tal que para todo submódulo S de M resulta que $S \simeq \mathfrak{B}/\mathfrak{A}$, donde $\mathfrak{B}$ es un ideal de A tal que $\mathfrak{A} \subseteq \mathfrak{B}$.*

Demostración. Se considera un epimorfismo $f\colon A_s \longrightarrow M$; y se toma $\mathfrak{A} = \operatorname{Ker} f$.

$$\forall\, S \in \sigma(M),\ \exists\, \mathfrak{B} \in \sigma_{\mathfrak{A}}(A_s) : S = f(\mathfrak{B}).$$

Pero, como $\operatorname{Ker} f|_{\mathfrak{B}} = \operatorname{Ker} f \cap \mathfrak{B} = \mathfrak{A} \cap \mathfrak{B} = \mathfrak{A}$ e $\operatorname{Im} f|_{\mathfrak{B}} = f(\mathfrak{B}) = S$, resulta que $S \simeq \mathfrak{B}/\mathfrak{A}$.

Definición. Un anillo A se dice íntegro (o de integridad) si, y sólo si, cualesquiera sean $a, b \in A$

$$a.b = 0 \Longrightarrow a = 0 \vee b = 0,$$

vale decir,

$$a \neq 0 \wedge b \neq 0 \Longrightarrow a.b \neq 0$$

(de modo tal que el producto de A define una estructura de semigrupo en A^*).

Definición. Un dominio íntegro (o dominio de integridad) es un anillo íntegro y conmutativo.

Ejemplos. i) Todo anillo de división es íntegro. En particular, todo cuerpo es un dominio íntegro.
Sea A un anillo conmutativo.

ii) $\mathbb{M}_n(A)$ no es íntegro, si $n > 1$.

iii) $A[X]$ es íntegro si, y sólo si, A es íntegro.

Definición. Un anillo A se dice principal a izquierda (derecha) si, y sólo si todo ideal a izquierda (derecha) es principal.

Definición. Un dominio principal es un dominio íntegro que es principal.

Ejemplos. i) $\mathbb{Z}$ y $K[X]$ (K cuerpo) son dominios principales.

ii) Si A es un anillo conmutativo tal que $A[X]$ es un dominio principal, entonces A es un cuerpo.

Se toma $f \in A[X]$ mónico, con término constante nulo (por ejemplo, $f = X$). Dado $a \in A$, $a \neq 0$, sea $\mathfrak{A} = \langle a, f \rangle$, y sea g un generador de $\mathfrak{A}$.

$g|a \Longrightarrow grg = 0$.

$g|f \Longrightarrow g \in U(A) \Longrightarrow 1 \in \mathfrak{A} \Longrightarrow \exists r, s \in A[X] : 1 = ra + sf \Longrightarrow 1 = r(0)a + s(0)f(0) \Longrightarrow a \in U(A)$.

Proposición 4.15. *Un anillo A es principal si, y sólo si, todo submódulo de un A-módulo cíclico es cíclico.*

Demostración. Suficiencia. A_s es cíclico.

Necesidad. Sea M un A-módulo cíclico, y sea S un submódulo de M; entonces $S \simeq \mathfrak{B}/\mathfrak{A}$, donde $\mathfrak{A}$ y $\mathfrak{B}$ son ideales de A tales que que $\mathfrak{A} \subseteq \mathfrak{B}$. Componiendo la proyección de $\mathfrak{B}$ en $\mathfrak{B}/\mathfrak{A}$ con un isomorfismo de $\mathfrak{B}/\mathfrak{A}$ en S, se obtiene un epimorfismo de $\mathfrak{B}$ en S; pero $\mathfrak{B}$ es cíclico, de donde S lo es.

Definición. Un A-módulo M se dice localmente cíclico si, y sólo si, todo submódulo de M de tipo finito es cíclico.

Sea A un dominio íntegro. Se define una relación de equivalencia $\sim$ en $A \times A^*$ pniendo $(a, b) \sim (c, d) \Longleftrightarrow a.d = b.c$. Sea $K = A \times A^*/\sim$, y sea $\pi \colon A \times A^* \longrightarrow K$ la proyección. Dados $a, b \in A$, $b \neq 0$, $\pi(a, b)$ se nota $\frac{a}{b}$, de modo que

$$\frac{a}{b} = \frac{c}{d} \Longleftrightarrow a.d = c.b.$$

Se definen + y . para K en la forma

$$\frac{a}{b}+\frac{c}{d}=\frac{a.d+b.c}{b.d}, \tag{1}$$

$$\frac{a}{b}.\frac{c}{d}=\frac{a.c}{b.d}. \tag{2}$$

+ y . están bien definidas y $(K,+,.)$ es un cuerpo (ejercicio), llamado el cuerpo de fracciones de A. Por ejemplo, $\frac{0}{1}$ es el elemento neutro de + y $-\frac{a}{b}=\frac{-a}{b}$; $\frac{1}{1}$ es el elemento neutro de . y si $\frac{a}{b}\neq\frac{0}{1}$ ($\frac{a}{b}=\frac{0}{1}\iff a=0$), $\left(\frac{a}{b}\right)^{-1}=\frac{b}{a}$. La aplicación $\varphi\colon A\longrightarrow K$, $\varphi(a)=\frac{a}{1}$ satisface:

i) $\varphi(a)=\varphi(b)\Longrightarrow a=b$.

ii) $\varphi(a+b)=\varphi(a)+\varphi(b)$.

iii) $\varphi(a.b)=\varphi(a).\varphi(b)$.

Luego, puede identificarse A con $\operatorname{Im}\varphi=\{\frac{a}{1}\,|\,a\in A\}$; y con tal identificación, $\frac{a}{b}=a.b^{-1}$:

$$\frac{a}{b}=\frac{a}{1}.\frac{1}{b}=\frac{a}{1}.\left(\frac{b}{1}\right)^{-1}=\varphi(a).\varphi(b)^{-1}.$$

K puede considerarse como A-módulo a través de φ:

$$a\cdot_\varphi x=\varphi(a).x\qquad(a\in A,x\in K).$$

Sea A un dominio íntegro, de cuerpo de fracciones K.

Definición. Se llama ideal fraccionario de A a un submódulo $\mathfrak{A}$ de K que

$$\exists\, c\in K\ :\ c\neq 0\wedge c\mathfrak{A}\in A.$$

Observación. i) En la definición, puede elegirse $c\in A$. Si $c=\frac{a}{b}$, $a\neq 0$ (pues $c\neq 0$) y $a\overset{A}{=}(bc)\mathfrak{A}=b(c\mathfrak{A})\subseteq bA\subseteq A$.

ii) Todo ideal es un ideal fraccionario.

Tomar $c=1$.

iii) Todo ideal fraccionario es isomorfo a un ideal.

Sea $f\colon K\longrightarrow K$ la aplicación $f(x)=c.x$ $(x\in K)$. f es un morfismo de A-módulos inyectivo ($c\neq 0$). Luego, $\mathfrak{A}\simeq f(\mathfrak{A})$; pero $f(\mathfrak{A})=c\mathfrak{A}$, como submódulo de K contenido en A, resulta un ideal de A.

iv) Todo submódulo de K de tipo finito es un ideal fraccionario de A. Sea $\mathfrak{A}$ un tal submódulo, y sea $(x_i)_{i\in I}$ una familia finita de generadores de $\mathfrak{A}$. Si $x_i=\frac{a_i}{b_i}$, se toma $c=\prod_{i\in I}b_i$, con lo cual $cx_i\in A$ $(i\in I)$; y así, $c\mathfrak{A}\subseteq A$:

$$c\sum_{i\in I}d_ix_i=\sum_{i\in I}d_i(cx_i)\in A$$

Proposición 4.16. *Si A es un dominio principal, K es un A-módulo localmente cíclico.*

Demostración. Por iv), basta ver que todo ideal fraccionario de A es cíclico, lo que resulta de iii). $\square$

Ejemplos. i) $\mathbb{Q}$ es un grupo localmente cíclico.
ii) Si K es un cuerpo, $K(X)$ es un $K[X]$-módulo localmente cíclico.

5. Módulos noetherianos y módulos artinianos

Sea M un A-módulo, y sea $\mathcal{C}$ un conjunto de submódulos de M.

Definición. Un submódulo S de M se dice maximal (minimal) en $\mathcal{C}$ si, y sólo si:
i) $S \in \mathcal{C}$.
ii) $T \in \mathcal{C} \wedge S \subseteq T \ (S \supseteq T) \Longrightarrow S = T$.

Observación. Si $\mathcal{C} = \sigma(M) - \{M\}$ $(\mathcal{C} = \sigma(M) - \{0\})$, entonces S es maximal (minimal) en $\mathcal{C}$ si, y sólo si, S es maximal (minimal).
Sea $(S_i)_{i\in\mathbb{N}}$ una sucesión de submódulos de M.

Definición. Se dice que $(S_i)_{i\in\mathbb{N}}$ es creciente (decreciente) si y sólo si

$$S_i \subseteq S_{i+1} \ (S_i \supseteq S_{i+1}) \qquad (i \in \mathbb{N}),$$

vale decir,

$$i \leq j \Longrightarrow S_i \subseteq S_j \ (S_i \supseteq S_j) \qquad (i, j \in \mathbb{N}).$$

Definición. Se dice que $(S_i)_{i\in\mathbb{N}}$ es estacionaria (o casiconstante) si y sólo si,

$$\exists\, n \in \mathbb{N}, \forall\, i \in \mathbb{N} \ : \ i \geq n \Longrightarrow S_i = S_n.$$

Proposición 5.1. *Dado un A-módulo M, son equivalentes:*
i) Todo conjunto no vacío de submódulos de M tiene algún elemento maximal (minimal).
ii) Toda sucesión creciente (decreciente) de submódulos de M es estacionaria.

Demostración. i) $\Longrightarrow$ ii). Sea $(S_i)_{i\in\mathbb{N}}$ una sucesión creciente en $\sigma(M)$, y sea $\mathcal{C} = \{S_i \,|\, i \in \mathbb{N}\}$. Como $\emptyset \neq \mathcal{C} \subseteq \sigma(M)$, sea $n \in \mathbb{N}$ tal que S_n es maximal en $\mathcal{C}$; entonces,

$$i \geq n \Longrightarrow S_i \supseteq S_n \Longrightarrow S_i = S_n.$$

ii) $\Longrightarrow$ i). Sea $\emptyset \neq \mathcal{C} \subseteq \sigma(M)$. Suponiendo que $\mathcal{C}$ no tiene elementos maximales, se define inductivamente una sucesión $(S_i)_{i\in\mathbb{N}}$ en $\mathcal{C}$ por: $S_1 \in \mathcal{C}$ $(\mathcal{C} \neq \emptyset)$; y supuesto definido

$S_h \in \mathcal{C}$, para un cierto $h \in \mathbb{N}$, se elige $S_{h+1} \in \mathcal{C}$ tal que $S_h \subset S_{h+1}$ (S_h no es maximal en $\mathcal{C}$). Por construcción, $(S_i)_{i\in\mathbb{N}}$ es una sucesión strictamente creciente:

$$S_i \subset S_{i+1} \ (i \in \mathbb{N});$$

y en consecuencia, es una sucesión creciente no estacionaria. □

Observación. Toda sucesión creciente (decreciente) de submódulos de M, que no es estacionaria, tiene una subsucesión estrictamente creciente (decreciente). Sea $(S_i)_{i\in\mathbb{N}}$ una sucesión en $\sigma(M)$ creciente y no estacionaria. Como "no estacionaria" significa

$$\forall\, n \in \mathbb{N}, \exists\, i \in \mathbb{N} \ : \ i > n \wedge S_i \neq S_n,$$

siendo creciente, se tiene que

$$\forall\, n \in \mathbb{N}, \exists\, i \in \mathbb{N} \ : \ i > n \wedge S_i \supset S_n.$$

Se define inductivamente una sucesión $(i_j)_{j\in\mathbb{N}}$ en $\mathbb{N}$ por: $i_1 \in \mathbb{N}$; y supuesto definido $i_h \in \mathbb{N}$, para un cierto $h \in \mathbb{N}$, se elige $i_{h+1} \in \mathbb{N}$ tal que $i_{h+1} > i_h$ y $S_{i_{h+1}} \supset S_{i_h}$. Por construcción, $(S_{i_j})_{j\in\mathbb{N}}$ es una subsucesión estrictamente creciente

Definición. Un A-módulo M se dice noetheriano (artiniano) si, y sólo si, M satisface una de las condiciones –y en consecuencia, la otra– de la Proposición.

Ejemplos. i) Los módulos simples, los módulos finitos y –más generalmente– los módulos con una cantidad finita de submódulos son noetherianos y artinianos.

Sea M un A-módulo, y sea $\emptyset \neq \mathcal{C} \subseteq \sigma(M)$. Si $\mathcal{C}$ es finito, entonces $\mathcal{C}$ tiene elementos maximales y elementos minimales.

Por la demostración de ii) $\Longrightarrow$ i) de la Proposición, si $\mathcal{C}$ no tiene elementos maximales, resulta que $\mathcal{C}$ es infinito. También puede procederse por inducción en $n = \not\in\mathcal{C}$. El caso $n = 1$ es trivial (el único elemento de $\mathcal{C}$ es maximal). Sea $n = h + 1$, con $h \in \mathbb{N}$; se toma $S \in \mathcal{C}$ y se considera $\mathcal{C}' = \mathcal{C} - \{S\}$. Por la hipótesis inductiva, $\mathcal{C}'$ tiene algún elemento maximal T. Si $T \not\subseteq S$, T es maximal en $\mathcal{C}$:

$$U \in \mathcal{C} \wedge T \subseteq U \Longrightarrow U \neq S \Longrightarrow U \in \mathcal{C}' \Longrightarrow T = U.$$

Si $T \subseteq S$, entonces S es maximal en $\mathcal{C}$:

$$U \in \mathcal{C} \wedge S \subseteq U \Longrightarrow T \subseteq U \Longrightarrow T = U \Longrightarrow S \subseteq T \Longrightarrow S = T; \text{ absurdo.}$$

ii) Los espacios vectoriales de dimensión finita son noetherianos y artinianos.

Sea V un K-espacio vectorial de dimensión finita, y sea $\emptyset \neq \mathcal{C} \subseteq \sigma(V)$. Si $C = \{\dim S \ : \ S \in \mathcal{C}\}$, entonces $\emptyset \neq C \subseteq \mathbb{N}_0$, de modo que C tiene mínimo. Sea, entonces, $S \in \mathcal{C}$ un espacio de dimensión mínima; S resulta minimal en $\mathcal{C}$:

$$T \in \mathcal{C} \wedge T \subseteq S \Longrightarrow \dim T \in C \wedge \dim T \leq \dim S \Longrightarrow \dim T = \dim S \Longrightarrow T = S.$$

En realidad, C es finito, porque $\dim V$ es una cota superior de C; y así, C tiene máximo. Sea, entonces, $S \in \mathcal{C}$ un subespacio de dimensión máxima; S resulta maximal en $\mathcal{C}$:

$$T \in \mathcal{C} \wedge S \subseteq T \Longrightarrow \dim T \in C \wedge \dim S \leq \dim T \Longrightarrow \dim S = \dim T \Longrightarrow S = T.$$

iii) Los espacios vectoriales de dimensión infinita no son noetherianos ni artinianos.

Sea V un K-espacio vectorial de dimensión infinita (vale decir, que no tiene dimensión finita).

Se define una sucesión $(v_i)_{i\in\mathbb{N}}$ en V por inducción global en la forma: supuesto definidos $v_i \in V$ para $1 \leq i \leq n$, con $n \in \mathbb{N}$, se elige $v_n \in V$ tal que v_n no es combinación lineal de $(v_i)_{1\leq i<n}$ ($(v_i)_{1\leq i<n}$ no es una familia de generadores de V).

Si $S_i = \langle v_j\rangle_{j\leq i}$, entonces $S_i \subset S_{i+1}$: $S_i \subseteq S_{i+1}$, pues $\{v_j \,|\, j \leq i\} \subseteq \{v_j \,|\, j \geq i+1\}$; y $S_{i+1} \nsubseteq S_i$, pues $v_{i+1} \in S_{i+1}$ y $v_{i+1} \notin S_i$.

Si $T_i = \langle v_j\rangle_{j\geq i}$, entonces $T_i \supset T_{i+1}$: $T_i \supseteq T_{i+1}$, pues $\{v_j \,|\, j \geq i\} \supseteq \{v_j \,|\, j \geq i+1\}$; y $T_{i+1} \nsupseteq T_i$, pues $v_i \in T_i$ y $v_{i+1} \notin T_{i+1}$. En efecto, si $v_i \in T_{i+1}$, puede escribirse $v_i = \sum_{j\geq i+1} k_j v_j$, con $k_j \in K$ $(j \geq i+1)$. Tomando $n = \max \operatorname{sop}_{j\geq i+1} k_j$, se tiene que $\operatorname{sop}_{j\geq i+1} k_j \subseteq \{j \,|\, i+1 \leq j \leq n\}$, con lo cual $v_i = \sum_{i+1\leq j\leq n} k_j v_j$. Luego, $v_n = \sum_{1\geq j<n} k'_j v_j$, con

$$k'_j = \begin{cases} 0, & \text{si } 1 \leq i, \\ 1/k_n, & \text{si } j = i, \\ -k_j/k_n, & \text{si } i+1 \leq j \leq n. \end{cases}$$

Proposición 5.2. *Si M es un A-módulo noetheriano (artiniano), se verifica:*
i) Todo submódulo S de M es noetheriano (artiniano).
ii) Dado un epimorfismo $f\colon M \longrightarrow\!\!\!\!\!\rightarrow N$, N resulta noetheriano (artiniano).

Demostración. i) es trivial, pues $\sigma(S) \subseteq \sigma(M)$.

ii) Sea $\emptyset \neq \mathcal{C} \subseteq \sigma(N)$; entonces $\emptyset \neq f^{-1}(\mathcal{C}) = \{f^{-1}(S) \,|\, S \in \mathcal{C}\} \subseteq \sigma(M)$, con lo cual existe $S \in \mathcal{C}$ tal que $f^{-1}(S)$ es maximal en $f^{-1}(\mathcal{C})$. Se afirma que S es maximal en $\mathcal{C}$:

$$T \in \mathcal{C} \wedge S \subseteq T \Longrightarrow f^{-1}(T) \in f^{-1}(\mathcal{C}) \wedge f^{-1}(S) \subseteq f^{-1}(T) \Longrightarrow f^{-1}(S) = f^{-1}(T)$$
$$\Longrightarrow S = T,$$

pues $f^*\colon \sigma(N) \longrightarrow\!\!\!\!\!\rightarrow \sigma(M)$ es inyectiva: $f_* \circ f^* = i_{\sigma(N)}$, siendo f epimorfismo.

Proposición 5.3. *Dado un morfismo de A-módulos $f\colon M \longrightarrow\!\!\!\!\!\rightarrow N$, si $\operatorname{Ker} f$ e $\operatorname{Im} f$ son noetherianos (artinianos), entonces M es noetheriano (artiniano).*

Demostración. Sea $(S_i)_{i\in\mathbb{N}}$ una sucesión creciente en $\sigma(M)$. Como $(S_i \cap \operatorname{Ker} f)_{i\in\mathbb{N}}$ es una sucesión creciente en $\sigma(\operatorname{Ker} f)$,

$$\exists\, p \in \mathbb{N},\ \forall\, i \in \mathbb{N} \,:\, i \geq p \Longrightarrow S_i \cap \operatorname{Ker} f = S_p \cap \operatorname{Ker} f.$$

Como $(f(S_i))_{i\in\mathbb{N}}$ es una sucesión creciente en $\sigma(\operatorname{Im} f)$,

$$\exists\, q \in \mathbb{N},\ \forall\, i \in \mathbb{N} \,:\, i \geq q \Longrightarrow f(S_i) = f(S_q).$$

Tomando $n \in \mathbb{N}$ tal que $n \geq \max\{p, q\}$,

$$i \geq n \Longrightarrow S_i \cap \operatorname{Ker} f = S_n \cap \operatorname{Ker} f \ \wedge \ f(S_i) = f(S_n).$$

Luego, queda probado que

$$i \geq n \Longrightarrow S_i = S_n$$

aplicando el

LEMA 5.4. *Dado un morfismo de A-módulos $f\colon M \longrightarrow N$, si S y T son submódulos de M tales que $S \subseteq T$, $S \cap \operatorname{Ker} f = T \cap \operatorname{Ker} f$ y $f(S) = f(T)$, entonces $S = T$.*

Demostración.

$$x \in T \Longrightarrow f(x) \in f(T) \Longrightarrow f(x) \in f(S) \Longrightarrow \exists\, y \in S : f(x) = f(y)$$
$$\Longrightarrow x - y \in \operatorname{Ker} f \cap T \Longrightarrow x - y \in S \Longrightarrow x \in S.\square$$

LEMA 5.5. *Si M es una A-módulo noetheriano, para toda parte C de M existe una parte finita F de C tal que $M\langle C\rangle = M\langle F\rangle$.*

Demostración. Sea $\mathcal{C} = \{\langle F\rangle \,|\, F \in \mathcal{F}(C)\}$. Como $\mathcal{C} \neq \emptyset$, sea $F \in \mathcal{F}(C)$ tal que $\langle F\rangle$ es maximal en $\mathcal{C}$. Se afirma que $\langle C\rangle = \langle F\rangle$. Es claro que $\langle F\rangle \subseteq \langle C\rangle$, pues $F \subseteq C$. Por otra parte,

$$\langle C\rangle \subseteq \langle F\rangle \Longleftrightarrow C \subseteq \langle F\rangle \Longleftrightarrow \forall\, x \in C : x \in \langle F\rangle;$$

pero, dado $x \in C$,

$$\left.\begin{array}{rl} F \in \mathcal{F}(C) \Longrightarrow & F \cup \{x\} \in \mathcal{F}(C) \\ F \subseteq F \cup \{x\} \Longrightarrow & \langle F\rangle \subseteq \langle F \cup \{x\}\rangle \end{array}\right\} \Longrightarrow \langle F\rangle = \langle F \cup \{x\}\rangle \Longrightarrow x \in \langle F\rangle.\square$$

LEMA 5.6. *Un A-módulo M es noetheriano si, y sólo si, todo submódulo de M es de tipo finito.*

Demostración. Necesidad. Si S es un módulo de M, aplicando el lema,

$$\exists\, F \in \mathcal{F}(S) : M\langle S\rangle = M\langle F\rangle.$$

Suficiencia. Sea $(S_i)_{i\in\mathbb{N}}$ una sucesión creciente de submódulos de M, y sea $U = \cup_{i\in\mathbb{N}} S_i$. Según un resultado anterior, U es un submódulo de M. Sea, entonces, F un sistema de generadores de U finito. Como $F \subseteq U$,

$$\forall\, x \in F, \exists\, i_x \in \mathbb{N} : x \in S_{i_x}.$$

Tomando $n = \max\{i_x | x \in F\}$ (n cualquiera, si $F = \emptyset$), como $S_{i_x} \subseteq S_n$ ($x \in F$), resulta que $F \subseteq S_n$, de donde $U = \langle F\rangle \subseteq S_n$. Por lo tanto,

$$i \geq n \Longrightarrow S_i = S_n.\square$$

Definiciones. Un anillo A se dice noetheriano a izquierda (derecha) si y sólo si, A_s (A_d) es un módulo noetheriano.

Un anillo A se dice artiniano a izquierda derecha) si y sólo si, A_s (A_d) es un módulo artiniano.

Ejemplos. i) Las álgebras de dimensión finita son anillos noetherianos y artinianos.

Dado un morfismo de anillos $f\colon A \longrightarrow B$, todo B-módulo M puede considerarse como A-módulo a través de $f : a \cdot_f x = f(a) \cdot x$ ($a \in A$, $x \in M$). Si $S \subseteq M$,

$$S \text{ es } \quad B - \text{estable} \Longrightarrow S \text{ es } \quad A - \text{estable},$$

con lo cual

$$S \text{ es } \quad B - \text{submódulo} \Longrightarrow S \text{ es } \quad A - \text{submódulo},$$

vale decir $\sigma_B(M) \subseteq \sigma_A(M)$. Luego, si M es noetheriano (artiniano) como A-módulo, resulta que M es noetheriano (artiniano) como B-módulo. Sea K un cuerpo y sea A una K-álgebra de dimensión finita. Si e es la identidad de A, se considera la transformación lineal $f = \varepsilon_e\colon K \longrightarrow A$; f resulta un morfismo de anillos

$$f(k{\cdot}k') = (k{\cdot}k'){\cdot}e = (k{\cdot}k'){\cdot}(e{\cdot}e) = k{\cdot}(k'{\cdot}(e{\cdot}e)) = k{\cdot}(e{\cdot}(k'{\cdot}e)) = (k{\cdot}e){\cdot}(k'{\cdot}e) = f(k){\cdot}f(k'),$$

$$f(1) = e.$$

Además, al considerar A como K-espacio vectorial a través de f, se obtiene la acción original:

$$k \cdot_f v = f(k) \cdot v = (k \cdot e) \cdot v = k \cdot (e \cdot v) = k \cdot v.$$

Luego, como A es K-noetheriano y artiniano, resulta que A es A-noetheriano y artiniano.

ii) Los anillos principales son noetherianos.

iii) Sea A un anillo:

Definición. Se dice que A es un divisor de cero a izquierda (derecha) si, y sólo si, $\exists\, b \in A : b \neq 0 \ \wedge\ b \cdot a = 0$ ($a \cdot b = 0$).

Observación. Son equivalentes:

i) A no tiene divisores de cero a izquierda $\neq 0$. $\quad \forall\, a \in A^*, \forall\, b \in A : b{\cdot}a = 0 \Longrightarrow b = 0.$

ii) A no tiene divisores de cero a derecha $\neq 0$. $\quad \forall\, a \in A^*, \forall\, b \in A : a{\cdot}b = 0 \Longrightarrow b = 0.$

iii) A es íntegro $\qquad\qquad\qquad\qquad\qquad\qquad \forall\, a, b \in A : a \cdot b = 0 \Longrightarrow a = 0 \vee b = 0.$

Si $c \in A$ no es divisor de cero a izquierda ni inversible a izquierda, entonces $(Ac^i)_{i \in \mathbb{N}}$ es estrictamente decreciente. Luego, si A es un anillo íntegro que no es de división, entonces A no es artiniano, ni a izquierda ni a derecha.

$$Ac^i \supseteq Ac^{i+1} \ : \ c^{i+1} = c \cdot c^i \in Ac^i.$$
$$Ac^i \not\subseteq Ac^{i+1} \ : \ c^i \notin Ac^{i+1}, \text{ pues :}$$

$$c^i \in Ac^{i+1} \Longrightarrow \exists\, a \in A \,:\, c^i = ac^{i+1} \Longrightarrow (ac-1)c^i = 0 \Longrightarrow ac - 1 = 0$$
$\Longrightarrow c$ es inversible a izquierda.

iv) $\mathbb{Z}$ y $K[X]$ (K cuerpo) son anillos noetherianos, pero no artinianos

v) Los ideales fraccionarios de un dominio noetheriano son de tipo finito.

PROPOSICIÓN 5.7. *Un anillo A es noetheriano (artiniano) si, y sólo si, todo A-módulo de tipo finito es noetheriano (artiniano).*

Demostración. Suficiencia. A_s es de tipo finito (es cíclico).
Necesidad. Sea M un A-módulo de tipo finito, y sea F un sistema de generadores de M finito. Se procede por inducción en $n = \not\sharp F$. El caso $n = 0$ (o sea, $F = \emptyset$) es trivial. Suponiendo $n > 0$, se toma $g \in F$ y se considera $S = M\langle F - \{g\}\rangle$. Por la hipótesis inductiva, S es noetheriano. Luego, empleando la proyección $\pi\colon M \longrightarrow\!\!\!\!\rightarrow M/S$, queda probado que M es noetheriano mostrando que M/S lo es; pero M/S es cíclico:

F sistema de generadores de $M \Longrightarrow \pi(F)$ sistema de generadores de M/S
$\Longrightarrow \pi(g)$ generadores de M/S.

Por lo tanto, basta ver que si C es un A-módulo cíclico, entonces C es noetheriano. En efecto, existe un epimorfismo de A_s en C.□

6. TORSIÓN Y DIVISIBILIDAD

Para un K-espacio vectorial V, se verifica:
i) $\forall\, k \in K, \forall\, v \in V \,:\, k \cdot v = 0 \Longrightarrow k = 0 \vee v = 0$.
ii) $\forall\, v \in V, \forall\, k \in K^*, \exists\, w \in V \,:\, v = k \cdot w$.
Sea M un A-módulo.

Notaciones: Si A, M_a nota $\operatorname{Ker}\eta_{a,M} = \{x \in M \mid a \cdot x = 0\}$, que es un subgrupo de M (si $a \in C(A)$, es un submódulo). Si $x \in M$, $A_n(x)$ (anulador de x) nota $\operatorname{Ker}\varepsilon_x = \{a \in A \mid a \cdot x = 0\}$, que es un ideal de A.

Definiciones. Se dice que $x \in M$ es sin torsión (o linealmente independiente) si y sólo si, $A_n(x) = 0$, o sea, $\forall\, a \in A \,:\, a \cdot x = 0 \Longrightarrow a = 0$.
Se dice que x es de torsión (o linealmente dependiente) si y sólo si, x no es sin torsión, vale decir, $A_n(x) \neq 0$, o explícitamente, $\exists\, a \in A \,:\, a \neq 0 \wedge a \cdot x = 0$.
Se llama torsión de M al conjunto $t(M)$ de elementos de M que son de torsión.
Se dice que M es de torsión si, y sólo si, $tM = M$, o sea, todo elemento de M es de torsión.

Se dice que M es sin torsión si, y sólo si, $tM = 0$, vale decir, 0 es el único elemento de torsión.

Propiedades:
i) $tM = \cup_{a \in A^*} M_a$.
ii) M es de torsión y sin torsión si, y sólo si, $M = 0$.
iii) M es sin torsión si, y sólo si, $\eta_{a,M}$ es un monomorfismo (de grupos) ($a \in A^*$).

Ejemplos. i) *Definición.* Un A-módulo M se dice mixto si, y sólo si, M no es de torsión y M no es sin torsión, vale decir, $\{0\} \subset tM \subset M$.

Por ejemplo, $\mathbb{R}/\mathbb{Z}$ es un grupo mixto, pues $t(\mathbb{R}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z}$.

Dado $u \in \mathbb{R}/\mathbb{Z}$, sea $u = \pi(x)$, con $x \in \mathbb{R}$.

$$u \text{ es de torsión} \iff \exists\, m \in \mathbb{Z} : m \neq 0 \wedge m \cdot u = 0 \iff \exists\, m \in \mathbb{Z} : m \neq 0 \wedge m \cdot x \in \mathbb{Z}$$
$$\iff x \in \mathbb{Q}.$$

$\therefore t(\mathbb{R}/\mathbb{Z}) = \pi(\mathbb{Q}) = \mathbb{Q}/\mathbb{Z}$.

Siendo $\pi_0 \colon \sigma(\mathbb{R}) \longrightarrow \sigma(\mathbb{R}/\mathbb{Z})$ inyectiva (es biyectiva),

$$\mathbb{Q} \neq \mathbb{Z}, \mathbb{R} \Longrightarrow \pi(\mathbb{Q}) \neq \pi(\mathbb{Z}), \pi(\mathbb{R}).$$

ii) Si A es un anillo infinito y M es un A-módulo finito, entonces M es de torsión. (Por ejemplo, los grupos finitos son de torsión.)

Si $x \in M$, $\varepsilon_x \colon A_s \longrightarrow M$ no es mono, vale decir, $A_n(x) \neq 0$. El resultado vale para $\not\in M < \not\in A$:

Siendo F y F' conjuntos finitos, $\not\in F \leq \not\in F' \iff$ existe una inyección de F en F'. Si c y d son cardinales, $c = \not\in C$ y $d = \not\in D$, se define

$$c \leq d \iff \text{existe una inyección de } C \text{ en } D.$$

Buena definición: independencia de C y D.

r) $c \leq c$.
a) $c \leq d \wedge d \leq c \Longrightarrow c = d$ (Cantor-Bernstein).
t) $c \leq d \wedge d \leq e \Longrightarrow c \leq e$.

También se define

$$c < d \iff c \leq d \wedge c \neq d.$$

Si A es un anillo infinito y M es un A-módulo localmente finito, entonces M es de torsión. (Por ejemplo los grupos localmente finitos son de torsión.)

Dado $x \in M$, considerar $\langle x \rangle$.

iii) *Definición.* Un A-módulo M se dice acotado si y sólo si, $a \cdot M = 0$, para algún $a \in A$, $a \neq 0$.

Si A es un dominio íntegro y M es un A-módulo de torsión finitamente generado (por ejemplo, M finito, si A es infinito), entonces M es acotado. (Así los grupos finitos son acotados.)

Sea $(x_i)_{i\in I}$ una familia finita de generadores de M, y sea $a_i \in A^*$ tal que $a_i \cdot x_i = 0$ $(i \in I)$. Si $a = \prod_{i\in I} a_i$, entonces $a \neq 0$; y dado $j \in I$, $a \cdot x_j = 0$, pues $a = \prod_{i\neq j} a_i \cdot a_j$. Luego, $a \cdot M = 0$:

$$x_i \in M_a \ (i \in I) \Longrightarrow M = M\langle x_i\rangle_{i\in I} \subseteq M_a.$$

Sea G un grupo. "G acotado" significa "$\exists\, n \in \mathbb{N} : nG = 0$". Si G es finito, puede tomarse $n = (G : 0)$; más aún, puede tomarse $n = \exp G$, para G acotado (comentario).

iv) Si A es un anillo tal que $A/\mathfrak{A}$ es finito para todo ideal $\mathfrak{A} \neq 0$, y M es un A-módulo de torsión finitamente generado, entonces M es finito. (Por ejemplo, los grupos de torsión fintamente generados son finitos.)

Sea $(x_i)_{i\in I}$ una familia finita de generadores de M. Como $M = \sum_{i\in I} M\langle x_i\rangle$, basta probar que M es finito en elcaso que M es cíclico. En efecto, si x es un generador de M, entonces $M \simeq A/A_n(x)$ y $A_n(x) \neq 0$.

Si A es un anillo tal que $A/\mathfrak{A}$ es finito para todo ideal $\mathfrak{A}ne0$, y M es un A-módulo de torsión, entonces M es localmente finito. (Por ejemplo, los grupos de torsión son localmente finitos.)

Todo submódulo de M es de torsión.

v) Sea $p \in \mathbb{Z}$, $p \neq 0$. $S_p = \left\{\frac{m}{p^n} \,|\, m \in \mathbb{Z} \wedge n \in \mathbb{N}_0\right\}$ es un subgrupo de $\mathbb{Q}$, que contiene a $\mathbb{Z}$.

Notación. $\mathbb{Z}_{p^\infty} = S_p/\mathbb{Z}$.

$\mathbb{Z}_{p^\infty}$ es un grupo de torsión; y no es acotado, si $p \neq \pm 1$. Dado $u \in \mathbb{Z}_{p^\infty}$, si $u = \pi\left(\frac{m}{p^n}\right)$, con $m \in \mathbb{Z}$ y $n \in \mathbb{N}_0$, entonces $p^n \cdot u = \pi(m) = 0$. Sea $a \in \mathbb{Z}$ tal que $a \cdot \mathbb{Z}_{p^\infty} = 0$. Si $n \in \mathbb{N}_0$,

$$a \cdot \pi\left(\frac{1}{p^n}\right) \Longrightarrow \frac{a}{p^n} \in \mathbb{Z} \Longrightarrow p^n | a \Longrightarrow |p|^n \leq |a|;$$

absurdo, pues $|p| > 1$.

Sea p primo.

Definición. Un grupo G se dice p-cuasicíclico si, y sólo si, los subgrupos propios de G admiten una numeración $(S_n)_{n\in\mathbb{N}_0}$ tal que S_n es un grupo cíclico de orden p^n $(n \in \mathbb{N}_0)$.

Comentario. Resulta $S_n \subseteq S_{n+1} (n \in \mathbb{N}_0)$ y $G = \cup_{n\in\mathbb{N}_0} S_n$. Dos grupos p-cuasicíclicos son isomorfos. $\mathbb{Z}_{p^\infty}$ es un grupo p-cuasicíclico.

Un grupo cuasicíclico, siendo un grupo no cíclico, cuyos subgrupos propios son finitos, resulta de torsión.

Un grupo cuasicíclico no es noetheriano (o sea, no es de tipo finito); pero es artiniano.

vi) Sea A umn dominio íntegro, y sea K el cuerpo de fracciones de A. Si S es un submódulo de K tal que $A \subseteq S$, entonces S/A es una A-módulo de torsión. En consecuencia, K/A y $A_{p^\infty} = \{\frac{a}{p^n} \,|\, a \in A \wedge n \in \mathbb{N}_0\}/A$ $(p \in A, p \neq 0)$ son de torsión. (Por ejemplo, $\mathbb{Q}/\mathbb{Z}$ y $\mathbb{Z}_{p^\infty}$ son grupos de torsión.)

Dado $u \in S/A$, si $u = \pi(\frac{a}{b})$, con $a, b \in A$ y $b \neq 0$, entonces $b \cdot u = \pi(a) = 0$.

vii) Si A es un anillo y $\mathfrak{A}$ es un ideal de A, entonces $A/\mathfrak{A}$ es de torsión si, y sólo si, $\forall\, a \in A$, $\exists\, b \in A^* : b \cdot a \in \mathfrak{A}$. En particular, si $\mathfrak{A}$ es un ideal bilátero, $A/\mathfrak{A}$ resulta de torsión; mas aún, acotado (fijar $b \in \mathfrak{A}$, $b \neq 0$).

viii) Sea A un anillo. Dado $a \in A$,

$$a \in t(A_s) \Longleftrightarrow a \text{ divisor de cero a izquierda.}$$
$$a \in t(A_d) \Longleftrightarrow a \text{ divisor de cero a derecha.}$$

Luego, son equivalentes:
.) A_s es sin torsión.
..) A_d es sin torsión.
...) A s íntegro.

ix) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ son sin torsión como módulos sobre los precedentes.
Un A-módulo M es sin torsión si, y sólo si, $\forall\, a \in A$, $\forall\, x \in M : a \cdot x = 0 \Longrightarrow a = 0 \vee x = 0$. En nuestro caso, $A \subseteq\subseteq M \subseteq \mathbb{C}$ y la acción de A en M está dada por el producto de $\mathbb{C}$, de modo que se satisface la condición enunciada.

x) Los espacios vectoriales son sin torsión; pero son localmente finitos cuando el cuerpo de escalares es finito.

xi) Sea A un dominio íntegro, un cuerpo de fracciones K. Si V es un K-espacio vectorial, entonces V es un A-módulo sin torsión. (Por ejemplo, si V es un $\mathbb{Q}$-espacio vectorial, V resulta un grupo sin torsión.)

Proposición 6.1. *Si A es un dominio íntegro, para todo A-módulo M se verifica que tM es un submódulo de M.*

Demostración.
i) $0 \in tM$, pues $1 \neq 0$ y $1 \cdot 0 = 0$.
ii) $x, y \in tM \Longrightarrow \exists\, a, b \in A : a, b \neq 0,\ a \cdot x = 0,\ b \cdot y = 0 \Longrightarrow a \cdot b \neq 0 \wedge (a.b) \cdot (x+y) = (a.b) \cdot x + (a.b) \cdot y = (b.a) \cdot x + (a.b) \cdot y = b \cdot (a \cdot x) + a \cdot (b \cdot y) = b \cdot 0 + a \cdot 0 = 0$.
iii) $a \in A \wedge x \in tM \Longrightarrow \exists\, b \in A : b \neq 0 \wedge b \cdot x = 0 \Longrightarrow b \cdot (a \cdot x) = (b \cdot a) \cdot x = (a \cdot b) \cdot x = a \cdot (b \cdot x) = a \cdot 0 = 0$.□

Definición. Siendo A conmutativo, se define

$$a|b \Longleftrightarrow \exists\, c \in A : a \cdot c = b.$$

$|$ es filtrante:

$$\forall\, a, b \in A : a|a \cdot b \wedge b|a \cdot b.$$

Si A también es íntegro, $|$ es filtrante en A^*. Luego, $tM = \cup_{a\in A^*} M_a$ es un submódulo de M, ya que

$$a|b \Longrightarrow M_a \subseteq M_b \qquad (a, b \in A).$$

PROPOSICIÓN 6.2. *Sea A un dominio íntegro. Dado un A-módulo M, se verifica:*
i) tM es el máximo submódulo de M de torsión.
ii) Si S es un submódulo de M, $tS = S \cap tM$. En particular, si M es de (sin) torsión, entonces S es de (sin) torsión.
iii) M/tM es sin torsión.
iv) Todo morfismo de A-módulos $f\colon M \longrightarrow N$ induce un morfismo $t(f)\colon tM \longrightarrow tN$. Si M es de torsión y f es un epimorfismo, entonces N es de torsión. Además, valen las fórmulas:

$$\begin{aligned} t(g \circ f) &= tg \circ tf, \\ t(i_m) &= i_{t(M)}, \\ t(f + f') &= tf + tf', \\ t(c \cdot f) &= c \cdot tf \qquad (c \in C(A)). \end{aligned}$$

Demostración. i) Significa:
.) tM es un submódulo de M y tM es sin torsión.
..) Si S es un submódulo de M y S es de torsión, entonces $S \subseteq tM$
ii) es trivial.
iii) Debe probarse que, si $a \in A^*$ y $x \in M$,

$$\begin{array}{ccc} a \cdot x \in tM & \Longrightarrow & x \in tM \\ \Downarrow & & \Uparrow \\ \exists\, b \in A^* : b \cdot (a \cdot x) = 0 & \Longrightarrow & b \cdot a \neq 0 \wedge (b \cdot a) \cdot x = 0 \end{array}$$

iv) Se tiene que $f(tM) \subseteq tN$, pues $a \cdot x = 0 \Longrightarrow a \cdot f(x) = 0$. Se define, entonces, $tf = f|_{tM}|^{tN}\colon tM \longrightarrow tN$. Siendo f epimorfismo y M de torsión, $N = f(M) = f(tM) \subseteq tN$. Las fórmulas son triviales, pues $tf(x) = f(x)$ $(x \in tM)$.□

Observación. "... es sin torsión" no es una propiedad mórfica. Por ejemplo, si A es un dominio íntegro, que no es un cuerpo, y $\mathfrak{A}$ es un ideal de A tal que $\mathfrak{A} \neq 0, A$, considerar la proyección $\pi\colon A \longrightarrow A/\mathfrak{A}$.

Comentario. Sean A y B anillos. Supóngase que

$$\begin{aligned} M \in \mathfrak{M}_s(A) &\mapsto F(M) \in \mathfrak{M}_s(B), \\ f \in \mathrm{Hom}_A(M, N) &\mapsto f(f) \in \mathrm{Hom}_B(F(M), F(N)) \begin{cases} F(g \circ f) = F(g) \circ F(f), \\ F(i_M) = i_{F(M)}. \end{cases} \end{aligned}$$

En tal caso, se dice que F es un <u>funtor</u> de A-módulos en B-módulos. F se dice aqditivo si, y sólo si, $F(f+f')=F(f)+F(f')$.

Si A es un dominio íntegro. t es un funtor aditivo de A-módulos en A-módulos.

$$\mathcal{C}\begin{cases}\text{objetos}: (M,S)|M \in \mathfrak{M}_s(A) \wedge S \in \sigma(M)\\ \text{morfismos}: f\colon (M,S)\longrightarrow(N,T)|f \in \mathrm{Hom}_A(M,N) \wedge f(S)\subseteq T\end{cases}$$

$$(M,S)\mapsto M/S,$$
$$f\colon (M,S)\longrightarrow(N,T)\mapsto \overline{f}\colon M/S\longrightarrow N/T.$$

"módulo cociente" es un funtor de $\mathcal{C}$ en A-módulos.

Sea M un A-módulo.

Notación. Si $a \in A$, $a\cdot M$ nota $\mathrm{Im}\,\eta_{a,M}=\{x \in M|\exists\, y \in M : x=a\cdot y\}$, que es un subgrupo de M (si $a \in C(A)$, es un submódulo).

Definiciones. Se dice que $x \in M$ es <u>divisible por</u> $a \in A$ si, y sólo si, $x \in a\cdot M$, o sea, $\exists\, y \in M : x=a\cdot y$.

Se dice que x es <u>divisible</u> si, y sólo si, x es divisible por todo $a \in A$, $a\neq 0$.

Se llama <u>divisibilidad</u> de M al conjunto $d(M)$ de elementos de M que son divisibles.

Se dice que M es <u>divisible</u> si, y sólo si, $dM=M$, vale decir, todo elemento de M es divisible.

Se dice que M es <u>indivisible</u> si, y sólo si, $dM=0$, o sea, 0 es el único elemento de M que es divisible.

Propiedades:

0) x es divisible por 0 si, y sólo si, $x=0$.

i) $dM=\cap_{a\in A^*}aM$.

ii) M es divisible e indivisible si, y sólo si, $M=)$.

iii) M es divisible si, y sólo si, $\eta_{a,M}$ es un epimorfismo (de grupos) $(a \in A^*)$.

$$dM=M \Longleftrightarrow M\subseteq dM \Longleftrightarrow M\subseteq aM(a\in A^*)\Longleftrightarrow aM=M(a\in A^*).$$

Ejemplos. i) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ son divisibles, como grupos abelianos o como módulos sobre los precedentes.

Un A-módulo M es divisible si, y sólo si, $\forall\, x \in M$, $\forall\, a \in A^*$, $\exists\, y \in M : x=a\cdot y$. (*) En nuestro caso, $A\subseteq M\subseteq\mathbb{C}$ y la acción de A en M está dada por el producto de $\mathbb{C}$. Además,

$$a \in A^* \Longrightarrow a^{-1}\in M.$$
$$x,y \in M \Longrightarrow x\cdot y \in M.$$

Luego, en (*) basta tomar $y=a^{-1}\cdot x$.

ii) Los espacios vectoriales son divisibles.

iii) Sea A un dominio íntegro, con cuerpo de fraccioines K. Si V es un K-espacio vectorial, etnonces V es un A-módulo divisible. (Por ejemplo, si V es un $\mathbb{Q}$-espacio vectorial, V rewsulta un grupo divisible.)

iv) Los grupos cuasicíclicos son divisibles.

Sea G un grupo infinito tal que todo subgrupo propio de G es finito (por ejemplo, G cuasicíclico). Si f es un endomorfismo no nulo de G, entonces f es un epimorfismo.

$$\operatorname{Im} f \neq G \Longrightarrow \operatorname{Im} f \text{ finito} \Longrightarrow G \text{ finito}.$$

Luego, si G es un grupo cuasicíclico, basta ver que $\eta_{a,G} \neq 0$, si $a \in \mathbb{Z}$ es no nulo.

Demostración para $\mathbb{Z}_{p^\infty}$ $(p \neq \pm 1)$. Escribiendo $a = p^n \cdot b$, con $n \in \mathbb{N}_0$ y $b \in \mathbb{Z}$ tal que $p \nmid b$, $a \cdot \pi\left(\frac{1}{p^{n+1}}\right) = \pi\left(\frac{a}{p^{n+1}}\right) = \pi\left(\frac{b}{p}\right) \neq 0$, pues $\frac{b}{p} \notin \mathbb{Z}$.

v) Sea A un anillo. A_s es divisible si, y sólo si, A es un anillo de división.

"A_s divisible" significa "$\forall\, x \in A,\ \forall\, a \in A^*,\ \exists\, y \in A : x = a \cdot y$", vale decir, "$\forall\, a \in A^* : aA = A$", o sea, "$A_d$ simple".

vi) $\mathbb{Z}$ es un grupo indivisible. Dado $x \in \mathbb{Z}$ y $m \in \mathbb{Z}^*$,

$$x \text{ divisible por } m \Longleftrightarrow m|x.$$

Luego, para $x \in \mathbb{Z}$,

$$x \text{ divisible } \Longleftrightarrow \forall\, m \in \mathbb{Z}^* : m|x \Longleftrightarrow x = 0.$$

Proposición 6.3. *Para todo A-módulo M se verifica que dM es un subgrupo de M; y si A es conmutativo, dM es un submódulo de M.*

Demostración. Se sabe que $dM = \cap_{a \in A^*} aM$.$\square$

Proposición 6.4. *Sea A un anillo conmutativo. Dado un A-módulo M, se verifica:*

i) dM es el máximo submódulo de M cuyos elementos son divisibles en M.

ii) Si S es un submódulo de M, $dS \subseteq S \cap dM$. En particular, si M es indivisible, entonces S lo es.

ii bis) Si A también es íntegro, $d(tM) = t(dM) = dM \cap tM$.

iii) M/dM es indivisible.

iv) Todo morfismo de A-módulos $f\colon M \longrightarrow N$ induce un morfismo $d(f)\colon dM \longrightarrow dN$. Si M es divisible y f es un epimorfismo, entonces N es divisible. Además, valen las fórmulas:

$$d(g \circ f) = dg \circ df, \quad d(i_M) = i_{dM}, \quad d(f + f') = df + df', \quad d(c \cdot f) = c \cdot df \ (c \in C(A)).$$

Demostración. i) significa:

.) dM es un submódulo de M y los elementos de dM son divisibles en M.

..) Si S es un submódulo de M y los elementos de S son divisibles en M, entonces $S \subseteq dM$.

ii) Dados $x \in S$ y $a \in A$,

$$x \text{ divisible por } a \text{ en } S : \exists\, y \in S : x = a \cdot y.$$
$$x \text{ divisible por } a \text{ en } M : \exists\, z \in M : x = a \cdot z.$$

Luego,

$$x \text{ divisible por } a \text{ en } S \Longrightarrow x \text{ divisible por } a \text{ en } M;$$

y así,

$$x \text{ divisible en } S \Longrightarrow x \text{ divisible en } M.$$

ii bis) Tomando $S = dM$ en $tS = S \cap tM$, resulta $t(dM) = dM \cap tM$; y tomando $S = tM$ en $dS \subseteq S \cap tM$, resulta $d(tM) \subseteq tM \cap dM$.

$dM \cap tM \subseteq d(tM)$. Sea $x \in M$ divisible y de torsión; y sea $c \in A^*$ tal que $c \cdot x = 0$. Dado $a \in A^*$, si $x = a \cdot y$, con $y \in M$, se tiene que $c \cdot a \neq 0$ y $(c \cdot a) \cdot y = c \cdot (a \cdot y) = c \cdot x = 0$.

iii) Debe probarse que, dado $x \in M$,

$$\forall\, a \in A^*, \exists\, y \in M : x - a \cdot y \in dM \Longrightarrow x \in dM.$$

En efecto, $x - a \cdot y = a \cdot z$, para algún $z \in M$, con lo cual $x = a \cdot (y + z)$.

iv) Se tiene que $f(dM) \subseteq dN$, pues $x = a \cdot y \Longrightarrow f(x) = a \cdot f(y)$. Completar (ejercicio).□

Observación. i) "...es divisible" no es una propiedad hereditaria. Por ejemplo, si A es un dominio íntegro, que no es cuerpo, y K es el cuerpo de fracciiones de A, considerar A como submódulo de K. En consecuencia, no vale la fórmula $dS = S \cap dM$.

ii) "...es indivisible" no es una propiedad mórfica. Por ejemplo, dado un primo p, considerar la proyección $\pi\colon S_p \longrightarrow \mathbb{Z}_{p^\infty}$.

S_p es p-divisible:

$$\frac{a}{p^n} = p^m \cdot \frac{a}{p^{m+n}}.$$

Sea $x \in S_p$ divisible. Se toma un primo $q \neq p$. Si $x = \frac{a}{p^n}$, con $a \in \mathbb{Z}$ y $n \in \mathbb{N}_0$

$$\frac{a}{p^n} = q^m \cdot \frac{b}{p^r} \Longrightarrow p^r a = p^n q^m b \Longrightarrow q^m | p^r a \Longrightarrow q^m | a.$$

Luego, $a = 0$.

iii) Si A es cualquier anillo, d es un funtor aditivo de A-módulos en $\mathbb{Z}$-módulos; en A-módulos si A es conmutativo.

Comentario sobre ????

Definición. Sea M un A-módulo. un submódulo S de M se dice <u>puro</u> si, y sólo si, $S \cap a \cdot M = a \cdot S$ $(a \in A)$, vale decir, $S \cap a \cdot M \subseteq S$ $(a \in A^*)$.

Proposición 6.5. *Dado un A-módulo M, se verifica:*

i) Si T es un submódulo puro de M y S es un submódulo puro de T, entonces S es un submódulo puro de M.

ii) Si S es un submódulo divisible de M, entonces S es un submódulo puro de M.

iii) Si S es un submódulo puro de M, entonces $dS = S \cap dM$. En particular, si M es divisible, S resulta divisible.

iv) Si S es un submódulo de M tal que M/S es sin torsión, entonces S es un submódulo puro de M.

v) Si A es un dominio íntegro, tM es un submódulo puro de M

vi) Si M es sin torsión y S es un submódulo puro de M, entonces M/S es sin torsión.

vii) Si $(S_i)_{i\in I}$ es una familia de submódulos puros de M y M es sin torsión, entonces $\cap_{i\in I} S_i$ es un submódulo puro de M.

viii) Si I es un conjunto filtrante no vacío y $(S_i)_{i\in I}$ es una familia creciente de submódulos puros de M, entonces $\cup_{i\in I} S_i$ es un submódulo puro de M.

Demostración. i)

$$S \cap aM = (S \cap T) \cap aM = S \cap (T \cap aM) = S \cap aT = aS \ (a \in A).$$

ii)

$$S \cap aM \subseteq S = aS \ (a \in A^*).$$

iii)

$$dS = \bigcap_{a\in A^*} aS = \bigcap_{a\in A^*} (S \cap aM) = S \cap (\bigcap_{a\in A^*} aM) = s \cap dM.$$

iv) Debe probarse que, dados $a \in A^*$ y $x \in M$,

$$a \cdot x \in S \Longrightarrow x \in S \Longrightarrow a \cdot x \in a \cdot S$$

v) sigue de iv).

vi) Debe probarse que, dados $a \in A^*$ y $x \in M$,

$$\begin{array}{ccc} a \cdot x \in S & \Longrightarrow & x \in S \\ \Downarrow & & \Uparrow \\ a \cdot x \in A \cdot S \Longrightarrow & \exists y \in S : a \cdot x = a \cdot y & \Longrightarrow x = y \end{array}$$

vii)

$$a \cdot \bigcap_{i\in I} S_i = \eta_a \left(\bigcap_{i\in I} S_i \right) = \bigcap_{i\in I} \eta_a(S_i) = \bigcap_{i\in I} a \cdot S_i = \bigcap_{i\in I} (S_i \cap a \cdot M) = \left(\bigcap_{i\in I} S_i \right) \cap a \cdot M \ (a \in A^*)$$

*) Dada una aplicación de conjuntos $f\colon C \longrightarrow D$, si $(S_i)_{i\in I}$ es una familia de subconjuntos de C, entonces $f(\cap_{i\in I} S_i) \subseteq \cap_{i\in I} f(S_i)$; y si $I \neq \emptyset$ y f es inyectiva, vale $=$.

*) Con las notaciones anteriores, $f(\cup_{i\in I} S_i) = \cup_{i\in I} f(S_i)$.

7. Producto directo y suma directa

Repaso conjuntista

$$C \times D = \{(x, y) \,|\, x \in C \wedge y \in D\}$$

Definición. $\{x, y\} = \{z \,|\, z = x \vee z = y\}$ (par no ordenado de x e y).
Propiedad. $\{x, y\} = \{y, x\}$.
Definición. $(x, y) = \{\{x\}, \{x, y\}\}$.
Propiedad. $(x, y) = (x', y') \Longleftrightarrow x = x' \wedge y = y'$. $\therefore x \neq y \Longrightarrow (x, y) \neq (y, x)$.

$$P = \{f \,|\, f\colon \{1, 2\} \longrightarrow C \cup D \wedge f(1) \in C \wedge f(2) \in D\}.$$

$P \underset{\psi}{\overset{\varphi}{\rightleftarrows}} C \times D$, $\varphi(f) = (f(1), f(2))$, $\psi(x, y)(1) = x \wedge \psi(x, y)(2) = y$.

$\varphi \circ \psi = i_{C\times D} : \varphi(\psi(x, y)) = (\psi(x, y)(1), \psi(x, y)(2)) = (x, y)$.
$\varphi \circ \psi = i_P : \psi(\varphi(f)) = f : \psi(\varphi(f))(1) = \psi(f(1), f(2))(1) = f(1)$.

Sea $(C_i)_{i\in I}$ una familia de conjuntos.

Definición. Se llama producto cartesiano de $(C_i)_{i\in I}$ a

$$\underset{i\in I}{X} = \{f \,|\, f\colon I \longrightarrow \cup_{i\in I} C_i \wedge f(i) \in C_i \ (i \in I)\}.$$

Observaciones. i) Dados conjuntos C y D, si se toma $I = \{1, 2\}$, $C_1 = C$ y $C_2 = D$, las aplicaciones $\underset{i\in I}{X} C_i \underset{\psi}{\overset{\varphi}{\rightleftarrows}} C \times D$ dadas por

$$\varphi(f) = (f(1), f(2)), \quad \psi(x, y)(1) = x \wedge \psi(x, y)(2) = y$$

son recíprocas.

ii) Dado un conjunto C, tomando $C_i = C$ $(i \in I)$ resulta que $\underset{i\in I}{X} C_i = C^I$.

iii) Es trivial que

$$\underset{i\in I}{X} C_i \neq \emptyset \Longrightarrow C_i \neq \emptyset \quad (i \in I).$$

La recíproca,

$$C_i \neq \emptyset \quad (i \in I) \Longrightarrow \underset{i\in I}{X} C_i \neq \emptyset,$$

es el axioma de elección para $(C_I)_{i\in I}$.

Definición. Dado $j \in I$, se llama proyección j-ésima de $\underset{i\in I}{X} C_i$ a la aplicación $p_j\colon \underset{i\in I}{X} C_i \longrightarrow C_j$ dada por

$$p_j(x) = x_j \quad (x \in \underset{i\in I}{X} C_i).$$

Observaciones. i) Dados $x, x' \in \underset{i\in I}{X} C_i$,

$$x = x' \Longleftrightarrow p_i(x) = p_i(x') \quad (i \in I).$$

ii) Dado un conjunto C y aplicaciones $f, g\colon C \longrightarrow \underset{i\in I}{X} C_i$, se verifica que

$$f = g \Longleftrightarrow p_i \circ f = p_i \circ g \quad (i \in I).$$

$f = g \Longleftrightarrow f(z) = g(z) \quad (z \in C) \Longleftrightarrow p_i(f(z)) = p_i(g(z)) \quad (z \in C, i \in I) \Longleftrightarrow (p_i \circ f)(z) = (p_i \circ g)(z) \quad (z \in C, i \in I) \Longleftrightarrow p_i \circ f = p_i \circ g \quad (i \in I)$.

iii) Dado $j \in I$, si $C_i \neq \emptyset$ $(i \in I, i \neq j)$, entonces p_j es suryectiva.

Dado $z \in C_j$, se elige $x_i \in C_i$ para $i \neq j$ (axioma de elección para $(C_i)_{i\in I, i\neq j}$) y se define $x_j = z$. Luego, $x = (x_i)_{i\in I} \in \underset{i\in I}{X} C_i$ y $p_j(x) = z$.

Sea $(M_i)_{i\in I}$ una familia de A-módulos.

Proposición 7.1. *Existe una única estructura de A-módulo en $\underset{i\in I}{X} M_i$ tal que $p_j\colon \underset{i\in I}{X} M_i \longrightarrow M_j$ es un morfismo, para todo $j \in I$.*

Demostración. Sea $P = \underset{i\in I}{X} M_i$. Se definen $+$ y $\cdot$ para P en la forma:

$$\left.\begin{array}{c} (x + x')_i = x_i +_{M_i} x_i' (\Longleftrightarrow p_i(x + x') = p_i(x) + p_i(x')), \\ (a \cdot x)_i = a \cdot_{M_i} x_i (\Longleftrightarrow p_i(a \cdot x) = a \cdot p_i(x)), \end{array}\right\} (*)$$

vale decir,

$$(x_i)_{i\in I} + (x_i')_{i\in I} = (x_i + x_i')_{i\in I},$$
$$a \cdot (x_i)_{i\in I} = (a \cdot x_i)_{i\in I}.$$

Se verifica que $(P, +, \cdot)$ es una A-módulo (ejercicio); y p_i es un morfismo, según $\Longrightarrow$ en $(*)$. La unicidad de la estructura resulta de $\Longleftarrow$ en $(*)$.$\square$

Observaciones. i) Dados A-módulos M y N, se considera $M \times N$ con la estructura de A-módulo :

$$(x, y) + (x', y') = (x +_M x', y +_M y'),$$
$$a \cdot (x, y) = (a \cdot_M x, a \cdot_N y).$$

Entonces, tomando $I = \{1, 2\}$, $M_1 = M$ y $M_2 = N$, las aplicaciones $\underset{i\in I}{X} M_i \underset{\psi}{\overset{\varphi}{\rightleftarrows}} M \times N$ dadas por

$$\varphi(z) = (z_1, z_2), \qquad \psi(x, y)_1 = x \wedge \psi(x, y)_2 = y$$

son morfismos recíprocos.

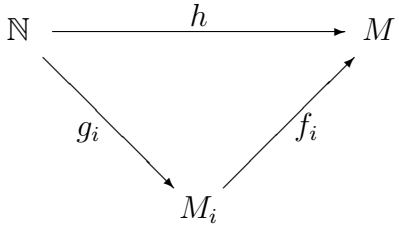
ii) Dado un A-módulo M, tomando $M_i = M$ $(i \in I)$ resulta $\underset{i\in I}{X} M_i = M^I$, como A-módulos.

iii) $\underset{i\in I}{X} = 0 \Longleftrightarrow M_i = 0$ $(i \in I)$.

$\Longrightarrow$. p_i es epimorfismo $(i \in I)$.

$\Longleftarrow$. Dado $x \in \underset{i\in I}{X} M_i$, como $x_i \in M_i$, resulta $x_i = 0$ $(i \in I)$.

Definición. Se llama producto directo (o producto) de $(M_i)_{i\in I}$ a un objeto $(M, (f_i)_{i\in I})$, donde M es un A-módulo y f_i es un morfismo de M en M_i $(i \in I)$, que satisface: si $(N, (g_i)_{i\in I})$ es un objeto de la misma especie, existe un único morfismo $h\colon N \longrightarrow M$ que hace conmutativo el diagrama

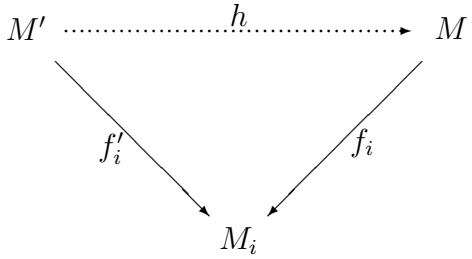


vale decir, $f_i \circ h = g_i$ $(i \in I)$.

Consistencia de la definición. i) Unicidad. Si $(M, (f_i)_{i\in I})$ y $(M', (f'_i)_{i\in I})$ son productos directos de $(M_i)_{i\in I}$, existe un único isomorfismo $h\colon M' \longrightarrow M$ tal que $f_i \circ h = f'_i$ $(i \in I)$.

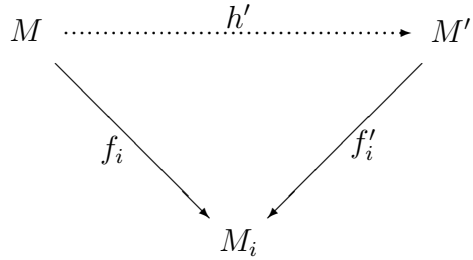
ii) Existencia. $(\underset{i\in I}{X} M_i, (p_i)_{i\in I})$ es un producto directo de $(M_i)_{i\in I}$.

Demostración. i) Como $(M, (f_i)_{i\in I})$ satisface la definición y $(M', (f'_i)_{i\in I})$ es un tal objeto,



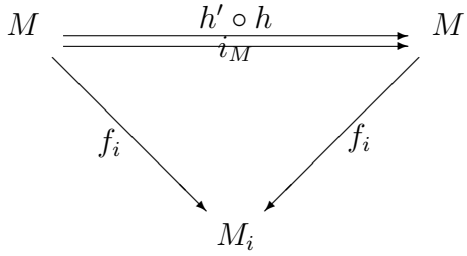
$\exists!\, h : f_i \circ h = f'_i$ $(i \in I)$.

Queda por verificar que h es un isomorfismo. Como $(M', (f'_i)_{i\in I})$ satisface la definición y $(M, (f_i)_{i\in I})$ es un tal objeto,



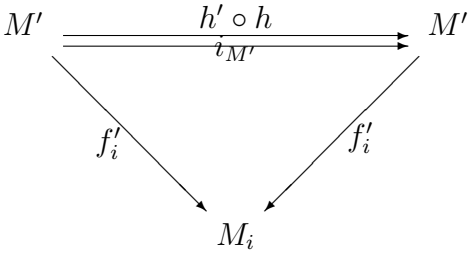
$\exists!\, h' : f'_i \circ h' = f_i \ (i \in I)$.

Se afirma que h' es el morfismo inverso de h. En efecto, como $(M, (f_i)_{i\in I})$ satisface la definición, por razones de unicidad,



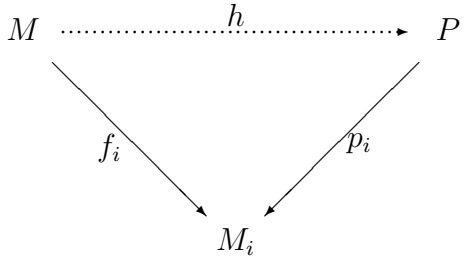
$f_i \circ (h \circ h') = f_i \wedge f_i \circ i_M = f_i \ (i \in I) \Longrightarrow h \circ h' = i_M$.

También, como $(M', (f'_i)_{i\in I})$ satisface la definición, por las mismas razones,



$f'_i \circ (h' \circ h) = f'_i \wedge f'_i \circ i_{M'} = f'_i \ (i \in I) \Longrightarrow h' \circ h = i_{M'}$.

ii) Sea $P = \underset{i\in I}{X} M_i$. Debe probarse que, dados un A-módulo M y morfismos $f_i \colon M \longrightarrow M_i \ (i \in I)$,



$\exists!\, h : p_i \circ h = f_i \ (i \in I)$.

Existencia de h. Definimos $h(x)_i = f_i(x) \ (i \in I)$, o sea, $h(x) = (f_i(x))_{i\in I}$. $p_i \circ h = f_i$ $(i \in I)$. Por definición, $p_i(h(x)) = f_i(x) \ (i \in I)$. h es un morfismo,

$$h(x + x')_i = f_i(x + x') = f_i(x) + f_i(x') = h(x)_i + h(x')_i = (h(x) + h(x'))_i \ (i \in I)$$
$$\Longrightarrow h(x + x') = h(x) + h(x'),$$

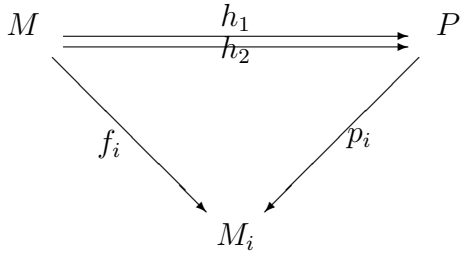
o también,

$$h(x + x') = (f_i(x + x'))_{i\in I} = (f_i(x) + f_i(x'))_{i\in I} = (f_i(x))_{i\in I} + (f_i(x'))_{i\in I} = h(x) + h(x')$$
$$h(a \cdot x)_{i\in I} = f_i(a \cdot x) = a \cdot f_i(x) = a \cdot h(x)_i = (a \cdot h(x))_i \ (i \in I) \Longrightarrow h(a \cdot x) = a \cdot h(x),$$

o también,

$$h(a \cdot x) = (f_i(a \cdot x))_{i \in I} = (a \cdot f_i(x))_{i \in I} = a \cdot (f_i(x))_{i \in I} = a \cdot h(x).$$

Unicidad de h. Debe probarse que, dados morfismos $h_1, h_2 \colon M \longrightarrow P$,



$$p_i \circ h_1 = f_i \wedge p_i \circ h_2 = f_i \ (i \in I) \Longrightarrow p_i \circ h_1 = p_i \circ h_2 \ (i \in I) \Longrightarrow h_1 = h_2.$$

Notación. Dados un A-módulo M y morfismos $f_i \colon M \longrightarrow M_i$ $(i \in I)$, el factorizador $h \colon M \longrightarrow \underset{i \in I}{X} M_i$ se nota $\prod_{i \in I} f_i$, vale decir, $(\prod_{i \in I} f_i)(x) = (f_i(x))_{i \in I}$ $(x \in M)$.

Observación. $\operatorname{Ker} \prod_{i \in I} f_i = \cap_{i \in I} \operatorname{Ker} f_i$. En particular, si existe $j \in I$ tal que f_j es un monomorfismo, entonces $\prod_{i \in I} f_i$ es un monomorfismo.

Ejemplos. i) Dado $j \in I$, se define un morfismo $f_{ji} \colon M_j \longrightarrow M_i$ $(i \in I)$ tomando

$$f_{ji} = \begin{cases} i_{M_j}, & \text{si } i = j, \\ 0_{M_j, M_i}, & \text{si } i \neq j. \end{cases}$$

Sea $u_j = \prod_{i \in I} f_{ji} \colon M_j \longrightarrow \underset{i \in I}{X} M_i$ (<u>inyección j-ésima</u> de $\underset{i \in I}{X} M_i$), vale decir, u_j está unívocamente determinado por las condiciones $p_i \circ u_j = f_{ji}$ $(i \in I)$. En particular, $p_j \circ u_j = i_{M_j}$, con lo cual p_j es una retracción y u_j es una sección. Explícitamente,

$$u_j(x)_i = \begin{cases} x, & \text{si } i = j, \\ 0, & \text{si } i \neq j. \end{cases}$$

ii) Dado un A-módulo M,tomando $M_i = M$ $(i \in I)$ se define un morfismo $f_i \colon M \longrightarrow M_i$ por : $f_i = i_M$ $(i \in I)$. Sea $\Delta = \prod_{i \in I} f_i \colon M \longrightarrow \underset{i \in I}{X} M_i = M^I$ (<u>diagonal</u> de M_i), vale decir Δ está unívocamente determinado por las condiciones $p_i \circ \Delta = i_M$ $(i \in I)$. En particular, si $I \neq \emptyset$, Δ es una sección. Explícitamente, $\Delta(x)_i = x$ $(i \in I)$.

Proposición 7.2. *Se verifica:*

i) Si π es una permutación de I, entonces $\underset{i \in I}{X} M_{\pi(i)} \simeq \underset{i \in I}{X} M_i$.

ii) Si $(I_j)_{j \in J}$ es una partición de I (en realidad, puede permitirse $I_j = \emptyset$), entonces $\underset{j \in J}{X} \left(\underset{i \in I_j}{X} M_i \right) \simeq \underset{i \in I}{X} M_i$.

Demostración. Sea $P = \underset{i\in I}{X} M_i$, y sean $p_i \colon P \longrightarrow M_i$ $(i \in I)$ las proyecciones.

i) Sea $P' = \underset{i\in I}{X} M_{\pi(i)}$, y sean $p'_i \colon P' \longrightarrow M_{\pi(i)}$ $(i \in I)$ las proyecciones. Computacionalmente se defines una aplicación $h \colon P' \longrightarrow P$ por

$$h(x')_i = x'_{\pi^{-1}(i)} \qquad (i \in I),$$

vale decir,

$$h(x') = (x'_{\pi^{-1}(i)})_{i\in I}.$$

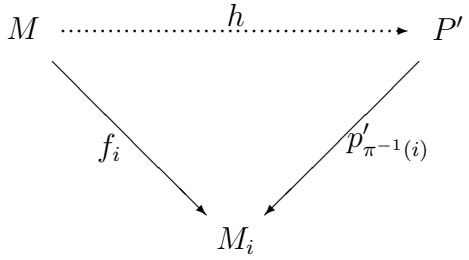
h es un morfismo (ejercicio). h es biyectiva, pues tiene por inversa la aplicación $h' \colon P \longrightarrow P'$ definida tomando $h'(x)_i = x_{\pi(i)}$ $(i \in I)$. En efecto, $h \circ h' = i_P$:

$$h(h'(x))_i = h'(x)_{\pi^{-1}(i)} = x_{\pi(\pi^{-1}(i))} = x_i \ (i \in I) \Longrightarrow h(h'(x) = x;$$

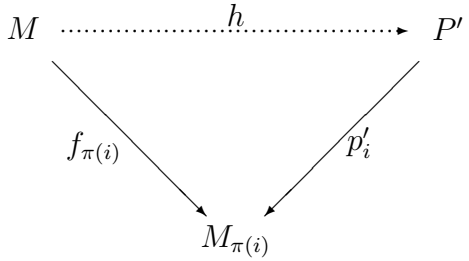
y también, $h' \circ h = i_{P'}$ (ejercicio).

Conceptualmente, basta ver que $(P', (p'_{\pi^{-1}(i)})_{i\in I})$ es un producto directo de $(M_i)_{i\in I}$, pues -en tal caso- existe un único isomorfismo $h \colon P' \longrightarrow P$ tal que $p_i \circ h = p'_{\pi^{-1}(i)}$ $(i \in I)$, a saber: $h = \prod_{i\in I} p'_{\pi^{-1}(i)}$, vale decir, $h(x') = (p'_{\pi^{-1}(i)}(x'))_{i\in I} = (x'_{\pi^{-1}(i)})_{i\in I}$.

En consecuencia, dados un A-módulo M y morfismo $f_i \colon M \longrightarrow M_i$ $(i \in I)$, debe probarse que



$\exists\,! h : p'_{\pi^{-1}(i)} \circ h = f_i$ $(i \in I) \iff ((\Longrightarrow)$ índice $\pi(i)$. $(\Longleftarrow)$ índice $\pi^{-1}(i).)$



$\exists\,! h : p'_i \circ h = f_{\pi(i)}$ $(i \in I)$
y esto último es cierto, porque $P', (p'_i)_{i\in I})$ es un producto directo de $(M_{\pi(i)})_{i\in I}$.

ii) Sea $P' = \underset{j\in J}{X}(\underset{i\in I_j}{X} M_i)$.

Computacionalmente. Se define una aplicación $h \colon P' \longrightarrow P$ por

$$h(x')_i = x'_{ji}, \text{ si } i \in I_j.$$

h está bien definida, porque

$$\forall\, i \in I, \quad \exists!\, j \in J : i \in I_j.$$

Si $\sigma\colon I \longrightarrow J$ es la aplicación $\sigma(i) = j$, si $i \in I_j$, entonces

$$h(x') = (x'_{\sigma(i)i})_{i\in I}.$$

h es un morfismo (ejercicio). h es biyectiva, pues tiene por inversa la aplicación $h'\colon P \longrightarrow P'$ dada por

$$h'(x)_{ji} = x_i \ \ (i \in I_j),$$

vale decir,

$$h'(x) = ((x_i)_{i\in I_j})_{j\in J}.$$

En efecto, $h \circ h' = i_P$:

$$\text{si } i \in i_J : \qquad h(h'(x))_i = h'(x)_{ji} = x_i \ \ (i \in I) \Longrightarrow h(h'(x)) = x;$$

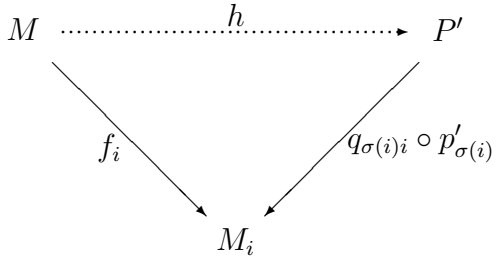
y también, $h' \circ h = i_{P'}$:

$$h' \circ h(x'))_{ji} = h(x')_i = x'_{ji} \ \ (i \in I_j) \Longrightarrow h'(h(x'))_j = x'_j \ \ (j \in J) \Longrightarrow h'(h(x')) = x'.$$

Conceptualmente. Sea $N_j = \underset{i\in I_j}{X} M_i$ $(j \in J)$, de modo que $P' = \underset{j\in J}{X} N_j$.

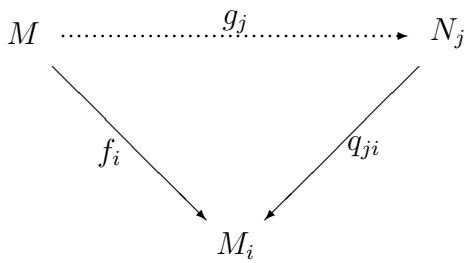
Se consideran las proyecciones $p'_j\colon P' \longrightarrow N_j$ $(j \in J)$, y para cada $j \in J$, $q_{ji}\colon N_j \longrightarrow M_i$ $(i \in I_j)$. Basta ver que $(P', (q_{\sigma(i)i} \circ p'_{\sigma(i)})_{i\in I})$ es un producto directo de $(M_i)_{i\in I}$, pues -en tal caso- existe un único isomorfismo $h\colon P' \longrightarrow P$ tal que $p_i \circ h = q_{\sigma(i)i \circ p'_{\sigma(i)}}$ $(i \in I)$, a saber: $h = \prod_{i\in I}(q_{\sigma(i)i} \circ p'_{\sigma(i)})$ vale decir, $h(x') = (q_{\sigma(i)i} \circ p'_{\sigma(i)})_{i\in I} = (x_{\sigma(i)i})_{i\in I}$.

En consecuencia, dados un A-módulo M y morfismo $f_i\colon M \longrightarrow M_i$ $(i \in I)$, debe probarse que

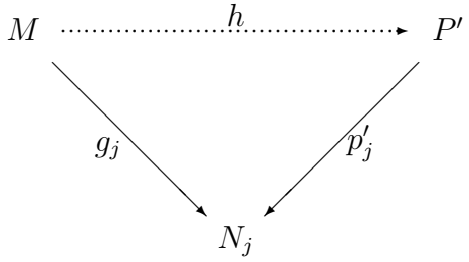


$\exists!\, h : (q_{\sigma(i)i} \circ p'_{\sigma(i)} \circ h = f_i \ (i \in I)$.

Existencia de h.



$\exists!\, g_j : q_{ji} \circ g_j = f_i \ (i \in I_j)$.

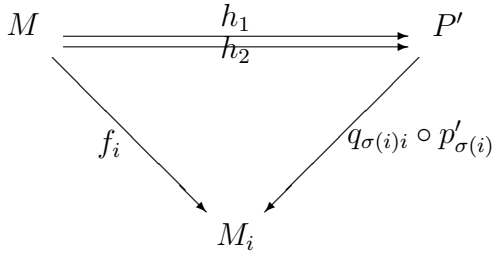


$\exists!\, h : p'_j \circ h = g_j \ (j \in J)$.

h ???????

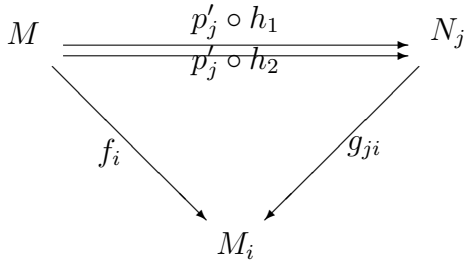
$$(q_{\sigma(i)i} \circ p'_{\sigma(i)} \circ h = q_{\sigma(i)i}(p'_{\sigma(i)}h) = q_{\sigma(i)i}g_{\sigma(i)} = f_i \ \ (i \in I).$$

Unicidad de h.



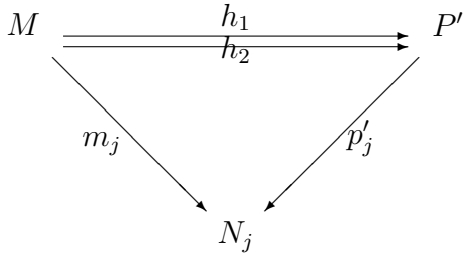
$(g_{\sigma(i)i} \circ p'_{\sigma(i)}) \circ h_1 = f_i \wedge (g_{\sigma(i)i} \circ p'_{\sigma(i)}) \circ h_2 = f_i \ (i \in I) \Longrightarrow h_1 = h_2$.

En efecto,



$q_{ji} \circ (p'_j) \circ h_1 = f_i \wedge q_{ji} \circ (p'_j \circ h_2 = f_i \ (i \in I_j) \Longrightarrow p'_j \circ h_1 = p'_j \circ h_2$.

$(q_{ji}(p'_j h_k) = (q_{ji}p'_{ji}h_k = (q_{\sigma(i)i}p'_{\sigma(i)})h_k = f_i$, k = 1,2).



$\underbrace{p'_j \circ h_1 = p'_j \circ h_2}_{m_j}$ $(j \in J) \Longrightarrow h_1 = h_2$, en abstracto.

PROPOSICIÓN 7.3. *Dada una familia de morfismos de A-módulos* $(f_i \colon M_i \longrightarrow N_i)_{i \in I'}$ *existe un único morfismo* $h \colon \underset{i \in I}{X} M_i \longrightarrow \underset{i \in I}{X} N_i$ *que hace conmutativo el diagrama*

$$\begin{array}{ccc} \underset{i \in I}{X} M_i & \xrightarrow{\quad h \quad} & \underset{i \in I}{X} N_i \\ \Big\downarrow{\scriptstyle p_j} & & \Big\downarrow{\scriptstyle p'_j} \\ M_j & \xrightarrow{\quad f_j \quad} & N_j \end{array}$$

vale decir, $p'_j \circ h = f_j \circ p_j$ $(j \in I)$, *a saber:* $h = \prod_{i \in I}(f_i \circ p_i)$; h *se nota* $\underset{i \in I}{X} f_i$. *Además, valen las fórmulas:*

$$\underset{i \in I}{X}(g_i \circ f_i) = \underset{i \in I}{X} g_i \circ \underset{i \in I}{X} f_i, \qquad \underset{i \in I}{X}(i_{M_i}) = i_{\underset{i \in I}{X} M_i}, \qquad \underset{i \in I}{X}(f_i + f'_i) = \underset{i \in I}{X} f_i + \underset{i \in I}{X} f'_i,$$
$$\underset{i \in I}{X}(c.f_i) = c.\underset{i \in I}{X} f_i \qquad (c \in C(A)).$$

Demostración.

$$\begin{array}{ccc} \underset{i \in I}{X} M_i & \xrightarrow{\quad h \quad} & \underset{i \in I}{X} N_i \\ & {\scriptstyle f_j \circ p_j} \searrow \quad \swarrow {\scriptstyle p'_j} & \\ & N_j & \end{array}$$

$\exists!\ h \colon p'_j \circ h = f_j \circ p_j$ $(j \in I)$. Explícitamente, $h = \prod_{i \in I}(f_i \circ p_i)$, vale decir, $h(x) = (f_i(x_i))_{i \in I}$ $(x \in \underset{i \in I}{X} M_i)$.

Primera fórmula. Los diagramas conmutativos

$$\begin{array}{ccc} \underset{i \in I}{X} M_i & \xrightarrow{\quad \overset{X}{f}_i \quad} & \underset{i \in I}{X} N_i \\ \Big\downarrow{\scriptstyle p_j} & & \Big\downarrow{\scriptstyle p'_j} \\ M_j & \xrightarrow{\quad f_j \quad} & N_j \end{array}$$

$$\begin{array}{ccc} \underset{i\in I}{X} N_i & \xrightarrow{\underset{g\ i}{X}} & \underset{i\in I}{X} P_i \\ \Big\downarrow{\scriptstyle p'_j} & & \Big\downarrow{\scriptstyle p''_j} \\ N_j & \xrightarrow{f_j} & P_j \end{array}$$

suministran el diagrama conmutativo

$$\begin{array}{ccc} \underset{i\in I}{X} M_i & \xrightarrow{\underset{g\ i}{X}\ \circ\ \underset{f\ i}{X}} & \underset{i\in I}{X} P_i \\ \Big\downarrow{\scriptstyle p_j} & & \Big\downarrow{\scriptstyle p''_j} \\ M_j & \xrightarrow{g_j \circ f_j} & N_j \end{array}$$

Luego, por razones de unicidad, $\underset{i\in I}{X}(g_i \circ f_i) = \underset{i\in I}{X} g_i \circ \underset{i\in I}{X} f_i$.□

Comentario

$$\mathcal{C}\begin{cases} \text{objetos} : (M_i)_{i\in I} \,|\, M_i \in \mathcal{M}_s(A)\ (i \in I) \\ \text{morfismos} : f\colon (M_i)_{i\in I} \longrightarrow (N_i)_{i\in I} \,|\, f = (f_i)_{i\in I},\ f_i \in \operatorname{Hom}_A(M_i, N_i)\ (i \in I). \end{cases}$$

$\underset{i\in I}{X}$ es un funtor aditivo de $\mathcal{C}$ en A-módulos.

Proposición 7.4. *Dada una familia de A-módulos $(M_i)_{i\in I}$ si S_i es un submódulo de M_i $(i \in I)$, $\underset{i\in I}{X} S_i$ se identifica a un submódulo de $\underset{i\in I}{X} M_i$, a saber: $\{x \in \underset{i\in I}{X} M_i \,|\, x_i \in S_i\ (i \in I)\}$.*

Demostración. Sean $P = \underset{i\in I}{X} M_i$ y $P' = \underset{i\in I}{X} S_i$, de modo que $P = \{x\colon I \longrightarrow \cup M_i \,|\, x_i \in M_i\ (i \in I)\}$ y $P' = \{x'\colon I \longrightarrow \cup S_i \,|\, x'_i \in S_i\ (i \in I)\}$. Si $\varphi\colon \cup S_i \longrightarrow \cup M_i$ es la inclusión, se define una aplicación $h\colon P' \longrightarrow P$ tomando $h(x') = \varphi \circ x'$, vale decir, $h(x')_i = x'_i\ (i \in I)$. h es un morfismo, pues $h = \underset{i\in I}{X} i_{S_i,M_i}$; y h es inyectiva, por serlo φ : $\varphi \circ x' = \varphi \circ y' \Longrightarrow x' = y'$. Por lo tanto, $P' \simeq \operatorname{Im} h$; pero $\operatorname{Im} h = \{x \in P \,|\, x_i \in S_i\ (i \in I)\}$:

$\subseteq$. Si $x' \in P'$, $h(x')_i = x'_i \in S_i\ (i \in I)$.

$\supseteq$. Dado $x \in P$ tal que $x_i \in S_i\ (i \in I)$, como $\operatorname{Im} x \subseteq \cup S_i$ puede considerarse $x' = x|^{\cup S_i}$; resulta que $x' \in P'$, pues $x'_i = x_i\ (i \in I)$, y $h(x') = \varphi \circ x' = x$.

Corolario 7.5. *Con la identificación de la proposición anterior, se verifica:*

i) $\operatorname{Ker} \underset{i\in I}{X} f_i = \underset{i\in I}{X} \operatorname{Ker} f_i$. *En particular, $\underset{i\in I}{X} f_i$ es un monomorfismo si, y sólo si, f_i lo es $(i \in I)$.*

ii) $\operatorname{Im} \underset{i\in I}{X} f_i = \underset{i\in I}{X}$. *En particular, si f_i es un epimorfismo $(i \in I)$, entonces $\underset{i\in I}{X} f_i$ lo es.*

Demostración. i) $\operatorname{Ker} X f_i = \{x \in X M_i \,|\, x_i \in \operatorname{Ker} f_i \ (i \in I)\}$, que se identifica con $X \operatorname{Ker} f_i$.

$$\operatorname{Ker} X f_i = 0 \Longleftrightarrow X \operatorname{Ker} f_i = 0 \Longleftrightarrow \operatorname{Ker} f_i = 0 \ (i \in I).$$

ii) $\operatorname{Im} X f_i = \{y \in X N_i \,|\, y_i \in \operatorname{Im} f_i \ (i \in I)\}$, que se identifica con $X \operatorname{Im} f_i$.

$$\operatorname{Im} f_i = N_i \ (i \in I) \Longrightarrow X \operatorname{Im} f_i = X N_i \Longleftrightarrow \operatorname{Im} X f_i = \underset{N_i}{X}. \square$$