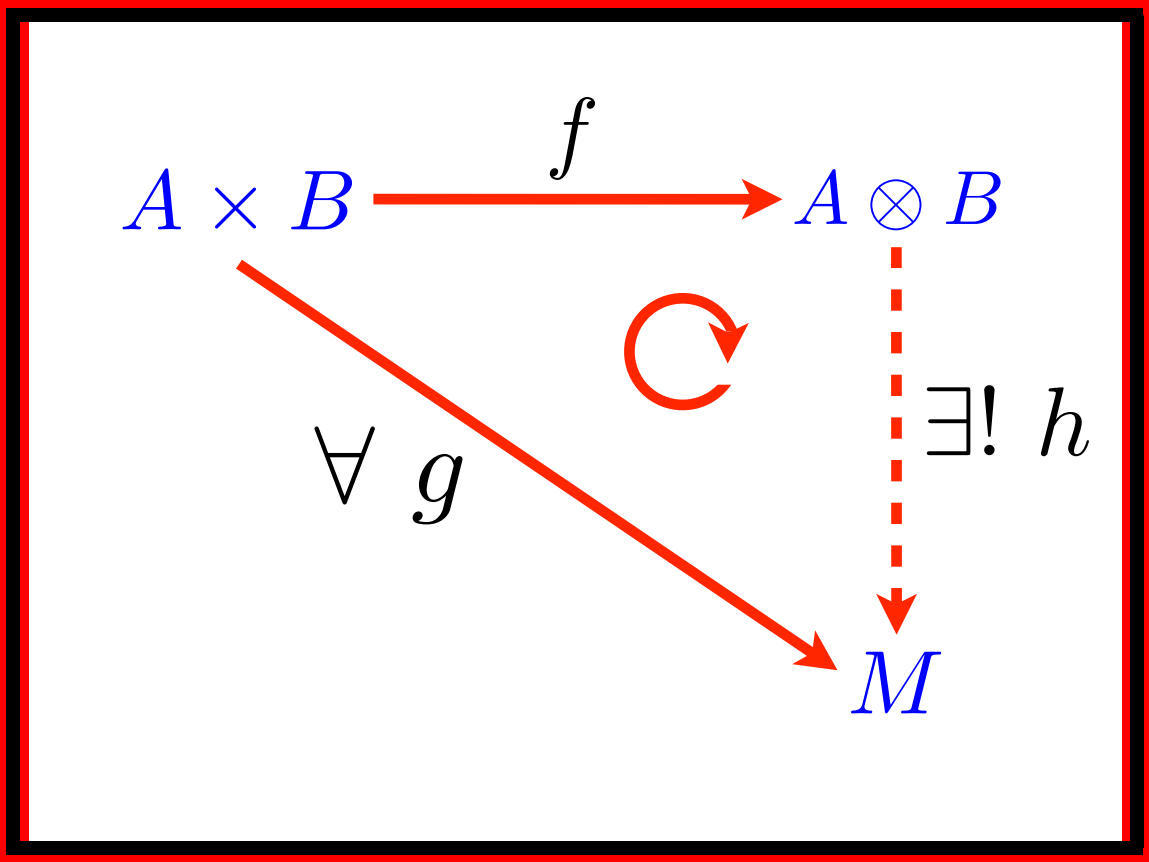
UNIVERSIDAD SIMÓN BOLÍVAR.
DEPARTAMENTO DE MATEMÁTICAS PURAS Y APLICADAS.

ÁLGEBRA CONMUTATIVA

Notas de curso



MARCO A. PÉREZ B.
SEPTIEMBRE, 2012.

Estas notas están basadas en un curso dado por **José Jatem** en la Universidad Simón Bolívar a principios de 2008. Cualquier error u omisión es responsabilidad del autor.

TABLA DE CONTENIDOS

CAPÍTULO 1

ANILLOS CONMUTATIVOS

1.1 Anillos conmutativos y homomorfismos

Definición 1.1.1. Un **anillo conmutativo** es un conjunto A junto con dos operaciones $+ : A \times A \longrightarrow A$ (suma) y $\cdot : A \times A \longrightarrow A$ (producto) que satisfacen las siguientes propiedades:

(i) $a + b = b + a$, para todo $a, b \in A$.

(ii) $a + (b + c) = (a + b) + c$, para todo $a, b, c \in A$.

(iii) Existe un elemento $0_A \in A$ tal que $a + 0_A = a$, para todo $a \in A$.

(iv) Para cada $a \in A$, existe un elemento $-a \in A$ tal que $a + (-a) = 0_A$.

(v) $a \cdot b = b \cdot a$, para todo $a, b \in A$.

(vi) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, para todo $a, b, c \in A$.

(vii) Existe un elemento $1_A \in A$ tal que $1_A \cdot a = a$, para todo $a \in A$.

(viii) $a \cdot (b + c) = a \cdot b + a \cdot c$, para todo $a, b, c \in A$.

Proposición 1.1.1.

(i) $0 \cdot a = 0$, para todo $a \in A$.

(ii) 0 es único.

(iii) 1 es único.

(iv) Para cada $a \in A$, $-a$ es único.

Demostración: Usaremos las propiedades de la definición anterior.

(i)

$$\begin{aligned} 0 \cdot a &= (0+0) \cdot a = 0 \cdot a + 0 \cdot a \\ 0 \cdot a + (-0 \cdot a) &= 0 \cdot a + [0 \cdot a + (-0 \cdot a)] \\ 0 &= 0 \cdot a + 0 \\ 0 &= 0 \cdot a \end{aligned}$$

(ii) Supongamos que existen $0, 0' \in A$ tales que $0 + a = 0' + a = 0$, para todo $a \in A$. En particular, tenemos $0 = 0 + 0' = 0'$.

(iii) Supongamos que existen $1, 1' \in A$ tales que $1 \cdot a = 1' \cdot a = a$, para todo $a \in A$. En particular, tenemos $1 = 1 \cdot 1' = 1'$.

(iv) Sea $a \in A$. Supongamos que existen $-a, a'$ tales que $a + (-a) = 0 = a + a'$. Tenemos

$$a' = a' + 0 = a' + [a + (-a)] = [a' + a] + (-a) = 0 + (-a) = -a.$$

□

Definición 1.1.2. Un elemento $a \in A$ se dice **invertible** si existe otro elemento en A, al cual denotaremos a^{-1}, tal que $a \cdot a^{-1} = 1$.

Proposición 1.1.2. Si $a \in A$ es invertible, entonces a^{-1} es único.

Demostración: Sean $a^{-1}, a' \in A$ tales que $a^{-1} \cdot a = 1$ y $a' \cdot a = 1$. Entonces

$$a' = a' \cdot 1 = a' \cdot (a \cdot a^{-1}) = (a' \cdot a) \cdot a^{-1} = 1 \cdot a^{-1} = a^{-1}.$$

□

Observacicón 1.1.1. Si $1 = 0$ entonces $A = \{0\}$.

Definición 1.1.3. Un **homomorfismo de anillos** es una función $f : A \longrightarrow B$, donde A y B son anillos, tal que si $a, b \in A$ entonces:

(i) $f(a +_A b) = f(a) +_B f(b)$, para todo $a, b \in A$.

(ii) $f(a \cdot_A b) = f(a) \cdot_B f(b)$, para todo $a, b \in A$.

(iii) $f(1_A) = 1_B$.

La primera condición equivale a decir que f es un homomorfismo de grupos, y por lo tanto

$$f(a - b) = f(a) - f(b) \quad \text{y} \quad f(0_A) = 0_B.$$

Para probar estar igualdades tenemos:

$$\begin{aligned} f(0_A) &= f(0_A + 0_A) = f(0_A) + f(0_A) \\ -f(0_A) + f(0 - A) &= (-f(0_A) + f(0_A)) + f(0_A) \\ 0_B &= f(0_A), \\ f(0_A) &= f(b + (-b)) = f(b) + f(-b) \Longrightarrow f(-b) = -f(b), \\ f(a - b) &= f(a + (-b)) = f(a) + (-f(b)) = f(a) - f(b). \end{aligned}$$

Definición 1.1.4. Un subconjunto S de un anillo A es un **subanillo** de A si es cerrado respecto de la suma y de la multiplicación, y si contiene la identidad de A ($1_A \in S$). Además, $0_A \in S$ y $-s \in S$, para todo $s \in S$.

Ejemplo 1.1.1. Los siguientes son ejemplos de anillos conmutativos: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $M(A)$, $M(\mathbb{Z})$, $M(\mathbb{R})$, $\mathbb{Z}_n$.

Sea S un subanillo de A. Existe un homomorfismo de anillos $\mathrm{i} : S \longrightarrow A$ dado por $s \mapsto s$, el cual se denomina **inclusión**. Si $f : A \longrightarrow B$ y $g : B \longrightarrow C$ son dos homomorfismos de anillos, entonces $g \circ f : A \longrightarrow C$ es un homomorfismo de anillos. De hecho, para todo $a, b \in A$ tenemos:

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

1.2 Ideales

Definición 1.2.1. Sean A un anillo e I un subconjunto de A. Se dice que I es un **ideal** de A si:

(i) Para todo $x, y \in I$, se tiene $x - y \in I$.

(ii) $0_A \in I$.

(iii) Para todo $a \in A$ y para todo $x \in I$, se tiene $a \cdot x \in I$.

Note que las dos primeras condiciones de la definicón anterior implican que I es un subgrupo abeliano de A.

Sea $a \in A$. Denotaremos $\langle a \rangle = \{r \cdot a \ / \ r \in A\}$.

Ejemplo 1.2.1. Los siguientes son ejemplos de ideales.

(i) $\langle 0 \rangle \subseteq A$, para todo anillo A.

(ii) $\langle a \rangle$, para todo $a \in A$. Tenemos:

$$\begin{aligned} r_1 \cdot a - r_2 \cdot a = (r_1 - r_2) \cdot a \in \langle a \rangle \ \text{ para todo } r_1 \cdot a, r_2 \cdot a \in \langle a \rangle, \\ 0 = 0 \cdot a \in \langle a \rangle, \\ r \cdot (x \cdot a) = (r \cdot x) \cdot a \in \langle a \rangle, \ \text{ para todo } r \in A \text{ y todo } x \cdot a \in \langle a \rangle. \end{aligned}$$

Sean A un anillo e I un ideal de A. Se define la siguiente relación de equivalencia en A: para todo $a, b \in A$ diremos que $a \equiv b \pmod{I}$ si $a - b \in I$.

(i) $\equiv$ es reflexiva: Para todo $a \in A$, tenemos $a - a = 0 \in I$. Así, $a \equiv a \pmod{I}$.

(ii) $\equiv$ es simétrica: Si $a \equiv b \pmod{I}$, entonces $a - b \in I$, de donde $b - a \in I$ y $b \equiv a \pmod{I}$.

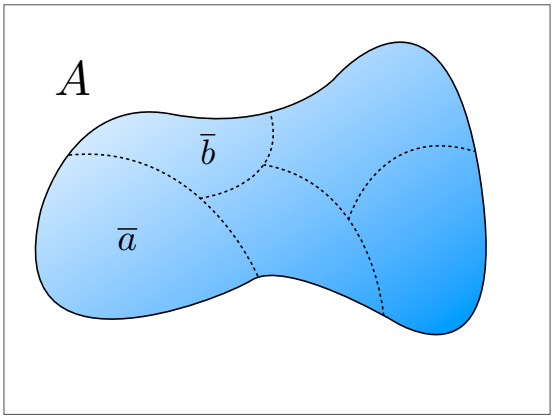
(iii) $\equiv$ es transitiva: Si $a \equiv b \pmod{I}$ y $b \equiv c \pmod{I}$, entonces $a - b, b - c \in I$. De donde $a - c \in I$ y $a \equiv c \pmod{I}$.

El anillo A queda dividido en clases de equivalencia. Para cada $a \in A$, la clase de a viene dada por

$$\overline{a} = \{b \in A \ / \ a \equiv b \pmod{I}\} = \{b \in A \ / \ a - b \in I\}.$$

El conjunto cociente viene dado por

$$\frac{A}{I} = \frac{A}{\equiv \pmod{I}} = \{\overline{a} \ / \ a \in A\}.$$



Definamos dos operaciones, suma y producto, en $\frac{A}{I}$:

$$+ : \frac{A}{I} \times \frac{A}{I} \longrightarrow \frac{A}{I} \quad \text{dada por} \quad \overline{a} + \overline{b} = \overline{a+b},$$
$$\cdot : \frac{A}{I} \times \frac{A}{I} \longrightarrow \frac{A}{I} \quad \text{dada por} \quad \overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

Hay que verificar que estas operaciones están bien definidas: si $\overline{a} = \overline{a'}$ y $\overline{b} = \overline{b'}$, veamos que $\overline{a} + \overline{b} = \overline{a'} + \overline{b'}$. Tenemos:

$$\begin{aligned} \overline{a} = \overline{a'} \text{ y } \overline{b} = \overline{b'} &\Longrightarrow a \equiv a' \pmod{I} \text{ y } b \equiv b' \pmod{I} \\ &\Longrightarrow a - a', b - b' \in I \\ &\Longrightarrow (a+b) - (a'+b') = (a-a') + (b-b') \in I \\ &\Longrightarrow a + b \equiv a' + b' \pmod{I}. \end{aligned}$$

Ahora veamos que $\overline{a} \cdot \overline{b} = \overline{a'} \cdot \overline{b'}$.

$$\begin{aligned} (a-a')b, a'(b-b') \in I &\Longrightarrow (ab - a'b) + (a'b - a'b') \in I \\ &\Longrightarrow ab - a'b' \in I \\ &\Longrightarrow a \cdot b \equiv a' \cdot b' \pmod{I} \\ &\Longrightarrow \overline{a} \cdot \overline{b} = \overline{a'} \cdot \overline{b'}. \end{aligned}$$

Por lo tanto, las operaciones $+_{\frac{A}{I}}$ y $\cdot_{\frac{A}{I}}$ están bien definidas. Denotemos $0_{\frac{A}{I}} = \overline{0}$ y $1_{\frac{A}{I}} = \overline{1}$ y $-\overline{a} = \overline{-a}$. Con estas operaciones y elementos, tenemos que $\frac{A}{I}$ is un anillo conmutativo.

Ejemplo 1.2.2. En $\mathbb{Z}$, consideremos el ideal $\langle m\rangle$. Note que $\frac{\mathbb{Z}}{\langle m\rangle} = \mathbb{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$. Si $0 \leq j < k \leq m-1$, entonces $m \not| (k-j)$, donde $k - j \leq m-1$. Luego $k - j \notin \langle m\rangle$, es decir $k \not\equiv j \pmod{\langle m\rangle}$. Note además que $\overline{0} = \{a \in Z \ / \ a = a - 0 \in \langle m\rangle\} = \langle m\rangle$.

Si $m = 3$, tenemos

$$\begin{aligned}\overline{0} &= \langle 3\rangle\,,\\ \overline{1} &= \{\ldots, -2, 1, 4, 7, \ldots\},\\ \overline{2} &= \{\ldots, -4, -1, 2, 5, 8, \ldots\}.\end{aligned}$$

¿A cuál clase pertenece -15 en $\mathbb{Z}_9$? Pues $-15 = (-2)\cdot 9 + 3$ y así $-15 \in \overline{3}$.

La función $\phi : A \longrightarrow \frac{A}{I}$ dada por $\phi(a) = \overline{a}$ es un homomorfismo de anillos, además es sobreyectivo.

$$\begin{aligned}\phi(a+b) &= \overline{a+b} = \overline{a} + \overline{b} = \phi(a) + \phi(b),\\ \phi(1) &= \overline{1} = 1_{\frac{A}{I}}.\end{aligned}$$

1.3 Divisores de cero, unidades y nilpotentes

Definición 1.3.1. Un elemento $x \in A$ es un **divisor de cero** si existe $y \in A\backslash\{0\}$ tal que $x \cdot y = 0$.

Ejemplo 1.3.1. $0 \in A$ es un divisor de cero si $A \neq \langle 0\rangle$.

En $\mathbb{Z}$, 0 es el único divisor de cero.

En $\mathbb{Z}_6$, $\overline{2}$ es un divisor de cero pues $\overline{2}\cdot\overline{3} = \overline{6} = \overline{0}$., mientras que $\overline{1}$ no es un divisor de cero.

En $M_2(\mathbb{R})$, $\begin{pmatrix} 0 & 1\\ 0 & 0\end{pmatrix}$ es un divisor de cero, pues

$$\begin{pmatrix} 0 & 1\\ 0 & 0\end{pmatrix}\cdot\begin{pmatrix} 0 & 1\\ 0 & 0\end{pmatrix} = \begin{pmatrix} 0 & 0\\ 0 & 0\end{pmatrix}.$$

En $\mathbb{Z}_8$, $\overline{2}$ es un divisor de cero pues $\overline{2}\cdot\overline{3} = \overline{6} = \overline{0}$. Además, $\overline{2}^3 = \overline{0}$. En este caso, $\overline{2}$ se dice que es un **elemento nilpotente**. Similarmente, $\overline{3}$ es un elemento nilpotente de $\mathbb{Z}_9$.

Definición 1.3.2. Un anillo D es un **dominio entero** si no tiene divisores de cero no nulos y si $1 \neq 0$ (es decir $D \neq \langle 0\rangle$).

Ejemplo 1.3.2. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ y $\mathbb{Z}_p$, con p primo, son ejemplos de dominios enteros.

Dado un anillo A, definamos $A[x] := \{a_0 + a_1x + \cdots + a_mx^m \ / \ a_i \in A \text{ y } n \in \mathbb{N}\}$ con las siguientes operaciones:

$$(a_0 + a_1x + \cdots + a_nx^n) + (b_0 + b_1x + \cdots + b_mx^m) = (a_0 + b_0) + (a_1 + b_1)x + \cdots$$

$$(a_0 + a_1x + \cdots + a_nx^n)\cdot(b_0 + b_1x + \cdots + b_mx^m) = c_0 + c_1x + \cdots + c_{m+n}x^{m+n}, \text{ donde } c_i = \sum_{k=0}^{i} a_kb_{i-k}.$$

Con estas operaciones, $A[x]$ es un anillo conmutativo.

Ejercicio 1.3.1. Si D es un dominio entero, entonces $D[x]$ es un dominio entero.

Si $\mathbb{K}$ es un cuerpo, entonces $\mathbb{K}[x]$ es un dominio entero. De forma similar, $\mathbb{K}[x,y] = [\mathbb{K}[x]][y]$ es un dominio entero. Inductivamente, se tiene que $\mathbb{K}[x_1, \ldots, x_n]$.

Definición 1.3.3. Un elemento $x \in A$ es una **unidad o invertible** si existe $y \in A$ tal que $x \cdot y = 1$.

El conjunto $U(A) := \{x \in A \ / \ x \text{ es una unidad}\}$ de las unidades de A es un grupo abeliano.

Definición 1.3.4. Un ideal en un anillo A se dice **principal** si es de la forma $\langle x \rangle = \{r \cdot x \ / \ r \in A\}$.

Note que $x \in U(A)$ si y sólo si $\langle x \rangle = A$. Un anillo K es un cuerpo si $U(K) = K \backslash \{0\}$.

Ejercicio 1.3.2. Si A y B son dos anillos y $\phi : A \longrightarrow B$ es un homomorfismo de anillos, entonces:

(i) $\text{Ker}(\phi) = \{a \in A \ / \ \phi(a) = 0\}$ es un ideal de A.

(ii) $\text{Im}(\phi) = \{b \in B \ / \ \text{existe } a \in A \text{ con } b = \phi(a)\}$ es un subanillo de B.

Definición 1.3.5. Un elemento $x \in A$ se dice **nilpotente** si existe $n \in \mathbb{N}$ tal que $x^n = 0$.

Note que si $x \in A$ es nilpotente entonces x es un divisor de cero. Pero no todo divisor de cero tiene que ser nilpotente, por ejemplo $\overline{3} \in \mathbb{Z}_6$ es un divisor de cero pero no es nilpotente.

Ejercicio 1.3.3.

(1) Sea A un anillo con $1 \neq 0$. Las siguientes condiciones son equivalentes:

  (i) A es un cuerpo.

  (ii) Los únicos ideales de A son los ideales triviales $\langle 0 \rangle$ y A.

  (iii) Si ϕ es un homomorfismo de anillos no nulo entonces ϕ es inyectivo.

(2) Sea $\phi : A \longrightarrow B$ un homomorfismo de anillos. Entonces, ϕ es inyectivo si y sólo si $\text{Ker}(\phi) = \langle 0 \rangle$. Y ϕ es sobreyectivo si y sólo si $\text{Im}(\phi) = B$.

(3) Si I y J son ideales en un anillo A, entonces $I + J$ es también un ideal en A.

1.4 Ideales primos y maximales

Definición 1.4.1. Sean P y $\mathcal{M}$ dos ideales en un anillo A. Se dice que P es **primo** si $x \cdot y \in P \Longrightarrow x \in P$ o $y \in P$. Se dice que $\mathcal{M}$ es **maximal** si dado otro ideal I en A que satisface $\mathcal{M} \subseteq I \subseteq A$, entonces $I = \mathcal{M}$ o $I = A$.

Proposición 1.4.1. Todo ideal maximal es primo.

Demostración: Sea $\mathcal{M}$ un ideal maximal en un anillo A. Supongamos que $x \cdot y \in \mathcal{M}$ y que $x \notin \mathcal{M}$. Luego, $\mathcal{M} \subsetneq \mathcal{M} + \langle x \rangle$. Como $\mathcal{M}$ es maximal, se tiene que $\mathcal{M} + \langle x \rangle = A$. Luego, existe $m \in \mathcal{M}$ y $r \in A$ tal que $1 = m + r \cdot x$. Luego, $y = y \cdot m + r \cdot (x \cdot y) \in \mathcal{M}$. □

Ejemplo 1.4.1. En $\mathbb{Z}$, todo ideal primo es maximal.

Ejercicio 1.4.1. Sea A un anillo, entonces:

(i) P es un ideal primo si y sólo si $\frac{A}{P}$ es un dominio entero.

(ii) $\mathcal{M}$ es un ideal maximal si y sólo si $\frac{A}{\mathcal{M}}$ es un cuerpo.

Proposición 1.4.2. Sea $\phi : A \longrightarrow B$ un homomorfismo de anillos. Si I es un ideal de B, entonces $\phi^{-1}(I)$ es un ideal de A.Más aún, si P es un ideal primo de B, entonces $\phi^{-1}(P)$ es un ideal primo de A.

Demostración: Sean $x, y \in \phi^{-1}(I)$. Luego, $\phi(x), \phi(y) \in I$ y así $\phi(x-y) = \phi(x) - \phi(y) \in I$, es decir $x - y \in \phi^{-1}(I)$. Por otro lado, $\phi(0_A) = 0_B \in I$, de donde $0_A \in \phi^{-1}(I)$. Finalmente, sean $x \in \phi^{-1}(I)$ y $r \in I$. Tenemos $\phi(r \cdot x) = \phi(r) \cdot \phi(x) \in I$, por lo que $r \cdot x \in I$.

Ahora, sea P un ideal primo se P. Supongamos que $x \cdot y \in \phi^{-1}(P)$. Entonces $\phi(x) \cdot \phi(y) = \phi(x \cdot y) \in P$. Como P es un ideal primo de B, se tiene que $\phi(x) \in P$ o $\phi(y) \in P$, es decir $x \in \phi^{-1}(P)$ o $y \in \phi^{-1}(P)$. □

Ejercicio 1.4.2. Dé un contraejemplo de que si I es un ideal de A, entonces $\phi(I)$ no es necesariamente un ideal de B.

En la proposición anterior, si $\mathcal{M}$ es un ideal maximal de B, no necesariamente $\phi^{-1}(\mathcal{A})$ es un ideal maximal de A. Por ejemplo, considere la inclusión $i : \mathbb{Z} \longrightarrow \mathbb{Q}$. Note que $\langle 0 \rangle$ es un ideal maximal de $\mathbb{Q}$, pero $\langle 0 \rangle = i^{-1}(\langle 0 \rangle)$ no es un ideal maximal de $\mathbb{Z}$.

1.5 Aplicaciones del Lema de Zorn

Definición 1.5.1. Un conjunto S se dice **parcialmente ordenado** si existe una relación $\leq$ en S que satisface las siguientes propiedades:

(i) $\leq$ es **antisimétrica**: $x \leq y$ y $y \leq x \Longrightarrow x = y$.

(ii) $\leq$ es **transitiva**: $x \leq y$ y $y \leq z \Longrightarrow x \leq z$.

(iii) $\leq$ es **reflexiva**: $x \leq x$, para todo $x \in S$.

Un conjunto S con un orden parcial $\leq$ se dice **totalmente ordenado** si para todo $x, y \in S$, se tiene $x \leq y$ o $y \leq x$. Una **cadena** $\mathcal{C}$ en un subconjunto parcialmente ordenado $(S, \leq)$ es un subconjunto de S totalmente ordenado. Un elemento $x \in S$ se dice que es una **cota superior** de una cadena $\mathcal{C}$ si para todo $c \in \mathcal{C}$ se tiene $c \leq x$. Un elemento $m \in S$ se dice **maximal** si $m = x$, para todo x tal que $m \leq x$.

Lema 1.5.1 (Lema de Zorn)**.** Si tida cadena $\mathcal{C}$ de un conjunto parcialmente ordenado S tiene una cota superior, entonces S tiene un elemento maximal.

Teorema 1.5.1. Todo anillo A con $1 \neq 0$ tiene un ideal maximal.

Demostración: Sea $\mathcal{A} = \{I \subsetneq A \ / \ I \text{ es un ideal de } A\}$. Note que $\mathcal{A}$ es un conjunto no vacío pues $\langle 0\rangle \in \mathcal{A}$. Además, $\mathcal{A}$ está parcialmente ordenado por la inclusión $\subseteq$. Probaremos que toda cadena $\mathcal{C}$ de $\mathcal{A}$ posee una cota superior, por lo que el teorema será consecuencia del lema de Zorn. Considere el conjunto $J = \bigcup\{I \ / \ I \in \mathcal{C}\}$. Note que J es un ideal de A. Si $J = A$, entonces $i \in J$, por lo que existe $I \in \mathcal{C}$ tal que $1 \in I$, y así $I = A$, llegando a una contradicción. Por lo tanto, $J \in \mathcal{A}$. Note que J es una cota superior de $\mathcal{C}$. Por el Lema de Zorn, $\mathcal{A}$ tiene un elemento maximal. □

Proposición 1.5.1. Si $J \subsetneq A$ es un ideal de un anillo $A \neq \langle 0\rangle$, entonces J está contenido en un ideal maximal.

Demostración: Considere el conjunto $\mathcal{A} = \{I \subsetneq A \ / \ J \subseteq I\}$. Note que $\mathcal{A}$ es no vacío pues $J \in \mathcal{A}$. El ideal $K = \bigcup\{I \ / \ I \in \mathcal{C}\}$ es una cota superior de $\mathcal{C}$, donde $\mathcal{C}$ es una cadena de $\mathcal{A}$. Por el Lema de Zorn, $\mathcal{A}$ tiene un elemento maximal. □

Ejemplo 1.5.1. En $\mathbb{Z}$, $\langle 2\rangle$ y $\langle 3\rangle$ son ideales maximales. Por otro lado, $\langle 6\rangle$ no es maximal pues $\langle 6\rangle \subseteq \langle 3\rangle$. Si p es primo, entonces $\langle p\rangle$ es un ideal maximal de $\mathbb{Z}$. En efecto, supongamos que I es un ideal tal que $\langle p\rangle \subsetneq I \subseteq \mathbb{Z}$. Luego, existe $x \in I$ tal que $x \notin \langle p\rangle$. Por otro lado, $x = p \cdot n + r$, para algún $n \in \mathbb{X}$ y $r = 0, 1, \ldots, p-1$. Note que $p \not| x$ y así $(p, x) = 1$. De donde existen $a, b \in \mathbb{Z}$ tales que $1 = a \cdot p + b \cdot x$, por lo que $1 \in I$. Por lo tanto, $I = \mathbb{Z}$.

Definición 1.5.2. Un anillo A se dice **noetheriano** si toda cadena de ideales en A es estacionaria. En otras palabras, para cualquier cadena de ideales $I_1 \subseteq I_2 \subseteq \cdots$, existe $m \in \mathbb{N}$ tal que $I_m = I_{m+1} = \cdots$.

Ejercicio 1.5.1. Si A es un anillo noetheriano, pruebe que existe un ideal maximal en A sin usar el Lema se Zorn.

1.6 Anillos locales, semilocales, y dominios de ideales principales

Definición 1.6.1. Un anillo A se dice **local** si tiene un único ideal maximal. Si $\mathcal{M}$ es el único ideal maximal, el anillo cociente $\frac{A}{\mathcal{M}}$ se denomina **anillo residual**.

Ejemplo 1.6.1. Todo cuerpo es un anillo local.

Proposición 1.6.1. Sea A un anillo, y $\mathcal{M} \subseteq A$ un ideal tal que si $x \in A \backslash \mathcal{M}$ entonces x es una unidad. Entonces A es local y $\mathcal{M}$ es un ideal maximal.

Demostración: El hecho de que $\mathcal{M}$ es maximal es inmediato. Sea $\mathcal{M}'$ otro ideal maximal. Entonces no puede ocurrir que $\mathcal{M}' \subseteq \mathcal{M}$. Luego, existe $m \in \mathcal{M}' \backslash \mathcal{M}$, donde m es una unidad y entonces $\mathcal{M}' = A$. □

Proposición 1.6.2. Sea $\mathcal{M}$ un ideal maximal en un anillo A tal que $\overline{1} \in \frac{A}{\mathcal{M}}$ está contenida en $U(A)$. Entonces A es un anillo local.

Demostración: Supongamos que existe otro ideal maximal $\mathcal{M}'$. Sea $x \in \mathcal{M}' \backslash \mathcal{M}$. Tenemos $\mathcal{M} + \langle x \rangle = A$. De donde $1 = m + a \cdot x$. Luego $\overline{1} = \overline{m} + \overline{a} \cdot \overline{x}$. De donde $a \cdot x \in U(A)$ y por tanto $x \in U(A)$. Entonces, $\mathcal{M}' = A$, obteniendo así una contradicción. □

Definición 1.6.2. Un anillo A se dice **semilocal** si tiene un número infinito de ideales maximales.

Definición 1.6.3. Un **dominio de ideales principales (DIP)** es un dominio entero cuyos ideales son todos principales.

Ejercicio 1.6.1.

(1) Demuestre que $\mathbb{Z}$ es un dominio de ideales principales.

(2) En un dominio de ideales principales, demuestre que todo ideal primo es maximal.

1.7 Nilradical y radical de Jacobson

Definición 1.7.1. El conjunto $\mathcal{N} = \{x \in A \ / \ x \text{ es nilpotente}\}$ se denomina **nilradical** de A.

Ejercicio 1.7.1. Demuestre que $\mathcal{N}$ es un ideal de A.

Proposición 1.7.1. El anillo cociente $\frac{A}{\mathcal{N}}$ no tiene elementos nilpotentes distintos de cero.

Demostración: Sea $\overline{x} \in \frac{A}{\mathcal{N}}$ un elemento nilpotente. Entonces existe $n \in \mathbb{N}$ tal que $\overline{x}^n = \overline{0}$. Luego, $x^n \in \mathcal{N}$, de donde existe $m \in \mathbb{N}$ tal que $x^{nm} = 0$. Tenemos que x es nilpotente, por lo que $\overline{x} = \overline{0}$. □

Proposición 1.7.2. $\mathcal{N} = \bigcap \{P \ / \ P \text{ es un ideal primo de } A\}$.

Demostración:

($\subseteq$) Si $x \in \mathcal{N}$ entonces existe $n \in \mathbb{N}$ tal que $x^n = 0$. De donde $x^n \in P$, para todo ideal P primo. Al ser P primo, nos queda $x \in P$, para todo P.

($\supseteq$) Supongamos que $x \notin \mathcal{N}$. Luego, $x^n \neq 0$, para todo $n \in \mathbb{N}$. Considere el conjunto

$$\mathcal{A} = \{I \subseteq A \ / \ I \text{ es un ideal de } A \text{ y } x^n \notin I, \text{ para todo } n \in \mathbb{N}\}.$$

Note que $\mathcal{A} \neq \emptyset$ pues $\langle 0 \rangle \in \mathcal{A}$. Además, $\mathcal{A}$ está ordenado parcialmente por la inclusión $\subseteq$. Sea $\mathcal{C}$ una cadena de $\mathcal{A}$. Considere el ideal $K = \bigcup\{I \ / \ I \in \mathcal{C}\}$. Note que $K \in \mathcal{A}$ y que K es una cota superior de $\mathcal{C}$. Por el Lema de Zorn, $\mathcal{A}$ tiene un elemento maximal $\mathcal{M}$. Ahora probaremos que $\mathcal{M}$ es un ideal primo. Supongamos que $a \notin \mathcal{M}$ y $b \notin \mathcal{M}$. Entonces $\mathcal{M} \subsetneqq \mathcal{M} + \langle a \rangle$ y $\mathcal{M} \subsetneqq \mathcal{M} + \langle b \rangle$. Como $\mathcal{M}$ es maximal en $\mathcal{A}$, nos queda que $\mathcal{M} + \langle a \rangle, \mathcal{M} + \langle b \rangle \notin \mathcal{A}$. De donde existen $n, m \in \mathbb{N}$ tales que $x^n = p_1 + c \cdot a$ y $x^m = p_2 + d \cdot b$, para algunos $p_1, p_2 \in \mathcal{M}$ y $c, d \in A$. Luego, $x^{n+m} \in \mathcal{M} + \langle a \cdot b \rangle$ y $\mathcal{M} + \langle a \cdot b \rangle \notin \mathcal{A}$. Por lo tanto, $\mathcal{M} \subsetneqq \mathcal{M} + \langle a \cdot b \rangle$ y $a \cdot b \notin \mathcal{M}$. Tenemos un ideal primo $\mathcal{M}$ tal que $x \notin \mathcal{M}$, es decir, $x \notin \bigcap\{P \ / \ P \text{ es un ideal primo de } A\}$.

□

Definición 1.7.2. El ideal $R = \bigcap\{\mathcal{M} \subseteq A \ / \ \mathcal{M} \text{ es un ideal maximal de } A\}$ se denomina **radical de Jacobson**.

Ejercicio 1.7.2. Para todo ideal maximal $\mathcal{M}$, demuestre que $x \notin \mathcal{M}$ si y sólo si $x \in U(A)$.

1.8 Suma de ideales y producto de anillos

De manera más general, la **suma de ideales**

$$\sum_{i \in I} I_i = \{x_1 + \cdots + x_n \ / \ x_i \in I_i \text{ y } n \in \mathbb{N}\}$$

es el menor ideal de A que contiene a cada I_i.

Ejercicio 1.8.1. Pruebe que $I + J$ es el "menor" ideal de A entre aquéllos que contienen a I y a J.

Definición 1.8.1. Sean $A_1, \ldots, A_n$ anillos. Se define el **producto directo** de ellos como el conjunto

$$\prod_{i=1}^{n} A_i = \{(a_1, \ldots, a_n) \ / \ a_i \in A_i\},$$

el cual resulta ser un anillo con las siguientes operaciones de suma y producto:

$$+ : \prod_{i=1}^{n} A_i \times \prod_{i=1}^{n} A_i \longrightarrow \prod_{i=1}^{n} A_i \qquad (a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n),$$

$$\cdot : \prod_{i=1}^{n} A_i \times \prod_{i=1}^{n} A_i \longrightarrow \prod_{i=1}^{n} A_i \qquad (a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) = (a_1 \cdot b_1, \ldots, a_n \cdot b_n).$$

Para cada $j = 1, \ldots, n$, la aplicación $p_j : \prod_{i=1}^{n} A_i \longrightarrow A_j$ dada por $(a_1, \ldots, a_n) \mapsto a_j$ se denomina **proyección sobre** A_j y es un homomorfismo de anillos.

CAPÍTULO 2

MÓDULOS SOBRE ANILLOS

2.1 Módulos y homomorfismos de módulos

Definición 2.1.1. Sea A un anillo (conmutativo) y $(M,+)$ un grupo abeliano. Diremos que M es un A**-módulo** si, provisto de una operación $\cdot : A \times M \longrightarrow M$ $(a,m) \mapsto a \cdot m$, satisface:

(i) Para todo $a,b \in A$ y para todo $m \in M$, $(a+b)\cdot m = a\cdot m + b\cdot m$.

(ii) Para todo $a \in A$ y para todo $m,n \in M$, $a\cdot(m+n) = a\cdot m + a\cdot n$.

(iii) Para todo $m \in M$, $1\cdot m = m$.

(iv) Para todo $a,b \in A$ y para todo $m \in M$, $(a\cdot b)\cdot m = a\cdot(b\cdot m)$.

Dado un grupo abeliano $(M,+)$, definimos

$$E(M) = \{g : M \longrightarrow M \ / \ g \text{ es un homomorfismo de grupos}\},$$

el conjunto de los endomorfismos en M. Dados dos endomorfismos $g,h : M \longrightarrow M$, definimos la suma punto a punto, es decir $g+h$ es el endomorfismo dado por $(g+h)(m) = g(m)+h(m)$; y la composición de la manera usual, $g\circ h : M \longrightarrow M$ es el endomorfismo dado por $(g\circ h)(m) = g(h(m))$. Con las siguientes operaciones de suma y producto,

$$\begin{aligned} + &: E(M)\times E(M) \longrightarrow E(M) \qquad (g,h) \mapsto g+h, \\ \cdot &: E(M)\times E(M) \longrightarrow E(M) \qquad (g,h) \mapsto g\circ h. \end{aligned}$$

se tiene que $E(M)$ deviene en un anillo.

Ejercicio 2.1.1. Probar que M es un A-módulo si y sólo si: $(M,+)$ es un grupo abeliano y existe un homomorfismo de anillos $f : A \longrightarrow E(M)$.

Ejemplo 2.1.1.

(i) Todo $\mathbb{K}$-espacio vectorial es un $\mathbb{K}$-módulo.

(ii) Todo anillo A es un A-módulo con las operaciones de A.

Ejercicio 2.1.2. Demostrar que todo grupo abeliano es un $\mathbb{Z}$-módulo con la suma en G y la siguiente operación:

$$\begin{aligned}\mathbb{Z} \times G &\longrightarrow G \\ (n, g) &\mapsto \begin{cases} g + \cdots + g \ n \text{ veces} & \text{si } n \geq 0, \\ -g - \cdots - g - n \text{ veces} & \text{si } n < 0. \end{cases}\end{aligned}$$

Definición 2.1.2. Sean M y N dos A-módulos y $f : M \longrightarrow N$ una función. Se dice que f es un **homomorfismo de A-módulos** si:

(i) Para todo $m_1, m_2 \in M$, $f(m_1 + m_2) = f(m_1) + f(m_2)$.

(ii) Para todo $a \in A$ y todo $m \in M$, $f(a \cdot m) = a \cdot f(m)$.

Denotamos el conjunto de homomorfismos de M en N como

$$\mathrm{Hom}_A(M, N) = \{f : M \longrightarrow N \ / \ f \text{ es un homomorfismo de } A\text{-módulos}\}.$$

Es fácil ver que la suma de homomorfismos de A-módulos es un homomorfismo de A-módulos. Definamos las siguientes operaciones en $\mathrm{Hom}_A(M, N)$:

$$\begin{aligned}\mathrm{Hom}_A(M, N) \times \mathrm{Hom}_A(M, N) &\longrightarrow \mathrm{Hom}_A(M, N) \\ (g, h) &\mapsto g + h, \\ A \times \mathrm{Hom}_A(M, N) &\longrightarrow \mathrm{Hom}(M, N) \\ (a, g) &\mapsto a \cdot g, \text{ donde } a \cdot g \text{ está dado por } (a \cdot g)(m) = a \cdot g(m).\end{aligned}$$

Con estas operaciones, $\mathrm{Hom}_A(M, N)$ es un A-módulo. Si $f : L \longrightarrow M$ y $g : M \longrightarrow N$ son homomorfismos de A-módulos, entonces $g \circ f : L \longrightarrow N$ es también un homomorfismo de A-m odulos:

$$\begin{aligned}(g \circ f)(m + n) &= g(f(m + n)) = g(f(m) + f(n)) = g(f(m)) + g(f(n)) = (g \circ f)(m) + (g \circ f)(n), \\ (g \circ f)(a \cdot m) &= g(f(a \cdot m)) = g(a \cdot f(m)) = a \cdot (g(f(m))) = a \cdot (g \circ f)(m),\end{aligned}$$

para todo $a \in A$ y $m, n \in L$. Con las operaciones $+$ y $\circ$, el conjunto $\mathrm{Hom}_A(M, N)$ es un anillo conmutativo.

Si $u : M' \longrightarrow M$ y $v : N \longrightarrow N'$ son homomorfismos de A-módulos, entonces

$$\begin{aligned}\overline{u} : \mathrm{Hom}_A(M, N) &\longrightarrow \mathrm{Hom}_A(M', N) \\ f &\mapsto f \circ u, \\ \overline{v} : \mathrm{Hom}_A(M, N) &\longrightarrow \mathrm{Hom}_A(M, N') \\ f &\mapsto v \circ f,\end{aligned}$$

también son homomorfismos de A-módulos:

$$\begin{aligned}\overline{u}(f + g) &= (f + g) \circ u = f \circ u + g \circ u = \overline{u}(f) + \overline{u}(g), \\ \overline{u}(a \cdot f) &= (a \cdot f) \circ u = a \cdot (f \circ u) = a \cdot \overline{u}(f), \\ \overline{v}(f + g) &= v \circ (f + g) = v \circ f + v \circ g = \overline{v}(f) + \overline{v}(g), \\ \overline{v}(a \cdot f) &= v \circ (a \cdot f) = a \cdot (v \circ f) = a \cdot \overline{v}(f).\end{aligned}$$

Definición 2.1.3. Sean M un A-módulo y N un subconjunto de M. Se dice que N es un **submódulo** de M si es un subgrupo de M y si para todo $a \in A$ y $n \in N$ se tiene $a \cdot n \in N$. Esto equivale a que las siguientes condiciones se satisfacen:

(i) Para todo $n_1, n_2 \in N$, $n_1 - n_2 \in N$.

(ii) $0 \in N$.

(iii) Para todo $a \in A$ y $n \in N$, $a \cdot n \in N$.

Ejemplo 2.1.2.

(i) Todo A-módulo es un submódulo de sí mismo.

(ii) $\{0\}$ es un submódulo de M, para todo A-módulo M.

(iii) Todo ideal de A es un submódulo del A-módulo A.

(iv) El conjunto $\mathbb{Z}$, como $\mathbb{Z}$-módulo, tiene por ideales a $\langle m \rangle$, para todo $m \in \mathbb{Z}$.

(v) En $\mathbb{Z}_n$, como $\mathbb{Z}$-módulo, se tiene que $\langle \overline{m} \rangle$ es un submódulo de $\mathbb{Z}_n$, para todo $m \in \mathbb{Z}$.

(vi) Si $f : M \longrightarrow N$ es un homomorfismo de A-módulos, entonces $\mathrm{Ker}(f) = \{m \in M \ / \ f(m) = 0\}$ y $\mathrm{Im}(f) = \{f(m) \ / \ m \in M\}$ son sunmódulos de M y N, respectivamente.

Teorema 2.1.1. Si $f : M \longrightarrow N$ es un homomorfismo de A-módulos, entonces:

(i) f es inyectivo si y sólo si $\mathrm{Ker}(f) = \langle 0 \rangle$.

(ii) f es sobreyectivo si y sólo si $\mathrm{Im}(f) = N$.

Dos A-módulos M y N se dicen ser **isomorfos** ($M \cong N$) si existe un homomorfismo de A-módulos $f : M \longrightarrow N$ biyectivo (f es un isomorfismo).

Teorema 2.1.2. Sean A un anillo y M un A-módulo. Entonces $\mathrm{Hom}_A(A, M) \cong M$.

Definición 2.1.4. La aplicación $\psi : \mathrm{Hom}_A(A, M) \longrightarrow M$ dada por $f \mapsto f(1)$ es un homomorfismo de A-módulos:

(i) $\psi(f + g) = (f + g)(1) = f(1) + g(1) = \psi(f) + \psi(g)$.

(ii) $\psi(a \cdot f) = (a \cdot f)(1) = a \cdot f(1) = a \cdot \psi(f)$.

(iii) ψ es inyectivo, ya que si $f \in \mathrm{Ker}(\psi)$ entonces $f(1) = 0$. Luego, para todo $a \in A$ se tiene

$$f(a) = f(a \cdot 1) = a \cdot f(1) = a \cdot 0 = 0.$$

(iv) ψ es sobreyectivo, ya que para todo $m \in M$ se define $f : A \longrightarrow M$ por $f(a) = a \cdot m$. Es claro que f es un homomorfismo de A-módulos. Además, $\psi(f) = f(1) = 1 \cdot m = m$.

Ejemplo 2.1.3. El conjunto $M(A)$ de matrices con coeficientes en A es un $\mathbb{Z}$-módulo. El conjunto

$$Z(M(A)) = \{X \in M(A) \ / \ BX = XB \text{ para todo } B \in M(A)\}$$

es un submódulo de $M(A)$.

Si N es un submódulo de M, se define la relación $m_1 \equiv m_2 \pmod N \iff m_1 - m_2 \in N$. Es claro que $\equiv \pmod N$ es una relación de equivalencia. Consideramos el conjunto cociente $\frac{M}{N} = \{\overline{m} \ / \ m \in M\}$, donde $\overline{m} = \{x \in M \ / \ m \equiv x((mod\mathrm{N}))\}$.

Ejercicio 2.1.3. Probar que con las operaciones $\overline{m_1} + \overline{m_2} = \overline{m_1 + m_2}$ y $a \cdot \overline{m} = \overline{a \cdot m}$, el conjunto $\frac{M}{N}$ es un A-módulo.

La aplicación $\pi : M \longrightarrow \frac{M}{N}$ dada por $\pi(m) = \overline{m}$ es un homomorfismo de A-módulos:

$$\pi(m_1 + m_2) = \overline{m_1 + m_2} = \overline{m_1} + \overline{m_2} = \pi(m_1) + \pi(m_2),$$
$$\pi(a \cdot m) = \overline{a \cdot m} = a \cdot \overline{m} = a \cdot \pi(m),$$

para todo $a \in A$ y $m_1, m_2, m \in M$.

Ejercicio 2.1.4. Probar que existe una correspondencia biyectiva entre los submódulos de M que contienen a N y los submódulos de $\frac{M}{N}$. *Sugerencia: Si J es un submódulo de M que contiene a N, defina $\psi(J) = \overline{J} = \{\overline{x} \ / \ x \in J\}$.*

Teorema 2.1.3. Si $f : M \longrightarrow N$ es un homomorfismo de A-módulos, entonces $\frac{M}{\mathrm{Ker}(f)} \cong \mathrm{Im}(f)$.

Demostración: Considere la proyección $\pi : M \longrightarrow \frac{M}{\mathrm{Ker}(f)}$. Definamos una aplicación $\overline{f}$ de $\frac{M}{\mathrm{Ker}(f)}$ en $\mathrm{Im}(f)$ por $\overline{f}(\overline{m}) = f(m)$. Veamos que $\overline{f}$ está bien definida. Supongamos que $m_1 \equiv m_2 \pmod{\mathrm{Ker}(f)}$. Luego, $m_1 - m_2 \in \mathrm{Ker}(f)$. De donde $0 = f(m_1 - m_2) = f(m_1) - f(m_2)$, y por tanto $f(m_1) = f(m_2)$. Ahora veamos que $\overline{f}$ es un homomorfismo de A-módulos:

$$\overline{f}(\overline{m_1} + \overline{m_2}) = \overline{f}(\overline{m_1 + m_2}) = f(m_1 + m_2) = f(m_1) + f(m_2) = \overline{f}(m_1) + \overline{f}(m_2),$$
$$\overline{f}(a \cdot \overline{m}) = \overline{f}(\overline{a \cdot m}) = f(a \cdot m) = a \cdot f(m) = a \cdot \overline{f}(\overline{m}),$$

para todo $a \in A$ y $\overline{m_1}, \overline{m_2}, \overline{m} \in \frac{M}{\mathrm{Ker}(f)}$. Finalmente, probaremos que $\overline{f}$ es un isomorfismo. Si $\overline{m} \in \mathrm{Ker}(\overline{f})$, tenemos que $m \in \mathrm{Ker}(f)$, por lo que $\overline{m} = \overline{0}$. Entonces $\overline{f}$ es inyectivo. Es claro que $\overline{f}$ es sobreyectivo. $\square$

Definición 2.1.5. El **conúcleo** de un homomorfismo de A-m odulos $f : M \longrightarrow N$ es el A-módulo cociente $\frac{N}{\mathrm{Im}(f)}$.

La intersección de submódulos es un submódulo: sea $\mathcal{F}$ una familia de submódulos de M, entonces

$$J = \bigcap \{N \ / \ N \in \mathcal{F}\}$$

es un submódulo de M.

(i) Si $x, y \in J$ entonces $x, y \in N$ para todo $N \in \mathcal{F}$. Luego $x - y \in N$ para todo $N \in \mathcal{F}$, es decir $x - y \in J$.

(ii) $0 \in N$ para todo $N \in \mathcal{F}$. De donde $0 \in J$.

(iii) Si $x \in J$ y $a \in A$ entonces $x \in N$ para todo $N \in \mathcal{F}$. De donde $a \cdot n \in N$ para todo $N \in \mathcal{F}$, es decir $a \cdot n \in J$.

Ejercicio 2.1.5. Si I y J son dos submódulos de M, demuestre que $I+J := \{x+y \ / \ x \in I,\ y \in J\}$ es un submódulo de M.

Veamos que

$$I+J = \bigcap\{N \ / \ N \in \mathcal{F}\},\ \text{donde } \mathcal{F} = \{N \subseteq M \ / \ N \text{ es un submódulo de } M \text{ e } I, J \subseteq N\}.$$

Si $x+y \in I+J$, donde $x \in I$ y $y \in J$, entonces $x, y \in N$ para todo $N \in \mathcal{F}$. Luego $x+y \in N$ para todo $N \in \mathcal{F}$, es decir $x+y \in \bigcap\{N \ / \ N \in \mathcal{F}\}$. Por otro lado, $I+J \in \mathcal{F}$, de donde $\bigcap\{N \ / \ N \in \mathcal{F}\} \subseteq I+J$.

Ejercicio 2.1.6. Si $\mathcal{F} = \{N_i \ / \ i \in I\}$ es una familia de submódulos de M, probar que

$$\sum_{i\in I} N_i = \{m_{i_1} + \cdots + m_{i_n} \ / \ m_{i_j} \in N_{i_j},\ i_j \in I\}$$

es un submódulo de M y que $\sum_{i\in I} N_i \supseteq \bigcap_{i\in I} N_i$.

Ejercicio 2.1.7. Probar que:

(i) Si L, M, N son A-módulos y $N \subseteq M \subseteq L$ entonces $\frac{L/N}{M/N} \cong \frac{L}{M}$. *Sugerencia: Use el teorema anterior para la aplicación* $f : L/N \longrightarrow L/M$ *dada por* $\overline{m}^N \mapsto \overline{m}^M$.

(ii) Si M_1, M_2 son submódulos de M entonces $\frac{M_1+M_2}{M_1} \cong \frac{M_2}{M_1\cap M_2}$.

Sea M un A-módulo e I un ideal de A, el conjunto

$$IM = \{x_1m_1 + \cdots + x_nm_n \ / \ n \in \mathbb{N},\ x_i \in I,\ m_i \in M\}$$

es un submódulo de M:

(i) Si $x_1m_1+\cdots+x_nm_n, x'_1m'_1+\cdots+x'_nm'_n \in IM$ entonces $x_1m_1+\cdots+x_nm_n-x'_1m'_1-\cdots-x'_nm'_n \in IM$.

(ii) $0_M = 0_A \cdot 0_M \in IM$.

(iii) Si $x_1m_1+\cdots+x_nm_n \in IM$ y $a \in A$ entonces $a\cdot(x_1m_1+\cdots+x_nm_n) = (a\cdot x_1)m_1+\cdots+(a\cdot x_n)m_n \in IM$.

2.2 Conductor y anulador

Definición 2.2.1. Si N y P son submódulos de M, el conjunto $(N:P) = \{a \in A \ / \ a\cdot P \subseteq N\}$ se denomina **conductor** de P en N.

El conductor $(N:P)$ es un ideal de A:

(i) Si $a, b \in (N:P)$ entonces $a\cdot P \subseteq N$ y $b\cdot P \subseteq N$. Luego, para todo $p \in P$ se tiene $(a-b)\cdot p = a\cdot p - b\cdot p \in N$, de donde $(a-b)\cdot P \subseteq N$.

(ii) $0 \in (N:P)$ porque $0\cdot P = \langle 0\rangle \subseteq N$.

(iii) Si $a \in (N:P)$ y $x \in A$ entonces $a\cdot P \subseteq N$ y $(x\cdot a)\cdot P = x\cdot(a\cdot P) \subseteq N$. De donde $x\cdot a \in (N:P)$.

Definición 2.2.2. Dado un A-módulo M, el conjunto $\text{Ann}(M) := \{x \in A \ / \ x \cdot m = 0, \text{ para todo } m \in M\}$ se denomina **anulador** de M .

Ejemplo 2.2.1.

(i) $\text{Ann}(\mathbb{Z}) = \langle 0 \rangle$.

(ii) $\text{Ann}(\mathbb{Z}_6) = \{6z \ / \ z \in \mathbb{Z}\}$.

(iii) $\text{Ann}(M) = (\langle 0 \rangle : M)$.

Sea A un anillo y M un A-módulo. Si $I \subseteq A$ es un ideal contenido en $\text{Ann}(M)$ entonces M es un $\frac{A}{I}$-módulo con la suma de M y el producto dado por $\cdot : \frac{A}{I} \times M \longrightarrow M$ dado por $(\overline{a}, m) \mapsto a \cdot m$. Veamos que este producto está bien definido. Supongamos que $\overline{a} = \overline{b}$. Entonces $a - b \in I \subseteq \text{Ann}(M)$. Luego, para todo $m \in M$ se tiene $(a - b) \cdot m = 0$, por lo que $a \cdot m = b \cdot m$. Además, este producto satisface los axiomas correspondientes en la definición de anillo:

$$(\overline{a} + \overline{b}) \cdot m = (\overline{a + b}) \cdot m = (a + b) \cdot m = a \cdot m + b \cdot m = \overline{a} \cdot m + \overline{b} \cdot m.$$

Un A-módulo M se dice fiel si $\text{Ann}(M) = \langle 0 \rangle$. El anulador $\text{Ann}_{\frac{A}{\text{Ann}(M)}}(M)$ como $\frac{A}{\text{Ann}(M)}$-módulo es $\langle 0 \rangle$. En efecto, si $\overline{x} \in \text{Ann}_{\frac{A}{\text{Ann}(M)}}(M)$ entonces $x \cdot \overline{x} \cdot m = 0$, por lo que $x \in \text{Ann}(M)$ y $\overline{x} = \overline{0}$. Tenemos que todo A-módulo M es fiel como $\frac{A}{\text{Ann}(M)}$-módulo.

Ejercicio 2.2.1. Demuestre que

(1) $\text{Ann}(M + N) = \text{Ann}(M) \cap \text{Ann}(N)$.

(2) Si N y P son submódulos de M entonces $(N : P) = \text{Ann}\left[\frac{N+P}{N}\right]$.

2.3 Módulos (finitamente) generados

Sea M un A-módulo y $x \in M$. Definimos $\langle x \rangle := \{a \cdot x \ / \ a \in A\}$ como el submódulo de M **generado** por x. Sean $x_1, \ldots, x_n \in M$. Si M es igual a $\langle x_1, \ldots, x_n \rangle := \{a_1 \cdot x_1 + \cdots + a_n \cdots x_n \ / \ a_i \in A\}$, se dice que M está generado por $\{x_1, \ldots, x_n\}$, o que M es un A-módulo **finitamente generado** (**f.g.**). De manera más general, diremos que M está generado por un conjunto $\{x_i\}_{i \in I}$ si

$$M = \sum_{i \in I} \langle x_i \rangle = \{a_{i_1} \cdot x_{i_1} + \cdots + a_{i_n} \cdot x_{i_n} \ / \ i_1, \ldots, i_n \in I, \ a_{i_1}, \ldots, a_{i_n} \in A, \ n \in \mathbb{N}\}.$$

Ejemplo 2.3.1. $\mathbb{K}[x] = \{a_0 + a_1 \cdot x + \cdots + a_n \cdot x^n \ / \ a_1, \ldots, a_n \in \mathbb{K}, \ n \in \mathbb{N}\}$ es un módulo generado por $\{x^n\}_{n \in \mathbb{N}}$.

Definición 2.3.1. Sean M y N A-módulos. Se define la **suma directa externa** de M y N como el A-módulo dado por el conjunto $M \oplus^{\text{ext}} N := \{(m, n) \ / \ m \in M \text{ y } n \in N\}$ junto con las siguientes operaciones:

$$(m_1, n_1) + (m_2, n_2) = (m_1 + m_2, n_1 + n_2), \text{ y}$$
$$a \cdot (m, n) = (a \cdot m, a \cdot n).$$

Ejercicio 2.3.1. Si N_1 y N_2 son submódulos de M, probar que la aplicación $\psi : N_1 \oplus^{\text{ext}} N_2 \longrightarrow N_1 + N_2$ dada por $(n_1, n_2) \mapsto n_1 + n_2$ es un isomorfismo de A-módulos si, y sólo si, $N_1 \cap N_2 = \langle 0 \rangle$.

Definición 2.3.2. Sean A un anillo, M un A-módulo y N_1, N_2 submódulos de M. La suma

$$N_1 + N_2 = \{n_1 + n_2 \ / \ n_1 \in N_1 \text{ y } n_2 \in N_2\}$$

se dice **suma directa interna** si $N_1 \cap N_2 = \langle 0 \rangle$, y la denotaremos por $N_1 \oplus^{\text{int}} N_2$.

Ejemplo 2.3.2. $\langle e_1 \rangle \oplus^{\text{int}} \langle e_2 \rangle = \mathbb{R}^2$, donde $e_1 = (1, 0)$ y $e_2 = (0, 1)$.

Sea $\mathcal{F} = \{N_i\}_{i \in \mathcal{A}}$ una familia de A-módulos. La suma directa externa de los módulos de $\mathcal{F}$ es

$$\bigoplus_{i \in \mathcal{A}}^{\text{ext}} N_i = \{(x_i)_{i \in \mathcal{A}} \ / \ x_i \neq 0 \text{ sólo para un número finito de índices } i \in \mathcal{A}\},$$

es decir $(x_i)_{i \in \mathcal{A}} = (\dots, 0, \dots, x_{i_1} \neq 0, \dots, x_{i_2} \neq 0, \dots, 0, \dots)$. La suma se define coordenada a coordenada, al igual que el producto por elementos de A:

$$(x_i)_{i \in \mathcal{A}} + (y_i)_{i \in \mathcal{A}} = (x_i + y_i)_{i \in \mathcal{A}},$$
$$a \cdot (x_i)_{i \in \mathcal{A}} = (a \cdot x_i)_{i \in \mathcal{A}}.$$

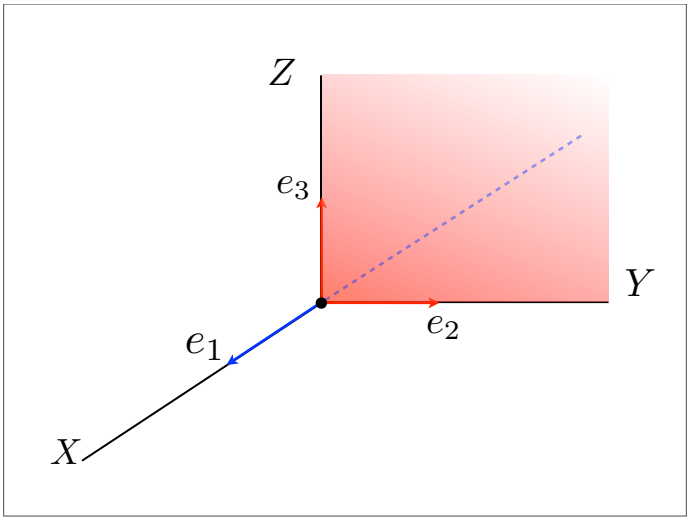
Con estas operaciones, la suma directa externa deviene en un A-módulo.

De forma similar, el producto directo de $\mathcal{F}$ viene dado por $\prod_{i \in \mathcal{A}} N_i = \{(x_i)_{i \in \mathcal{A}}\}$ y es un A-módulo con las operaciones anteriores. Si $\mathcal{A}$ es finito, note que $\prod_{i \in \mathcal{A}} N_i = \bigoplus_{i \in \mathcal{A}}^{\text{ext}} N_i$.

Ejercicio 2.3.2. Sea $\{N_i\}_{i \in \mathcal{A}}$ una familia de A-módulos. Entonces la aplicación $\psi : \bigoplus_{i \in \mathcal{A}}^{\text{ext}} N_i \longrightarrow \sum_{i \in \mathcal{A}} N_i$ dada por $(n_i)_{i \in \mathcal{A}} \mapsto n_{i_1} + \cdots + n_{i_r} + 0$ (donde los n_{i_j} son no-nulos) es un isomorfismo si, y sólo si, para todo i se tiene $N_i \cap \left(\sum_{j \in \mathcal{A} \setminus \{i\}} N_j \right) = \langle 0 \rangle$.

Se define la suma directa interna $\sum_{i \in \mathcal{A}} N_i$ si para todo $i \in \mathcal{A}$ se tiene $N_i \cap \left(\sum_{j \in \mathcal{A} \setminus \{i\}} N_j \right)$. Se denota por $\bigoplus_{i \in \mathcal{A}}^{\text{int}} N_i$.

Ejemplo 2.3.3. $\langle e_1 \rangle \oplus^{\text{int}} \langle e_2 \rangle \oplus^{\text{int}} \langle e_3 \rangle = \mathbb{R}^3$, $\langle e_1 \rangle \cap (\langle e_2 \rangle \oplus \langle e_3 \rangle) = \{0\}$.



Ejemplo 2.3.4. $\mathbb{R}[x] = \langle 1 \rangle \oplus \langle x \rangle \oplus \langle x^2 \rangle \oplus \cdots$.

Sean A_i anillos, donde $i = 1, 2, \ldots, n$. Tenemos que $A = \prod_{i=1}^{n} A_i$ es un anillo con las siguientes operaciones:

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n),$$
$$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) = (a_1 \cdot b_1, \ldots, a_n \cdot b_n).$$

Sean $I_i = \{(0, \ldots, a_i, \ldots, 0) \ / \ a_i \in A_i\} \subseteq A = \prod_{i=1}^{n} A_i$. Considere los homomorfismos $\delta_i : A \longrightarrow A_i$ dados por $(a_1, \ldots, a_n) \mapsto a_i$. Tenemos que $\delta_i|_{I_i}$ es inyectivo y sobreyectivo. Note que $(1, \ldots, 1) \notin I_i$, por lo que I_i no es un subanillo de A.

Ejercicio 2.3.3. Considere el producto $(a_1, \ldots, a_n) \cdot b = a_i \cdot b$. Con este producto, A_i es un A-módulo. Más aún, $(0, \ldots, 1, \ldots, 0)$ es un divisor de cero en A_i y $A = \bigoplus_{i=1}^{\text{int n}} I_i$.

2.4 Producto tensorial de módulos

Sean M, N y P A-módulos. Una función $\psi : M \times N \longrightarrow P$ se dice **bilineal** si:

(1) Para todo $m_1, m_2 \in M$, $n \in N$ y $a \in A$, se tiene: $\psi(m_1 + am_2, n) = \psi(m_1, n) + a\psi(m_2, n)$.

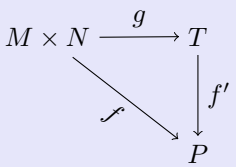
(2) Para todo $m \in M$, $n_1, n_2 \in N$ y $a \in A$, se tiene: $\psi(m, n_1 + an_2) = \psi(m, n_1) + a\psi(m, n_2)$.

Dados A-módulos $M_1, \ldots, M_k$ y P, una función $\psi : M_1 \times \cdots \times M_k \longrightarrow P$ se dice k**-lineal** si para todo $1 \leq i \leq k$, dados $m_1 \in M_1$, $\ldots$, $m_i \in M_i$, $\ldots$, $m_k \in M_k$ y $a \in A$, se tiene:

$$\psi(m_1, \ldots, m_i + am_i', \ldots, m_k) = \psi(m_1, \ldots, m_i, \ldots, m_k) + a \cdot \psi(m_1, \ldots, m_i', \ldots, m_k).$$

Proposición 2.4.1. Dados A-módulos M y N, existe un par (T, g) donde T es un A-módulo y g es una función bilineal $M \times N \longrightarrow T$ que satisface:

(1) Para todo A-módulo P y toda función bilineal $f : M \times N \longrightarrow P$, existe un único homomorfismo de A-módulos $f' : T \longrightarrow P$ tal que $f' \circ g = f$, es decir, el siguiente diagrama es conmutativo:



(2) Si (T', g') es otro par, donde T' es un A-módulo y $g' : M \times N \longrightarrow T'$ es un homomorfismo de A-módulos, que satisface (1), entonces existe un isomorfismo $j : T \longrightarrow T'$ tal que $j \circ g = g'$.

Demostración:

(1) Considere el A-módulo libre $C = A^{M\times N} = \{\sum_{i=1}^{n} a_i(m_i, n_i) \ / \ a_i \in A,\ m_i \in M,\ n \in \mathbb{N}\}$. Sea D el submódulo de C generado por los elementos de la forma

$$(x + x', y) - (x, y) - (x', y),\ (x, y + y') - (x, y) - (x, y'),\ (ax, y) - a(x, y) \ \text{ y } \ (x, ay) - a(x, y),$$

donde $x, x' \in M$, $y, y' \in N$, y $a \in A$. Sea $T = \frac{C}{D}$ y $g : M \times N \longrightarrow T$ el homomorfismo dado por $(m, n) \mapsto \overline{(m, n)} := m \otimes n$. Tenemos

$$g(m + am', n) = (m + am') \otimes n = \overline{(m + am', n)}.$$

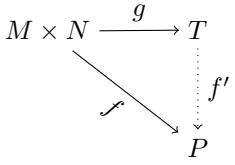
Como $(m + am', n) = (m, n) - (am', n) \in D$, tenemos

$$\overline{(m + am', n)} = \overline{(m, n)} + \overline{(am', n)} \text{ y } \overline{(am', n)} = a(m', n),$$

es decir

$$g(m + am', n) = m \otimes n + am' \otimes n = g(m, n) + ag(m', n).$$

Sea P un A-módulo y $f : M \times N \longrightarrow P$ bilineal. Queremos construir un único homomorfismo de A-módulos $f' : T \longrightarrow P$ tal que el siguiente diagrama conmuta:



Definimos $f_0 : C \longrightarrow P$ como $f_0(m, n) = f(m, n)$ para todo $(m, n) \in M \times N$, y extendemos por linealidad. Ahora definimos $f' : T \longrightarrow P$ como $f'(m \otimes n) = f_0(m, n) = f(m, n)$. Note que

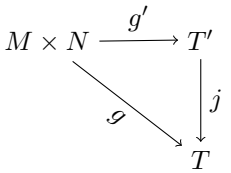
$$\begin{aligned} f_0[(m + am', n) - (m, n) - a(m', n)] &= f[(m + am', n) - (m, n) - a(m', n)] \\ &= f_0(m + am') - f_0(m, n) - af_0(m', n) \\ &= f(m, n) - af(m', n) - f(m, n) - af(m', n) \\ &= 0. \end{aligned}$$

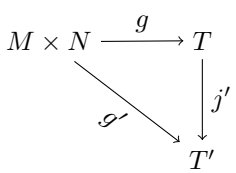
Luego para todo $\alpha \in D$, tenemos $f_0(\alpha) = 0$, es decir $D \subseteq \text{Ker}(f_0)$. Para ver que f' está bien definida, si $\alpha, \beta \in C$ son tales que $\overline{\alpha} = \overline{\beta}$ en T, entonces $\alpha - \beta \in D$ y por tanto $f'(\alpha - \beta) = 0$. De donde $f'(\overline{\alpha}) = f'(\overline{\beta})$. Además, para todo $(m, n) \in M \times N$, tenemos

$$f(m, n) = f'(m \otimes n) = f' \circ g(m, n),$$

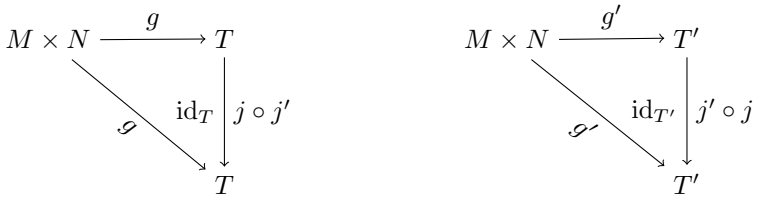
de donde $f = f' \circ g$.

(2) Sean (T, g) y (T, g') dos pares que satisfacen (1). Tenemos $T = \langle g(M \times N)\rangle$ y $T' = \langle g'(M \times N)\rangle$. Usando la propiedad (1), tenemos los siguientes diagramas conmutativos:





Tenemos $g = j \circ g' = j \circ (j' \circ g) = (j \circ j') \circ g$ y $g' = j' \circ g = j' \circ (j \circ g') = (j' \circ j) \circ g'$. De donde tenemos los siguientes diagrama conmutativos:



Por (1), tenemos $j \circ j' = \mathrm{id}_T$ y $j' \circ j = \mathrm{id}_{T'}$. De donde $T = T'$ y $g = g'$.

□

Ejercicio 2.4.1. Probar la unicidad de f' en la proposición anterior.

2.5 Ideales y módulos finitamente generados

Proposición 2.5.1. Sea A un anillo, I un ideal de A, M un A-módulo finitamente generado y $\phi : M \longrightarrow M$ tal que $\phi(M) \subseteq I \cdot M$. Entonces ϕ satisface un polinomio $x^n + \cdots + a_1 x + a_0$ con coeficientes en I.

Demostración: Sea $M = \langle x_1, \ldots, x_n \rangle$. Considere $\phi(x_1), \ldots, \phi(x_n) \in I \cdot M$. Tenemos

$$\begin{aligned} \phi(x_1) &= a_{11}x_1 + \cdots + a_{n1}x_n, \\ &\vdots \\ \phi(x_n) &= a_{1n}x_1 + \cdots + a_{nn}x_n, \end{aligned}$$

donde cada $a_{ij} \in I$. Luego,

$$A_\phi = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \in M_n(I).$$

Tenemos el polinomio $p_\phi(x) = \det(x\mathrm{Id} - A_\phi) = x^n + \cdots + a_1 x + a_0$, donde $a_{n-1}, \ldots, a_0 \in I$. Además, $(A_\phi)^n + a_{n-1}(A_\phi)^{n-1} + \cdots + a_1 A_\phi + a_0 \mathrm{Id} = 0$. □

Corolario 2.5.1. Si M es un A-módulo finitamente generado y $I \subseteq A$ es un ideal de A tal que $I \cdot M = M$, entonces existe $x \equiv 1 (\mathrm{mod}\ I)$ tal que $x \cdot M = 0$.

Demostración: Considere el homomorfismo identidad $\mathrm{id} : M \longrightarrow M$, donde $\mathrm{id}(M) = M \subseteq I \cdot M$. Por la proposición anterior, existe un polinomio existen $a_0, a_1, \ldots, a_{n-1} \in I$ tales que

$$0 = \mathrm{Id}^n + a_{n-1}\mathrm{Id}^{n-1} + \cdots + a_1\mathrm{Id} + a_0\mathrm{Id} = (A_{\mathrm{id}})^n + a_{n-1}(A_{\mathrm{id}})^{n-1} + \cdots + a_1 A_{\mathrm{id}} + a_0\mathrm{Id}.$$

Sea $x = 1 + a_{n-1} + \cdots + a_1 + a_0$. Tenemos $x \cdot \mathrm{Id} = 0$, de donde $x = 0$ y así $x - 1 = a_{n-1} + \cdots + a_1 + a_0 \in I$, es decir $x \equiv 1 (\mathrm{mod}\ I)$. □

Lema 2.5.1 (de Nakayama)**.** Sea M un A-módulo finitamente generado e I un ideal de A contenido en el radical de Jacobson R. Entonces $I \cdot M = M \Longrightarrow M = 0$.

Demostración: Por el corolario anterior, existe $x \equiv 1 (\mathrm{mod}\ I)$ tal que $x \cdot M = 0$. Como $x - 1 \in I \subseteq R$, tenemos que $x \in U(A)$, por lo que $x \cdot M = 0 \Longrightarrow M = x^{-1}x \cdot M = 0$. □

Corolario 2.5.2. Sea M un A-módulo finitamente generado, $N \subseteq M$ un submódulo, e $I \subseteq A$ un ideal contenido en el radical de Jacobson R. Entonces $M = I \cdot M + N \Longrightarrow M = N$.

Demostración: $I \cdot \left(\frac{M}{N}\right) = I \cdot \left(\frac{M+N}{N}\right) = \frac{I \cdot M + I \cdot N}{N} = \frac{I \cdot M + N}{N} = \frac{M}{N} \Longrightarrow \frac{M}{N} = 0 \Longrightarrow M = N.$ □

Ejercicio 2.5.1. Recuerde que si A es un anillo local y $\mathcal{M}$ es su ideal maximal, entonces $K = A/\mathcal{M}$ es un cuerpo.

(1) Buscar ejemplos de anillos locales que no sean cuerpos.

(2) $\frac{M}{\mathcal{M} \cdot M}$ es un K-espacio vectorial de dimensión finita.

2.6 Sucesiones exactas

Proposición 2.6.1. La sucesión

$$M' \xrightarrow{u} M \xrightarrow{v} M'' \longrightarrow 0$$

de A-módulos y homomorfismos de A-módulos es exacta si, y sólo si, para todo A-módulo N la sucesión

$$0 \longrightarrow \mathrm{Hom}(M'', N) \xrightarrow{\overline{v}} \mathrm{Hom}(M, N) \xrightarrow{\overline{u}} \mathrm{Hom}(M', N)$$

es exacta, donde

$$\overline{v}(f) = f \circ v : M \longrightarrow N, \text{ para todo } f : M'' \longrightarrow N,$$
$$\overline{u}(g) = g \circ u : M' \longrightarrow N, \text{ para todo } g : M \longrightarrow N.$$

Demostración:

($\Longrightarrow$) Probemos exactitud en $\overline{v}$, es decir, veamos que $\overline{v}$ es inyectivo. Sea $f : M'' \longrightarrow N$ un homomorfismo de A-módulos tal que $f \in \mathrm{Ker}(\overline{v})$. Luego $\overline{v}(f) = f \circ v = 0$. De donde $\mathrm{Im}(v) \subseteq \mathrm{Ker}(f)$. Por otro lado, $m'' \in \mathrm{Im}(v)$, para todo $m'' \in M$, pues v es sobreyectivo. Así, existe $m \in M$ tal que $m'' = v(m)$. Nos queda $f(m'') = f \circ v(m) = 0$. Entonces $f \equiv 0$ y $\mathrm{Ker}(\overline{v}) = \{0\}$.

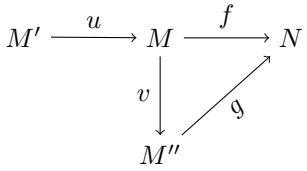
Ahora probemos la exactitud en $\overline{u}$, es decir $\mathrm{Im}(\overline{v}) = \mathrm{Ker}(\overline{u})$. Considere $f \circ v = \overline{v}(f) \in \mathrm{Im}(\overline{v})$, donde $f : M'' \longrightarrow N$. Tenemos

$$(\overline{u} \circ \overline{v})(f) = \overline{u}(\overline{v}(f)) = \overline{u}(f \circ v) = f \circ (v \circ u) = f \circ 0 \equiv 0, \text{ pues } \mathrm{Im}(u) = \mathrm{Ker}(v).$$

Luego, $\overline{u}[\overline{v}(f)] = 0 \Longrightarrow \mathrm{Im}(\overline{v}) \subseteq \mathrm{Ker}(\overline{u})$. Ahora, si $f \in \mathrm{Ker}(\overline{u})$, $f : M \longrightarrow N$, entonces

$$0 = f \circ u = \overline{u}(f).$$

De donde $\mathrm{Ker}(v) = \mathrm{Im}(u) \subseteq \mathrm{Ker}(f)$. Como v es sobreyectivo, para cada $m'' \in M''$ existe $m \in M$ tal que $m'' = v(m)$. Definimos $g(m'') = f(m)$. Tenemos el siguiente diagrama:



Veamos que g es una aplicación bien definida. Sean $m_1, m_2 \in M$ tales que $v(m_1) = v(m_2)$. Entonces $v(m_1 - m_2) = 0$, es decir $m_1 - m_2 \in \mathrm{Ker}(v) = \mathrm{Im}(u)$. De donde existe $m' \in M$ tal que $u(m') = m_1 - m_2$. Tenemos $0 = f \circ u(m') = f(m_1 - m_2)$, es decir $f(m_1) = f(m_2)$. Finalmente, $g \circ v = f$, es decir $f = \overline{v}(g) \in \mathrm{Im}(\overline{v})$.

($\Longleftarrow$) Veamos que v es sobreyectivo. Para $N = \frac{M''}{\mathrm{Im}(v)}$, la sucesión

$$0 \longrightarrow \mathrm{Hom}\left(M'', \frac{M''}{\mathrm{Im}(v)}\right) \xrightarrow{\overline{v}} \mathrm{Hom}\left(M, \frac{M''}{\mathrm{Im}(v)}\right) \xrightarrow{\overline{u}} \mathrm{Hom}\left(M', \frac{M''}{\mathrm{Im}(v)}\right)$$

es exacta. Considere la proyección canónica $\pi : M'' \longrightarrow \frac{M''}{\mathrm{Im}(v)}$. Tenemos

$$(\pi \circ v)(m) = \pi(v(m)) = \overline{v(m)} = 0,$$

es decir $\overline{v}(\pi) = \pi \circ v \equiv 0$. Como $\overline{v}$ es injectivo, tenemos que $\pi \equiv 0$. Luego, $m'' \in \mathrm{Im}(v)$ para todo $m'' \in M''$. De donde v es sobreyectivo.

Ahora verifiquemos la exactitud en u ($\mathrm{Im}(u) = \mathrm{Ker}(v)$). La sucesión

$$0 \longrightarrow \mathrm{Hom}(M'', M'') \xrightarrow{\overline{v}} \mathrm{Hom}(M, M'') \xrightarrow{\overline{u}} \mathrm{Hom}(M', M'')$$

es exacta. Considere el homomorfismo identidad $\mathrm{id} : M \longrightarrow M$. Tenemos

$$v = \mathrm{id} \circ v = \overline{v}(\mathrm{id}) \in \mathrm{Im}(\overline{v}) = \mathrm{Ker}(\overline{u}).$$

De donde $v \circ u = \overline{u}(v) = 0$ implica $\mathrm{Im}(u) \subseteq \mathrm{Ker}(v)$. Falta ver que $\mathrm{Ker}(v) \subseteq \mathrm{Im}(u)$. La sucesión

$$0 \longrightarrow \mathrm{Hom}\left(M'', \frac{M}{\mathrm{Im}(u)}\right) \xrightarrow{\overline{v}} \mathrm{Hom}\left(M, \frac{M}{\mathrm{Im}(u)}\right) \xrightarrow{\overline{u}} \mathrm{Hom}\left(M', \frac{M}{\mathrm{Im}(u)}\right)$$

es exacta. Considere la proyección $\pi : M \longrightarrow \frac{M}{\mathrm{Im}(u)}$. Note que $\overline{u}(\pi) = \pi \circ u \equiv 0$. De donde $\mathrm{Im}(u) \subseteq \mathrm{Ker}(\pi) = \mathrm{Im}(u)$. Tenemos $\pi \in \mathrm{Ker}(\pi) = \mathrm{Im}(\overline{v})$, es decir que existe $f : M'' \longrightarrow \frac{M}{\mathrm{Im}(u)}$ tal que $\pi = \overline{v}(f) = f \circ v$. Si $m \in \mathrm{Ker}(v)$, entonces $v(m) = 0$ implica que $(f \circ v)(m) = 0$, es decir $\pi(m) = 0$. Tenemos $m \in \mathrm{Ker}(\pi)$. Finalmente, $\mathrm{Ker}(v) \subseteq \mathrm{Ker}(\pi) = \mathrm{Im}(u)$.

□

Proposición 2.6.2 (dual)**.** La sucesión

$$0 \longrightarrow N' \xrightarrow{u} N \xrightarrow{v} N''$$

es exacta si, y sólo si, para todo A-módulo M la sucesión

$$0 \longrightarrow \mathrm{Hom}(M, N') \xrightarrow{\overline{u}} \mathrm{Hom}(M, N) \xrightarrow{\overline{v}} \mathrm{Hom}(M, N'')$$

es exacta, donde

$$\overline{u}(f) = u \circ f,$$
$$\overline{v}(g) = v \circ g.$$

Ejercicio 2.6.1. Demuestre la proposición anterior.

CAPÍTULO 3

DOMINIOS EUCLÍDEOS

3.1 Dominios euclídeos y dominios de ideales principales

Definición 3.1.1. Un dominio entero D se dice **dominio euclídeo** si existe una función

$$\delta : D\backslash\{0\} \longrightarrow \mathbb{N} \cup \{0\}$$

que satisface:

(1) Para $a, b \in D\backslash\{0\}$, si $a|b$ (i.e. $b = c\dot{a}$ para algún $c \in D$) entonces $\delta(a) \leq \delta(b)$.

(2) Dados $a, b \in D$, donde $b \neq 0$, existen $q, r \in D$ tales que $a = b \cdot q + r$ con $r = 0$ o $\delta(r) \leq \delta(b)$.

Ejemplo 3.1.1.

(1) $\mathbb{Z}$ con la función $|\ | : \mathbb{Z}\backslash\{0\} \longrightarrow \mathbb{N} \cup \{0\}$ es un dominio euclídeo. En efecto, si $a|b$ entonces $|a| \leq |b|$. Si $a, b \in \mathbb{Z}$ y $b \neq 0$, entonces $a = b \cdot q + r$, donde $0 \leq r \leq |b|$.

(2) Sea $\mathbb{K}$ un cuerpo, $\mathbb{K}[x]$ es un dominio euclídeo, con la función grado : $\mathbb{K}[x]\backslash\{0\} \longrightarrow \mathbb{N} \cup \{0\}$ dada por

$$\text{grado}(a_0 + a_1 \cdot x + \cdots + a_n \cdot x^n) = n,$$

si $a_n \neq 0$. Dado el polinomio $p(x) = q(x) \cdot t(x)$, tenemos que $\text{grado}(p(x)) = \text{grado}(q(x)) + \text{grado}(t(x))$, luego $\text{grado}(q(x)) \leq \text{grado}(p(x))$.

Sean $p(x), q(x) \in \mathbb{K}[x]$, con $q(x) \neq 0$. Veamos que existen $t(x)$ y $r(x)$ tales que $p(x) = t(x) \cdot q(x) + r(x)$ con $r(x) = 0$ o $\text{grado}(r(x)) \leq \text{grado}(q(x))$. Tenemos tres casos a considerar:

i) Si $\text{grado}(q(x)) < \text{grado}(p(x))$ entonces $q(x) = p(x) \cdot 0 + q(x)$.

ii) Si $\text{grado}(q(x)) = \text{grado}(p(x))$, entonces:

$$\begin{aligned} p(x) &= p_0 + \cdots + p_n x^n,\ q(x) = q_0 + \cdots + q_n x^n \\ \left(p(x) \cdot \frac{q_n}{p_n}\right) &= c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} + q_n x^n \\ q(x) - p(x) \cdot \frac{q_n}{p_n} &= d_0 + d_1 x + \cdots + d_{n-1} x^{n-1} = r(x) \\ q(x) &= \frac{q_n}{p_n} \cdot p(x) + r(x),\ \text{donde } \text{grado}(r(x)) < n = \text{grado}(p(x)). \end{aligned}$$

iii) Supongamos grado$(p(x)) <$ grado$(q(x))$. Sea $q(x) = n^{n+1}$ y $p(x) = p_0 + \cdots + p_n x^n$. Tenemos

$$\begin{aligned} p(x) \cdot \left(\frac{1}{p_n} \cdot x\right) &= c_1 x + c_2 x^2 + \cdots + c_n x^n + x^{n+1} \\ q(x) - p(x) \cdot \left(\frac{1}{p_n} \cdot x\right) &= d_1 x + d_2 x^2 + \cdots + d_n x^n = s(x) \\ q(x) &= p(x) \cdot \left(\frac{1}{p_n} \cdot x\right) + s(x) \\ &= p(x) \cdot t(x) + p(x) \cdot t_0(x) + r(x) \\ &= p(x) \cdot [t(x) + t_0(x)] + r(x), \text{ grado}(r(x)) < \text{grado}(p(x)). \end{aligned}$$

Supongamos cierto que x^{n+1}, x^{n+2}, $\ldots$, x^{n+k-1} pueden escribirse como $x^{n+i} = p(x) \cdot t_i(x) + r_i(x)$ con $r_i \equiv 0$ o grado$(r_i(x)) <$ grado$(p(x))$:

$$\begin{aligned} q(x) &= x^{n+k} \\ p(x) &= p_0 + p_1 x + \cdots + p_n x^n \\ p(x) \cdot \frac{1}{p_n} x^k &= c_k x^k + \cdots + c_{n+k-1} x^{n+k-1} + x^{n+k} \\ q(x) - p(x) \cdot \frac{1}{p_n} x^k &= d_k x^k + \cdots + d_{n+k-1} x^{n+k-1} \\ &= [p(x)t_k(x) + r_k(x)] + \cdots + [p(x)t_{n+k-1}(x) + r(x)], \\ &\text{donde } r_i \equiv 0 \text{ o grado}(r_i(x)) < \text{grado}(p(x)). \\ &= p(x)[t_k(x) + \cdots + t_{n+k-1}(x)] + [r_k(x) + \cdots + r_{n+k-1}(x)], \\ &\text{donde } r(x) := r_k(x) + \cdots + r_{n+k-1}(x) = 0 \text{ o grado}(r(x)) < \text{grado}(p(x)). \end{aligned}$$

Proposición 3.1.1. Si D es un dominio euclídeo, entonces D es un dominio de ideales principales.

Demostración: Sea I un ideal de D. Si $I = \langle 0 \rangle$ entonces no hay nada que probar. Sea $x \in I \backslash \{0\}$ un elemento con grado mínimo en $\{\text{grado}(y) \ / \ y \in I\}$. Veamos que $I = \langle x \rangle$. Es claro que $\langle x \rangle \subseteq I$. Sea $y \in I$. Luego, $y = x \cdot p + r$, con $r = 0$ o grado$(r) <$ grado(x). Tenemos que la desigualdad anterior no puede ser cierta porque x posee grado mínimo. Luego, $r = 0$ y $y = x \cdot p$. □

Ejemplo 3.1.2. En particular, $\mathbb{Z}$ y $\mathbb{K}[x]$ son dominios de ideales principales por ser dominios euclídeos.

Ejercicio 3.1.1. En $\mathbb{Z}$, el máximo común divisor de dos enteros no nulos a y b es un número natural (a, b) que satisface:

(1) $(a, b)|a$ y $(a, b)|b$.

(2) Si $k|a$ y $k|b$ entonces $k \leq (a, b)$.

Esto equivale a: un número natural d es igual a (a, b) si, y sólo si,

(1)' $d|a$ y $d|b$.

(2)' Si $k|a$ y $k|b$, entonces $k|d$.

Ejercicio 3.1.2. El mínimo común múltiplo de dos enteros a y b es el número natural $[a,b]$ que satisface:

(1) $a|[a,b]$ y $b|[a,b]$.

(2) Si k satisface $a|k$ y $b|k$ entonces $[a,b] \leq k$.

Esto equivale a: $m = [a,b]$ si, y sólo si,

(1)' $a|m$ y $b|m$.

(2)' Si $k \in \mathbb{N}$ satisface $a|k$ y $b|k$, entonces $m|k$.

Ejercicio 3.1.3. En $\mathbb{Z}$, probar directamente que:

(1) $\langle m \rangle + \langle n \rangle = \langle (m,n) \rangle$.

(2) $\langle m \rangle \cap \langle n \rangle = \langle [m,n] \rangle$.

(3) $m \cdot n = (m,n) \cdot [m,n]$.

Ejercicio 3.1.4. Probar la Proposición 1.11 (página 9) del libro de M. F. Atiyah e I. G. MacDonald.

Sea $\phi : M \longrightarrow M$ un homomorfismo de A-módulos, donde $M = \langle x_1, \ldots, x_n \rangle$ es finitamente generado. Se puede considerar la matriz $A_\phi \in M_n(A)$. Así:

$$\begin{aligned} \phi(x_1) &= a_1 1 x_1 + \cdots + a_{n1} x_n, \\ &\vdots \\ \phi(x_n) &= a_{1n} x_1 + \cdots + a_{nn} x_n. \end{aligned}$$

Tenemos

$$A_\phi = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}.$$

Si $y \in M$, entonces $y = b_1 x_1 + \cdots + b_n x_n$, de donde

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \cdot \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} a_{11}b_1 + \cdots + a_{1n}b_n \\ \vdots \\ a_{n1}b_1 + \cdots + a_{nn}b_n \end{pmatrix}.$$

Además:

$$\begin{aligned} \phi(y) &= \phi(b_1 x_1 + \cdots + b_n x_n) = b_1 \phi(x_1) + \cdots + b_n \phi(x_n) \\ &= b_1(a_{11}x_1 + \cdots + a_{n1}x_n) + \cdots + b_n(a_{1n}x_1 \cdots + a_{nn}x_n) \\ &= (a_{11}b_1 + \cdots + a_{1n}b_n)x_1 + \cdots + (a_{n1}b_1 + \cdots + a_{nn}b_n)x_n. \end{aligned}$$

Definamos el polinomio de ϕ como

$$p_\phi(x) = \det(xI - A_\phi) = \begin{vmatrix} x - a_{11} & \cdots & -a_{1n} \\ \vdots & \ddots & \vdots \\ -a_{n1} & \cdots & x - a_{nn} \end{vmatrix}$$

Ejercicio 3.1.5. Probar que grado$(p_\phi) = n$ y el coeficiente de x^n en p_ϕ es 1.

En general, evaluar ϕ en un polinomio $a_m x^m + \cdots + a_1 x + a_0$ nos da $a_m(A_\phi)^m + \cdots + a_1 A_\phi + a_0 I$. Al evaluar ϕ en $p_\phi(x)$ nos da $0 = \det(A_\phi \cdot I - A_\phi) = p_\phi(\phi) = A_\phi^m + c_{n-1}A_\phi^{n-1} + \cdots + c_0 I$.

Teorema 3.1.1. Todo dominio de ideales principales es un anillo noetheriano.

Demostración: Sea $\langle x_1\rangle \subseteq \langle x_2\rangle \subseteq \cdots \subseteq \langle x_n\rangle \subseteq \cdots$ una cadena de ideales principales. Sea x el generador del ideal $\bigcup_{i\in\mathbb{N}} \langle x_i\rangle$. Entonces $x \in \bigcup_{i\in\mathbb{N}} \langle x_i\rangle$, luego existe $k \in \mathbb{N}$ tal que $x \in \langle x_k\rangle$. Por lo tanto

$$\bigcup_{i\in\mathbb{N}} \langle x_i\rangle = \langle x\rangle \subseteq \langle x_k\rangle \subseteq \bigcup_{i\in\mathbb{N}} \langle x_i\rangle .$$

Entonces, $\langle x_{k+l}\rangle \subseteq \langle x_k\rangle \subseteq \langle x_{k+l}\rangle$ para todo $l \in \mathbb{N}$, por lo que la cadena anterior es estacionaria. □

3.2 Cuerpo de fracciones de un dominio entero

En los dominios enteros se da la ley de cancelación, es decir que si $a \neq 0$ y $a \cdot x = a \cdot y$ entonces $x = y$. Si $\mathbb{K}$ es un cuerpo, entonces $\mathbb{K}$ contiene un dominio $D = \{z \cdot 1_\mathbb{K} \ / \ z \in \mathbb{Z}\}$, donde

$$z \cdot 1_\mathbb{K} = \begin{cases} 1_\mathbb{K} + \cdots + 1_\mathbb{K} \ z\text{-veces}, & \text{si } z > 0, \\ 0, & \text{si } z = 0, \\ -(|z| \cdot 1_\mathbb{K}), & \text{si } z < 0. \end{cases}$$

El recíproco también vale: "Todo dominio entero se sumerge en un cuerpo". Es decir, si D es un dominio entero, entonces existe un cuerpo K y un homomorfismo inyectivo de anillos $\psi : D \hookrightarrow K$.

Sea D un dominio entero. Vamos a construir un cuerpo K tal que D se sumerge en K. Se define la siguiente relación en $D \times D\backslash\{0\}$:

$$(a, b) \sim (c, d) \iff ad = bc.$$

Es fácil ver que $\sim$ es una relación de equivalencia. Sea $K := \frac{D\times D\backslash\{0\}}{\sim}$. Denotamos la clase de (a, b) como $\overline{(a, b)} := \frac{a}{b}$. Se definen la suma y la multiplicación en K como:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd},$$
$$\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}.$$

Veamos que estas operaciones están bien definidas. Supongamos que $\frac{a}{b} = \frac{a'}{b'}$ y $\frac{c}{d} = \frac{c'}{d'}$. Entonces $ab' = a'b$ y $cd' = c'd$. Para ver que la suma está bien definida, hay que probar que $(ad + bc)b'd' = (a'd' + b'c')bd$:

$$(ad + bc)b'd' = adb'd' + bcb'd' = a'dbd' + bc'b'd = (a'd' + b'c')bd.$$

Para la multiplicacón, hay que probar $acb'd' = a'c'bd$:

$$acb'd' = (ab')(cd') = (a'b)(c'd) = (a'c')(bd).$$

Con esta suma y producto, K deviene en un anillo, donde el elemento neutro está dado por $0_K = \frac{0}{k}$, para cualquier $k \in D\backslash\{0\}$. Para todo $\frac{a}{b}$, tenemos

$$\frac{0}{k} + \frac{a}{b} = \frac{b\cdot 0 + k\cdot a}{k\cdot b} = \frac{k\cdot a}{k\cdot b} = \frac{a}{b}.$$

Sea $1_K = \frac{1}{1} = \frac{x}{x}$, para cualquier $x \in D\backslash\{0\}$. Tenemos

$$1_k \cdot \frac{a}{b} = \frac{1}{1}\cdot\frac{a}{b} = \frac{1\cdot a}{1\cdot b} = \frac{a}{b}.$$

Dado $\frac{a}{b}$, su inverso respecto a la suma está dado por $-\left(\frac{a}{b}\right) = \frac{-a}{b} = \frac{a}{-b}$. En efecto,

$$\frac{a}{b} + \frac{-a}{b} = \frac{ab-ab}{b^2} = \frac{0}{b^2} = 0_K.$$

Además, todo $\frac{a}{b} \neq 0_K$ $(a \neq 0)$ es invertible respecto a la multiplicación, su inverso viene dado por $\frac{b}{a}$. Considere la aplicación $\psi : D \longrightarrow K$ dada por $d \mapsto \frac{d}{1}$. Tenemos:

$$\psi(d_1 + d_2) = \frac{d_1+d_2}{1} = \frac{d_1}{1} + \frac{d_2}{1} = \psi(d_1) + \psi(d_2),$$
$$\psi(d_1 \cdot d_2) = \frac{d_1\cdot d_2}{1} = \frac{d_1}{1}\cdot\frac{d_2}{1} = \psi(d_1)\cdot\psi(d_2).$$

Entonces, ψ es un homomorfismo de anillos. Más aún, ψ es inyectivo. Si $d \in \mathrm{Ker}(\psi)$ entonces $\frac{d}{1} = 0_K$, lo cual implica que $d = 0$.

3.3 Elementos divisibles, unidades, asociados, irreducibles y primos

Definición 3.3.1. Sea D un dominio entero.

(1) Para todo $a, b \in D$, diremos que a **divide a** b, denotado por $a|b$, si existe $c \in D$ tal que $b = ac$. Note que todo $a \in D$ divide a cero.

(2) Un elemento $u \in D$ es una **unidad** si $u|1$. Denotaremos por $U(D)$ el conjunto de las unidades de D.

(3) Dos elementos $a, b \in D$ se dicen **asociados** si $a|b$ y $b|a$, o equivalentemente, si existe $u \in U(D)$ tal que $a = ub$. (Note que esto define una relación de equivalencia).

(4) Un elemento $x \in D$ se dice **irreducible** si $x \notin U(D)$ y $x = ab \Longrightarrow a$ es una unidad o b es una unidad (o equivalentemente, $a \sim x$ o $b \sim x$ según la relación dada en (3)).

(5) Un elemento $x \in D$ se dice **primo** si $x \notin U(D)$, $x \neq 0$ y $x|ab \Longrightarrow x|a$ o $x|b$.

En todo dominio entero, un elemento primo es irreducible. En efecto, supongamos que $p \in D$ es primo, es decir $p \notin U(D)$, $p \neq 0$ y $p|ab \Longrightarrow p|a$ o $p|b$. Si $p = ab$ entonces $p|ab$. Luego, $p|a$ o $p|b$. Luego $p = pa'b$ o $p = apb'$. De donde $1 = a'b$ o $1 = ab'$. Entonces $a \in U(D)$ o $b \in U(D)$. Por lo tanto, p es irreducible.

Sin embargo, no siempre es cierto que en todo dominio los irreducibles sean primos. Como contraejemplo, considere el dominio $D = \{a + b\sqrt{5}i \ / \ a, b \in \mathbb{Z}\}$. Considere la norma $||a+bi||^2 = a^2 + 5b^2 \in \mathbb{Z}$. Sabemos que $\alpha \in U(D)$ si, y sólo si $\alpha\cdot\beta = 1$ para algún $\beta \in D$. Luego, $||\alpha\beta||^2 = ||\alpha||^2||\beta||^2 = 1 \Longrightarrow ||\alpha||^2 = 1$. De donde $a = \pm 1$ and $b = 0$. Tenemos $U(D) = \{-1, 1\}$. El elemento 2 es irreducible. En efecto, supongamos que $2 = \alpha\cdot\beta$. Luego $4 = ||\alpha||^2||\beta||^2$, donde $||\alpha||^2 \neq 2$. Tenemos $||\alpha||^2 = 1, 4$ y $||\beta||^2 = 1, 4$. Por otro lado, $2|6 = 2$,

donde $6 = 2 \cdot 3 = (1+\sqrt{5}i)(1-\sqrt{5}i) = 1+5$. Si $2|(1+\sqrt{5}i)$ entonces $1+\sqrt{5}i = 2(a+b\sqrt{5}i) = 2a+2b\sqrt{5}i$ $\Longrightarrow a = \frac{1}{2}$ (contradicción). Entonces $2 \not| (1+\sqrt{5}i)$. De forma similar, $2 \not| (1-\sqrt{5}i)$. Por lo tanto, 2 no es primo.

En $\mathbb{Z}$, los conceptos de "irreducible"y "primo" son equivalentes.

Teorema 3.3.1. En un dominio entero D, $p \in D$ es primo si, y sólo si $\frac{R}{\langle p \rangle}$ es un dominio entero.

Demostración: Tenemos: $ab \in \langle p \rangle \iff p|ab \iff p|a$ o $p|b \iff a \in \langle p \rangle$ o $b \in \langle p \rangle \iff \langle p \rangle$ es primo. $\square$

Lema 3.3.1. Sea D un dominio entero. Entonces:

(1) $s|t \iff \langle t \rangle \subseteq \langle s \rangle$.

(2) $u \in U(D) \iff \langle u \rangle = D$.

(3) $U(D)$ es un grupo abeliano con la multiplicación de D.

3.4 Dominio de factorización única

Definición 3.4.1. Un dominio D se dice **de factorización única** (DFU) si:

(1) Para todo $x \in D\backslash\{0\}$ existen $y_1, \ldots, y_n \in D$ irreducibles y $u \in U(D)$ tales que $x = uy_1 \cdots y_n$.

(2) Si $ux_1 \cdots x_n = vy_1 \cdots y_m$, en donde $u, v \in U(D)$ y $x_1, \ldots, x_n, y_1, \ldots, y_m$ son irreducibles, entonces $n = m$ y existe una permutación σ de $\{1, \ldots, n\}$ tal que $y_i = x_{\sigma(i)}$ para todo $i = 1, \ldots, n$.

Un dominio D se dice ser un UDF' si satisface (1) y

(2)' Todo elemento irreducible en D es primo.

Ejemplo 3.4.1. $D = \{a+b\sqrt{5}i \ / \ a, b \in \mathbb{Z}\}$ no es un DFU, pues $6 = 2 \cdot 3 = (1+\sqrt{5}i) \cdot (1-\sqrt{5}i)$.

Teorema 3.4.1. Sea D un dominio entero. Entonces D es un DFU si, y sólo si, D es un DFU'.

Note que

- y irreducible y $x \sim y \Longrightarrow y$ irreducible.
- y primo y $x \sim y \Longrightarrow x$ primo.
- x, y primos y $y|x \Longrightarrow x \sim y$.

Demostración:

($\Longrightarrow$) Sea $y \in D$ irreducible. Supongamos que $y|ab$. Escribamos $a = ux_1 \cdots x_n$ y $b = vz_1 \cdots z_m$. Sea $q \in D$ tal que $ab = qy$. Tenemos $(ux_1 \cdots x_n)(vz_1 \cdots z_m) = wy_1 \cdots y_k y$. Luego, $y \sim x_j$ o $y \sim z_l$. Luego, $y|a$ o $y|b$.

($\Longleftarrow$) Supongamos $ux_1 \cdots x_n = vy_1 \cdots y_m$. Usamos inducción en n. Si $n = 1$, entonces $ux_1 = vy_1 \cdots y_m$. Tenemos

$$x_1 = (wy_1 \cdots y_{m-1})y_m.$$

Luego, $x_1|vy_1 \cdots y_{m-1}$ o $x_1|y_m$. Si $x_1|y_m$ entonces $x_1 \sim y_m$, $y_m = w'x_1$. Así, $u = vy_1 \cdots y_{m-1}$ es una unidad, por lo que $m - 1 = 0$ y $m = 1$. Si $x_1|(wy_1 \cdots y_{m-1})y_m$ entonces $x_1 \sim y_k$. Se supone cierto que $ux_1 \cdots x_{n-1} = vy_1 \cdots y_m$. Esto implica que $m = n - 1$ y $x_i \sim y_{\sigma(i)}$, para todo $i = 1, \ldots, n$, donde $\sigma \in S_n$. Si $ux_1 \cdots x_{n-1}x_n = vy_1 \cdots y_m$, tenemos

$$x_n|(vy_1 \cdots y_{m-1})y_m \implies x_n|vy_1 \cdots y_{m-1} \text{ o } x_n|y_m.$$

Si $x_n|y_m$ entonces $x_n \sim y_m$. Luego $ux_1 \cdots x_{n-1} = wy_1 \cdots y_{m-1}$. Continuando de esta manera, tenemos que $n = m$. Si $x_n|vy_1 \cdots y_{m-1}$ entonces $x_n \sim y_k$. Nos queda

$$ux_1 \cdots x_{n-1} = wy_1 \cdots y_{k-1}y_{k+1} \cdots y_m.$$

□

Teorema 3.4.2. Todo DIP es un DFU.

Demostración: Probemos que si D es un DIP entonces D es un DFU'.

(1) Supongamos que D no satisface (1), veremos que D no es un DIP. Si D no satisface (1) entonces existe $x \in D\backslash\{0\}$ no factorizable como en (1). En particular, x no es irreducible, es decir $x = y_1z_1$ tal que $y_1, z_1 \notin U(D)$. Al menos uno entre y_1 y z_1 no es factorizable como en (1). Entonces y_1 no es irreducible, por lo que $y_1 = y_2z_2$, donde $y_2, z_2 \notin U(D)$. Al menos y_2 no es factorizable como en (1), y continuamos repitiendo este procedimiento de manera indefinida. Así encontramos una sucesión de elementos en D, x, y_1, y_2, ... Tenemos $x \not| y_1$. En efecto, si $x|y_1$ entonces $x = y_1z_1 = xy_1'z_1$, de donde $y_1'z_1 = 1$ y por tanto $z_1 \in U(D)$. De forma similar, se tiene $y_1 \not| y_2$, $y_2 \not| y_3$, ... Así tenemos la siguiente cadena ascendente no-estacionaria de ideales:

$$\langle x \rangle \subsetneqq \langle y_1 \rangle \subsetneqq \langle y_2 \rangle \subsetneqq \cdots$$

Entonces D no es noetheriano, y por lo tanto no es un DIP.

(2)' Sea $x \in D$ irreducible. Luego, $x \notin U(D)$ y $x \neq 0$. Si $x|ab$, consideramos el ideal $\langle x \rangle + \langle a \rangle = \langle c \rangle$ para algún $c \in D$. Luego $x = cd \implies c \in U(D)$ o $d \in U(D)$. Luego $\langle c \rangle = \langle 1 \rangle = D$ o $\langle x \rangle = \langle a \rangle$. Si se da el primer caso, entonces $1 = px + ta$, para algunos $p, t \in D$. Luego $b = pbx + tab$, de donde $x|b$. Para el segundo caso, tenemos $x|a$.

□

Ejemplo 3.4.2. En $\mathbb{C}[x]$, los irreducibles son los elementos de grado 1. En $\mathbb{R}[x]$, los elementos de grado impar no son irreducibles. Por otro lado, x^4+1 es irreducible en $\mathbb{R}[x]$.

En un DFU se tiene el siguiente algoritmo para calcular el máximo común divisor de dos elementos a y b.

$$\begin{aligned}
b &= aq_0 + r_0,\ r_0 = 0 \text{ o } \delta(r_0) < \delta(a),\\
a &= r_0q_1 + r_1,\ r_1 \text{ o } \delta(r_1) < \delta(r_0),\\
r_0 &= r_1q_2 + r_2,\ r_2 = 0 \text{ o } \delta(r_2) < \delta(r_1),\\
&\vdots\\
r_{k-2} &= r_{k-1}q_k + r_k,\ r_k = 0 \text{ o } \delta(r_k) < \delta(r_{k-1}),\\
r_{k-1} &= r_kq_{k+1} + r_{k+1},\ r_{k+1} = 0.
\end{aligned}$$

Tenemos $r_k|r_{k-1}$, $r_k|r_{k-2}$, $\ldots$, $r_k|r_2$, $r_k|r_1$, $r_k|r_0$, $r_k|a$, $r_k|b$. Por otro lado, note que si $d|a$ y $d|b$ entonces $d|r_0 \Longrightarrow d|r_1 \Longrightarrow \cdots \Longrightarrow d|r_k$. Por lo tanto, $r_k = (a,b)$.

Ejemplo 3.4.3. Dados $p(x) = x^4-3x^2+x-1$ y $q(x) = x^2+2x+1$, tenemos $p(x) = (x^2-2x)q(x)+(3x-1)$. Note que $(p(x), q(x)) = 1$.

Ejemplo 3.4.4. En $\mathbb{Z}$, tenemos $(28, 15) = 1$.

CAPÍTULO 4

MÓDULOS DE FRACCIONES

4.1 Conjuntos multiplicativamente cerrados

Sea S un subconjunto de un anillo A. Decimos que S es **multiplicativamente cerrado** si:

(1) $1 \in S$.

(2) Para cualesquiera $a, b \in S$, se tiene $ab \in S$.

Se define la relación $\equiv \subseteq A \times S$ de la siguiente manera:

$$(a, s) \equiv (b, t) \iff \text{existe } u \in S \text{ tal que } u(at - bs) = 0.$$

Veamos que $\equiv$ es una relación de equivalencia:

(a) $\equiv$ es reflexiva: Sea $a \in A$ y $s \in S$. De $1(as - as) = 0$ se sigue $(a, s) \equiv (a, s)$.

(b) $\equiv$ es simétrica: Si $(a, s) \equiv (b, t)$ entonces existe $u \in S$ tal que $u(at - bs) = 0$. De donde $u(bs - at) = 0$, es decir $(b, t) \equiv (a, s)$.

(c) $\equiv$ es transitiva: Si $(a, s) \equiv (b, t)$ y $(b, t) \equiv (c, q)$ entonces existen $u, v \in S$ tales que

$$u(at - bs) = 0 \ (1),$$
$$v(bq - ct) = 0 \ (2).$$

Luego,

$$(1) \times qv: \ uqvat = uqvbs,$$
$$(2) \times su: \ vsubq = vsuct.$$

Entonces,

$$uqvat = vsuct$$
$$(uvt)(aq) = (uvt)(cs)$$
$$uvt(aq - cs) = 0, \text{ donde } uvt \in S.$$

Entonces, $(a, s) \equiv (c, q)$.

Denotamos

$$S^{-1}A := \frac{A \times S}{\equiv}.$$

El conjunto $S^{-1}A$ de denomina **anillo de fracciones de** A. La clase de (a, s) la denotaremos por $\overline{(a, s)} := \frac{a}{s}$.
Para todo $t \in S$ tenemos $\frac{a}{s} = \frac{at}{st}$, pues $1(ast - ats) = 0$.
Se definen las siguientes operaciones:

$$+ : S^{-1}A \times S^{-1}A \longrightarrow S^{-1}A \qquad \left(\frac{a}{s}, \frac{b}{t}\right) \mapsto \frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st},$$
$$\cdot : S^{-1} \times S^{-1}A \longrightarrow S^{-1}A \qquad \left(\frac{a}{s}, \frac{b}{t}\right) \mapsto \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}.$$

Veamos que estas operaciones están bien definidas. Supongamos que $\frac{a}{s} = \frac{a'}{s'}$ y $\frac{b}{t} = \frac{b'}{t'}$. Entonces existen $u, v \in S$ tales que:

$$uas' = ua's \ (1),$$
$$vbt' = vb't \ (2).$$

Tenemos:

$$(1) \times vtt' : \ uvatt's' = uva'tt's,$$
$$(2) \times uss' : \ uvbss't' = uvb'ss't.$$

Sumando las expresiones anteriores, tenemos:

$$uvs't'(at + bs) = uvst(a't' + b's')$$
$$uv[(at + bs)s't'] = uv[(a't' + b's')], \text{ donde } uv \in S.$$

Se sigue que la suma está bien definida. De manera similar, se puede ver que

$$(uv)(abs't') = (uv)(a'b'st).$$

Se sigue que el producto está bien definido. Con estas operaciones, $S^{-1}A$ deviene en un anillo. El elemento neutro con respecto a la suma viene dado por $0_{S^{-1}A} = \frac{0_A}{s}$, para cualquier $s \in S$. En efecto:

$$\frac{a}{t} + \frac{0_A}{s} = \frac{as}{ts} = \frac{a}{t}.$$

El elemento identidad de la multiplicación viene dado por $1_{S^{-1}A} = \frac{s}{s}$, para cualquier $s \in S \backslash \{0\}$. En efecto:

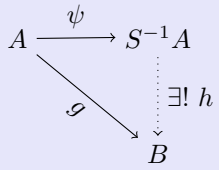
$$\frac{s}{s} \cdot \frac{a}{t} = \frac{as}{st} = \frac{a}{t}.$$

Dado $\frac{a}{s} \in S^{-1}A$, su inverso respecto a la suma está dado por $-\left(\frac{a}{s}\right) = \frac{-a}{s}$. Se tiene

$$\frac{a}{s} + \frac{-a}{s} = \frac{as - as}{s^2} = \frac{0}{s^2} = 0_{S^{-1}A}.$$

Si $-s \in S$, entonces podemos escribir $-\frac{a}{s} = \frac{a}{-s}$. Si $A = D$ es un dominio y $S = D\backslash\{0\}$, entonces $K = S^{-1}D$ es el cuerpo de fracciones. Considere el homomorfismo de anillos $\psi : A \longrightarrow S^{-1}A$ dado por $a \mapsto \frac{a}{1}$. Si A no tiene divisores de cero, entonces ψ is inyectivo. En efecto, si $\psi(a) = 0$ entonces $\frac{a}{1} = \frac{0}{1}$. De donde existe $u \in S\backslash\{0\}$ tal que $u \cdot a = 0$. Como S no tiene divisores de cero, nos queda $a = 0$.

Proposición 4.1.1 (Propiedad universal)**.** Sean A un anillo, S un subconjunto multiplicativamente cerrado de A, y B otro anillo. Si $g : A \longrightarrow B$ es un homomorfismo de anillos tal que para todo $s \in S$, $g(s) \in U(B)$, entonces existe un único homomorfismo de anillos $h : A \longrightarrow B$ tal que $g = h \circ \psi$, donde $\psi : A \longrightarrow S^{-1}A$ es el homomorfismo $a \mapsto \frac{a}{1}$.



Demostración: Definamos $h : S^{-1}A \longrightarrow B$ por $h\left(\frac{a}{s}\right) = g(a) \cdot (g(s))^{-1}$. Primero veamos que h está bien definida. Supongamos que $\frac{a}{s} = \frac{a'}{s'}$. Luego existe $u \in S$ tal que $uas' = ua's$. Tenemos

$$\begin{aligned} g(uas') &= g(ua's) \\ g(u) \cdot g(a) \cdot (g(s))^{-1} &= g(u) \cdot g(a') \cdot (g(s'))^{-1} \\ g(a) \cdot (g(s))^{-1} &= g(a') \cdot (g(s'))^{-1}, \text{ porque } g(u) \text{ es una unidad de } B. \end{aligned}$$

Por lo tanto, h está bien definida. El fácil ver que h es un homomorfismo de anillos. Además,

$$(h \circ \psi)(a) = h\left(\frac{a}{1}\right) = g(a) \cdot (g(1))^{-1} = g(a).$$

Falta ver que h es el único homomorfismo de anillos $S^{-1}A \longrightarrow B$ que satisface $h \circ \psi = g$. Supongamos que $h' : S^{-1}A \longrightarrow B$ es otro homomorfismo de anillos tal que $h' \circ \psi = g$. Tenemos

$$\begin{aligned} h'\left(\frac{a}{1}\right) &= h' \circ \psi(a) = g(a) = h \circ \psi(a) = h\left(\frac{a}{1}\right), \\ h'\left(\frac{1}{s}\right) &= h'\left(\left(\frac{s}{1}\right)^{-1}\right) = \left(h'\left(\frac{s}{1}\right)\right)^{-1} = \left(h\left(\frac{s}{1}\right)\right)^{-1} = h\left(\frac{1}{s}\right), \\ h'\left(\frac{a}{s}\right) &= h'\left(\frac{a}{1} \cdot \frac{1}{s}\right) = h'\left(\frac{a}{1}\right) \cdot h'\left(\frac{1}{s}\right) = h\left(\frac{a}{1}\right) \cdot h\left(\frac{1}{s}\right) = h\left(\frac{a}{s}\right). \end{aligned}$$

□

Proposición 4.1.2 (Propiedades)**.**

(1) $s \in S \Longrightarrow \psi(s) \in U(S^{-1}A)$.

(2) $\psi(a) = 0 \Longrightarrow$ existe $s \in S$ tal que $s \cdot a = 0$.

(3) Para todo $\frac{a}{s} \in S^{-1}A$, $\frac{a}{s} = \psi(a) \cdot (\psi(s))^{-1}$.

Corolario 4.1.1. Si $g : A \longrightarrow B$ es un homomorfismo de anillos que satisface:

(1) para todo $s \in S$, $g(s) \in U(B)$;

(2) $g(a) = 0 \Longrightarrow$ existe $s \in S$ tal que $s \cdot a = 0$;

(3) para todo $b \in B$, existe $a \in A$ y $s \in S$ tal que $b = g(a) \cdot (g(s))^{-1}$;

entonces existe un único isomomorfismo de anillos $h : S^{-1}A \longrightarrow B$ tal que $g = h \circ \psi$.

Demostración: Por la propiedad universal, existe un único homomorfismo de anillos $h : S^{-1}A \longrightarrow B$ tal que $g = h \circ \psi$. Veamos que h es un isomorfismo. Sea $\frac{a}{s} \in \text{Ker}(h)$. Tenemos

$$0 = h\left(\frac{a}{s}\right) = h\left(\frac{a}{1}\right) \cdot h\left(\frac{1}{s}\right) = h\left(\frac{a}{1}\right) \cdot \left(h\left(\frac{1}{s}\right)\right)^{-1} = g(a) \cdot (g(s))^{-1}.$$

Luego $g(a) = 0$. Por (2), existe $s' \in S$ tal que $s' \cdot a = 0$. Así tenemos

$$\frac{a}{s} = \frac{s'a}{s's} = \frac{0}{s's} = 0_{S^{-1}A}.$$

Por lo tanto, h es inyectivo. Ahora sea $b \in B$. Por (3), existen $a \in A$ y $s \in S$ tales que $b = g(a) \cdot (g(s))^{-1}$. Tenemos

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

Por lo tanto, h es sobreyectivo. □

4.2 Módulos de fracciones

Sean A un anillo, S un subconjunto de A multiplicativamente cerrado, y M un A-módulo. En $M \times S$ se define la siguiente relación $\equiv \subseteq (M \times S) \times (M \times S)$:

$$(m, s) \equiv (m', s') \iff \text{si, y sólo si existe } u \in S \text{ tal que } u(s'm - sm') = 0.$$

Así como se hizo en el capítulo anterior, se puede demostrar que $\equiv$ es una relación de equivalencia. Denotamos el conjunto cociente de $M \times S$ por esta relación como

$$S^{-1}M := \frac{M \times S}{\equiv}.$$

En $S^{-1}M$, denotamos la clase del elemento (m, s) por $\overline{(m, s)} := \frac{m}{s}$. Note que para todo $\frac{m}{s} \in S^{-1}M$ y todo $t \in S$, se tiene $\frac{m}{s} = \frac{tm}{ts}$, pues $1 \cdot (stm - tsm) = 0$. Se definen las siguientes operaciones:

$$+ : S^{-1}M \times S^{-1}M \longrightarrow S^{-1}M \qquad \left(\frac{m}{s}, \frac{m'}{s'}\right) \mapsto \frac{s'm + sm'}{ss'},$$
$$\cdot : S^{-1}A \times S^{-1}M \longrightarrow S^{-1}M \qquad \left(\frac{a}{s}, \frac{m}{t}\right) \mapsto \frac{am}{st}.$$

Así como se hizo en el capítulo anterior, se puede probar que estas operaciones están bien definidas. El conjunto $S^{-1}M$ deviene en un $S^{-1}A$-módulo con estas operaciones, al cual denominaremos **módulo de**

fracciones de M. El elemento neutro viene dado por $0_{S^{-1}M} = \frac{0_M}{s}$, para cualquier $s \in S$ no nulo. En efecto,

$$\frac{m}{t} + \frac{0_M}{s} = \frac{sm}{st} = \frac{m}{t}.$$

Para cada $\frac{m}{t}$, su elemento inverso respecto a la suma viene dado por $\frac{-m}{t}$.

Si P es un ideal primo, entonces $S = A \backslash P$ es un conjunto multiplicativamente cerrado. En este caso, denotaremos $S^{-1}A$ por A_P y a $S^{-1}M$ por M_P. Para $f \in A$, $\{f^n \ / \ n \in \mathbb{N} \cup \{0\}\}$ es un conjunto multiplicativamente cerrado, donde $f^0 = 1$. En este caso, denotaremos a $S^{-1}A$ por A_f y a $S^{-1}M$ por M_f.

Sea A un anillo, S un subconjunto de A multiplicativamente cerrado, M y N A-módulos, y $g : M \longrightarrow N$ un homomorfismo de A-módulos. Se define $S^{-1}(g) : S^{-1}M \longrightarrow S^{-1}N$ como

$$S^{-1}(g)\left(\frac{m}{s}\right) := \frac{g(m)}{s}, \text{ para todo } \frac{m}{s} \in S^{-1}M.$$

Veamos que $S^{-1}(g)$ está bien definido. Supongamos que $\frac{m}{s} = \frac{m'}{s'}$. Entonces existe $u \in S$ tal que $us'm = usm'$. De donde

$$\begin{aligned} g(us'm) &= g(usm') \\ us'g(m) &= usg(m') \\ &\Longrightarrow \\ \frac{g(m)}{s} &= \frac{g(m')}{s'}. \end{aligned}$$

Ahora veamos que $S^{-1}(g)$ es un homomorfismo de $S^{-1}A$-módulos.

$$\begin{aligned} S^{-1}(g)\left(\frac{m}{s} + \frac{m'}{s'}\right) &= S^{-1}(g)\left(\frac{s'm + sm'}{ss'}\right) = \frac{g(s'm) + g(sm')}{ss'} = \frac{s'g(m)}{ss'} + \frac{sg(m')}{ss'} = \frac{g(m)}{s} + \frac{g(m')}{s'} \\ &= S^{-1}(g)\left(\frac{m}{s}\right) + S^{-1}(g)\left(\frac{m'}{s'}\right), \\ S^{-1}(g)\left(\frac{a}{t} \cdot \frac{m}{s}\right) &= S^{-1}(g)\left(\frac{am}{ts}\right) = \frac{g(am)}{ts} = \frac{a}{t} \cdot \frac{g(m)}{s} = \frac{a}{t} \cdot S^{-1}(g)\left(\frac{m}{s}\right). \end{aligned}$$

Proposición 4.2.1. Sea $M' \xrightarrow{f} M \xrightarrow{g} M''$ una sucesión exacta de A-módulos y de homomorfismos de A-módulos. Entonces la sucesión

$$S^{-1}M' \xrightarrow{S^{-1}(f)} S^{-1}M \xrightarrow{S^{-1}(g)} S^{-1}M''$$

es exacta.

Demostración: Sabemos que $\mathrm{Im}(f) = \mathrm{Ker}(g)$. Hay que ver que $\mathrm{Im}(S^{-1}(f)) = \mathrm{Ker}(S^{-1}(g))$. Sea $S^{-1}(f)\left(\frac{m'}{s}\right) = \frac{f(m')}{s} \in \mathrm{Im}(S^{-1}(f))$. Tenemos $f(m') \in \mathrm{Im}(f) = \mathrm{Ker}(g)$. Tenemos

$$S^{-1}(g)\left(\frac{f(m')}{s}\right) = \frac{g \circ f(m')}{s} = \frac{0}{s} = 0.$$

Entonces, $\mathrm{Im}(S^{-1}(f)) \subseteq \mathrm{Ker}(S^{-1}(g))$. Ahora supongamos que $\frac{m}{s} \in \mathrm{Ker}(S^{-1}(g))$. Entonces

$$S^{-1}(g)\left(\frac{m}{s}\right) = \frac{g(m)}{s} = 0_{S^{-1}M''} = \frac{0_{M''}}{1}.$$

De donde existe $u \in S$ tal que $u \cdot g(m) = 0_{M''}$. Luego, $g(um) = 0_{M''}$. Tenemos $um \in \mathrm{Ker}(g) = \mathrm{Im}(f)$. Así, existe $m' \in M'$ tal que $f(m') = um$. Entonces,

$$\frac{m}{s} = \frac{um}{us} = S^{-1}(f)\left(\frac{m'}{us}\right) \in \mathrm{Im}(S^{-1}(f)).$$

□

Corolario 4.2.1. Si N es un submódulo de M entonces $S^{-1}N$ es isomorfo a un submódulo de $S^{-1}M$.

Demostración: La sucesión $0 \longrightarrow N \overset{i}{\hookrightarrow} M$ es exacta. Por lo tanto,

$$\langle 0 \rangle = S^{-1}0 \overset{S^{-1}(0)=0}{\longrightarrow} S^{-1}N \overset{S^{-1}(i)}{\longrightarrow} S^{-1}M$$

es exacta. Se sigue que $S^{-1}(i)$ es inyectivo, y por ende $S^{-1}N \cong \mathrm{Im}(S^{-1}(i)) \subseteq S^{-1}M$.

□

Proposición 4.2.2. Si N y P son submódulos de M entonces

(1) $S^{-1}N + S^{-1}P = S^{-1}(N + P)$.

(2) $S^{-1}(N \cap P) = S^{-1}N \cap S^{-1}P$.

(3) $S^{-1}\left(\frac{M}{N}\right) \cong \frac{S^{-1}M}{S^{-1}N}$.

Demostración:

(1) Tenemos $S^{-1}N + S^{-1}P \ni \frac{n}{s} + \frac{p}{t} = \frac{tn+sp}{st} \in S^{-1}(N + P)$. Ahora sea $\frac{n+p}{s} \in S^{-1}(N + P)$. Tenemos

$$\frac{n+p}{s} = \frac{s(n+p)}{s^2} = \frac{sn+sp}{s^2} = \frac{n}{s} + \frac{p}{s} \in S^{-1}N + S^{-1}P.$$

(2) Sea $\frac{x}{s} \in S^{-1}(N \cap P)$. Tenemos $x \in N \cap P$. De donde $\frac{x}{s} \in S^{-1}N$ y $\frac{x}{s} \in S^{-1}P$. Ahora sea $\alpha \in S^{-1}N \cap S^{-1}P$. Luego, existen $n \in N$, $p \in P$ y $s, t \in S$ tales que $\alpha = \frac{n}{s}$ y $\alpha = \frac{p}{t}$. Se sigue que existe $u \in S$ tal que $utn = usp \in N \cap P$. Por lo tanto, $\frac{n}{s} = \frac{utn}{uts} \in S^{-1}(N \cap P)$.

(3) Considere la sucesión exacta $M \overset{\pi}{\longrightarrow} \frac{M}{N} \longrightarrow 0$. Luego tenemos que la sucesión

$$S^{-1}M \overset{S^{-1}(\pi)}{\longrightarrow} S^{-1}\left(\frac{M}{N}\right) \overset{S^{-1}(0)}{\longrightarrow} S^{-1}(0)$$

es también exacta. De donde $S^{-1}(\pi) : S^{-1}M \longrightarrow S^{-1}\left(\frac{M}{N}\right)$ es sobreyectivo. Ahora vamos a ver que $\mathrm{Ker}(S^{-1}(\pi)) = S^{-1}N$. Si $\frac{n}{s} \in S^{-1}N$ entonces $S^{-1}(\pi)\left(\frac{n}{s}\right) = \frac{\pi(n)}{s} = \frac{0_{M/N}}{s} = 0_{S^{-1}\left(\frac{M}{N}\right)}$. Si $\frac{m}{s} \in \mathrm{Ker}(S^{-1}(\pi))$ entonces $0 = \frac{\overline{0}}{1} = S^{-1}(\pi)\left(\frac{m}{s}\right) = \frac{\pi(m)}{s} = \frac{\overline{m}}{s}$. De donde existe $u \in S$ tal que $u\overline{m} = \overline{0}$. Luego, $um \in N$. Entonces, $\frac{m}{s} = \frac{um}{us} \in S^{-1}N$. Por lo tanto,

$$\frac{S^{-1}M}{S^{-1}N} = \frac{S^{-1}M}{\mathrm{Ker}(S^{-1}(\pi))} \cong \mathrm{Im}(S^{-1}(\pi)) = S^{-1}\left(\frac{M}{N}\right).$$

□

El anillo $S^{-1}A$ es un A-módulo con la misma suma y con el producto dado por

$$a \cdot \frac{b}{s} = \frac{ab}{s}.$$

Si M es un A-módulo, entonces $S^{-1}M$ también es un A-módulo con la misma suma, pero con el producto dado por

$$a \cdot \frac{m}{s} = \frac{am}{s}.$$

Ejercicio 4.2.1. Sean A un anillo, S un subconjunto de A multiplicativamente cerrado, y M un A-módulo. Entonces, como A-módulo, se tiene $S^{-1}A \otimes_A M \cong S^{-1}M$.

CAPÍTULO 5

DESCOMPOSICIÓN PRIMARIA

5.1 Ideales primarios y P-primarios

Definición 5.1.1. Un ideal Q de un anillo A ($Q \subsetneq A$) se dice **primario** si siempre que $xy \in Q$, entonces $x \in Q$ o existe $n \in \mathbb{N}$ tal que $y^n \in Q$. Esto equivale a decir que $\frac{A}{Q} \neq 0$ y que todo divisor de cero de $\frac{A}{Q}$ es nilpotente.

Sea $f : A \longrightarrow B$ un homomorfismo de anillos e I un ideal de B, entonces $f^{-1}(I) = \{x \in A \ / \ f(x) \in I\}$ es un ideal de A. Si $J \subseteq A$ es un ideal de A, $f(J)$ no tiene por qué ser un ideal de B. Por ejemplo, considere la inclusión $i : \mathbb{Z} \longrightarrow \mathbb{Q}$ y el ideal $J = \langle 2 \rangle$. En este caso $i(J) = J$ no es un ideal de $\mathbb{Q}$.

La **extensión de** J **en** B es el ideal generado por $f(J)$, es decir

$$\langle f(J) \rangle = \left\{ \sum_{i=1}^{n} b_i f(x_i) \ / \ b_i \in B, \ x_i \in J, \ n \in \mathbb{N} \right\}.$$

Sea $f : A \longrightarrow B$ un homomorfismo de anillos. Si Q es un ideal primario de B, entonces su contracción $f^{-1}(Q)$ es un ideal primario de A. En efecto,

$$\begin{aligned} xy \in f^{-1}(Q) &\Longrightarrow f(x)f(y) \in Q \\ &\Longrightarrow f(x) \in Q \text{ o existe } n \in \mathbb{N} \text{ tal que } f^n(y) \in Q \\ &\Longrightarrow f(x) \in Q \text{ o existe } n \in \mathbb{N} \text{ tal que } f(y^n) \in Q \\ &\Longrightarrow x \in f^{-1}(Q) \text{ o existe } n \in \mathbb{N} \text{ tal que } y^n \in f^{-1}(Q). \end{aligned}$$

Si I es un ideal de A, el **radical** de I es el conjunto $r(I) := \{x \in A \ / \ x^n \in I, \text{ para algún } n \in \mathbb{N}\}$.

Proposición 5.1.1. Si Q es un ideal primario de un anillo A, entonces su radical $r(Q)$ es el menor ideal primo que contiene a Q.

Demostración: Supongamos que $xy \in r(Q)$. Entonces existe $n \in \mathbb{N}$ tal que $x^n y^n \in Q$. Como Q es primario, se tiene que $x^n \in Q$ o que existe $m \in \mathbb{N}$ tal que $y^{nm} \in Q$. De donde $x \in r(Q)$ o $y \in r(Q)$.

Ahora, consideremos un ideal primo P que contiene a Q. Entonces para todo $x \in r(Q)$ existe $n \in \mathbb{N}$ tal que $x^n \in Q \subseteq P$. Como P es primo, se tiene que $x \in P$.

□

Definición 5.1.2. Si $P = r(Q)$ para algún ideal primo P, entonces Q se dice P-primario.

Ejemplo 5.1.1.

(1) P primo $\Longrightarrow$ P primario.

(2) $Q = \langle x, y^2 \rangle$ en $\mathbb{K}[x, y]$, donde $\mathbb{K}$ es un cuerpo, es un ideal primario.

Ejercicio 5.1.1. Probar que los ideales primarios de $\mathbb{Z}$ son $\langle 0 \rangle$ y $\langle p^n \rangle$, donde n es cualquier natural y p cualquier número primo.

Proposición 5.1.2. Sea I un ideal de A. Si $r(I)$ es un ideal maximal de A, entonces I es primario.

Demostración: Primero veamos que las potencias de un ideal maximal $\mathcal{M}$ son ideales $\mathcal{M}$-primarios. Sea $\mathcal{M}$ un ideal maximal y consideremos $n \in \mathbb{N}$. Veamos que $r(\mathcal{M}^n) = \mathcal{M}$. Es claro que $\mathcal{M} \subseteq r(\mathcal{M}^n)$. Ahora sea $x \in r(\mathcal{M}^n)$. Entonces $x^k \in \mathcal{M}^n \subseteq \mathcal{M}$, para algún $k \in \mathbb{N}$. Como todo ideal maximal es primo, se tiene que $x \in \mathcal{M}$. Para ver que $\mathcal{M}^n$ es $\mathcal{M}$-primario, falta ver que $\mathcal{M}^n$ es primario. Supongamos que $xy \in \mathcal{M}^n$. Supongamos también que $x \notin \mathcal{M}^n$ y $y \notin r(\mathcal{M}^n)$. Luego existe $r \in r(\mathcal{M}^n)$ y $a \in A$ tales que $1 = r + ay$. Sea $m \in \mathcal{M}$ un entero positivo tal que $r^m \in \mathcal{M}^n$. Tenemos $1 = 1^m = r^m + p(r, ay) + a^m y^m$. Como $r \in r(\mathcal{M}^n) = \mathcal{M}$, se tiene $p(r, ay) \in \mathcal{M}$, y así $r^m + p(r, ay) \in \mathcal{M}^n$. Ahora tenemos $x = r^m x + xp(r, ay) + a^m y^m x \in \mathcal{M}^n$, porque $x(r^m + p(r, ay)) \in \mathcal{M}^n$ y $xy^m \in \mathcal{M}^n$. De donde $x \in \mathcal{M}^n$, obteniendo así una contradicción. Por lo tanto, $\mathcal{M}^n$ es $\mathcal{M}$-primario.

Supongamos que $xy \in I$, $x \notin I$, y que $y \notin r(I)$. Como $r(I)$ es maximal, tenemos que $r(I) + \langle y \rangle = \langle 1 \rangle$. Luego existe $r \in r(I)$ y $a \in A$ tal que $1 = r + ay$. Sea $n \in \mathbb{N}$ tal que $r^n \in I$. Nos queda $x = xr^n + xp(r, ay) + a^n xy^n$, donde $r^n \in I$, $p(r, ay) \in r(I) = I$, y $xy^n \in I$. Se sigue $x \in I$, obteniendo así una contradicción. □

5.2 Teoremas de unicidad

Lema 5.2.1. $r\left(\bigcap_{i=1}^n I_i\right) = \bigcap_{i=1}^n r(I_i)$.

Demostración: Sea $x \in r\left(\bigcap_{i=1}^n I_i\right)$. Luego existe $m \in \mathbb{N}$ tal que $x^m \in \bigcap_{i=1}^n I_i$. De donde $x^m \in I_i$, para todo $1 \leq i \leq n$, es decir, $x \in r(I_i)$ para todo $1 \leq i \leq n$. Ahora sea $x \in \bigcap_{i=1}^n r(I_i)$. Para cada $1 \leq i \leq n$, se tiene que existe $m_i \in \mathbb{N}$ tal que $x^{m_i} \in I_i$. Sea m el mínimo común múltiplo de $m_1, \ldots, m_n$. Entonces $x^m \in I_i$, para todo $1 \leq i \leq n$, es decir $x^m \in \bigcap_{i=1}^n I_i$. □

Lema 5.2.2. Si $I_1, \ldots, I_n$ son ideales P-primarios en A, entonces $I = \bigcap_{i=1}^{n} I_i$ es P-primario.

Demostración: Primero, notamos que $r(I) = \bigcap_{i=1}^{n} r(I_i) = \bigcap_{i=1}^{n} P = P$, por el lema anterior. Ahora veamos que I es primario. Supongamos que $xy \in I$. Luego, $xy \in I_i$, para cada $1 \leq i \leq n$. Supongamos que $x \notin I$. Luego existe $1 \leq i \leq n$ tal que $x \notin I_i$. Por otro lado, $xy \in I_i$. De donde existe $n_i \in \mathbb{N}$ tal que $y^{n_i} \in I_i$, es decir $y \in r(I_i) = P = r(I)$. □

Lema 5.2.3. Si I es un ideal P-primario y $x \in A$, entonces:

(1) $x \in I \Longrightarrow (I : x) = \langle 1 \rangle = A$.

(2) $x \notin I \Longrightarrow (I : x)$ es P-primario ($r(I : x) = P$).

(3) $x \notin P \Longrightarrow (I : x) = I$ y $r(I : x)$.

Demostración:

(1) Si $x \in I$ entonces para todo $a \in A$, $ax \in I \Longrightarrow a \in (I : x)$.

(2) Supongamos que $x \notin I$. Veamos primero que $r(I : x) = P$. Para todo $p \in P$, existe $n \in \mathbb{N}$ tal que $p^n \in I$. Luego, $p^n x \in I$, es decir $p^n \in (I : x) \subseteq r(I : x)$. Ahora sea $y \in r(I : x)$. Luego existe $m \in \mathbb{N}$ tal que $y^m \in (I : x)$. De donde $y^m x \in I$. Como I es primario y $x \notin I$, se tiene que existe $k \in \mathbb{N}$ tal que $y^{km} \in I$. Luego, $y \in r(I) = P$.

Ahora veamos que $(I : x)$ es primario. Supongamos $yz \in (I : x)$. Entonces $xyz \in I$. Como $x \notin I$ e I es primario, se tiene que existe $n \in \mathbb{N}$ tal que $y^n z^n \in I$, es decir $yz \in r(I) = P = r(I : x)$. Supongamos que $z \notin r(I : x) \supseteq (I : x)$. Como $z \notin r(I)$ y $(xy)z \in I$, se tiene $xy \in I$ ($y \in (I : x)$) porque I es primario.

(3) Supongamos que $x \notin P$. Es claro que $I \subseteq (I : x)$. Sea $y \in (I : x)$. Luego $xy \in I$. Como $x \notin P = r(I)$, se sigue $y \in I$, porque I es primario. Por lo tanto, $(I : x) = I$. De esto se tiene que $r(I : x) = r(I) = P$.

□

Definición 5.2.1. Sea I un ideal de A tal que $I = \bigcup_{i=1}^{n} I_i$, donde cada I_i es un ideal primario. Si además,

(1) $r(I_i) \neq r(I_j)$ para todo $i \neq j$, y

(2) para todo j, $\bigcap_{i \neq j} I_i \not\subseteq I_j$,

entonces diremos que la descomposición $I = \bigcap_{i=1}^{n} I_i$ es **minimal**. Los ideales primos $P_1, \ldots, P_n$ (donde $P_i = r(I_i)$) se denominan **ideales primos mínimos** de I.

Teorema 5.2.1 (Primer Teorema de Unicidad)**.** Sea I un ideal de A e $I = \bigcap_{i=1}^{n} I_i$ una descomposición primaria minimal de I, donde $r(I_i) = P_i$.

(1) Si $r(I : x)$ es primo, entonces existe $1 \leq i \leq n$ tal que $r(I : x) = P_i$.

(2) Para todo $1 \leq i \leq n$, existe $x_i \in A$ tal que $r(I : x_i) = P_i$.

Demostración:

(1) Sea $P = r(I : x)$, que es un ideal primo que contiene a I. Entonces, $I = \bigcap_{i=1}^{n+1} I_i$ donde $I_{n+1} = P$. Además, $r(I) = (\bigcap_{i=1}^{n} P_i) \cap P$ y $P = r(I : x) = r\left((\bigcap_{i=1}^{n} I_i) : x\right) = \bigcap_{i=1}^{n} r(I_i : x)$. Si $x \notin I_i$ entonces $r(I_i : x) = P_i$. Si $x \in I_i$, entonces $r(I_i : x) = A$. Así tenemos

$$P = \left(\bigcap_{i=1,\ x \in I_i}^{k} A \right) \cap \left(\bigcap_{i=k+1,\ x \notin I_i}^{n} P_i \right) = \bigcap_{i=k+1}^{n} P_i.$$

Es claro que para todo i, $P \subseteq P_i$. Si $P_{k+1} \not\subseteq P$ entonces existe $p_{k+1} \in P_{k+1} - P$. Tenga en cuenta que $\prod_{i=k+1}^{n} P_i \subseteq \bigcap_{i=k+1}^{n} P_i \subseteq P$. Luego para todo $p_{k+2} \in P_{k+2}, \ldots, p_n \in P_n$, se tiene $p_{k+1}(p_{k+2} \cdots p_n) \in P$, de donde $p_{k+2} \cdots p_n \in P$. Si $P_{k+2} \not\subseteq P$ entonces existe $p_{k+2} \in P_{k+2} - P$. Luego para todo $p_{k+3} \in P_{k+3}, \ldots, p_n \in P_n$, tenemos $p_{k+2}(p_{k+3} \cdots p_n) \in P$. Como $p_{k+2} \notin P$, nos queda $p_{k+3} \cdots p_n \in P$. Seguimos descartando si es necesario, pero como $\prod_{i=k+1}^{n} P_i \subseteq P$, en algún momento hallaremos $k+1 \leq l \leq n$ tal que $P_l \subseteq P$. Luego, $P = P_l$, de donde $P_l = P = r(I : x)$.

(2) Fijemos i entre 1 y n. Sabemos que $I_i \not\supseteq \bigcap_{j \neq i} I_j$. Luego existe $x \in \bigcap_{j \neq i} I_j$ tal que $x \notin I_i$. Luego, $(I : x) = \bigcap_{j \neq i} (I_j : x) \cap (I_i : x)$, donde $(I_j : x) = A$. Así, $(I : x) = (I_i : x)$. De donde $r(I : x) = r(I_i : x) = P_i$.

□

Proposición 5.2.1. Sea I un ideal **descomponible**, es decir que I posee una descomposición primaria minimal $I = \bigcap_{i=1}^{n} I_i$. Sea $P_i = r(I_i)$, para cada $1 \leq i \leq n$. Si P es un ideal primo e $I \subseteq P$, entonces existe $1 \leq k \leq n$ tal que $I_k \subseteq P$.

Demostración: Si $I = \bigcap_{i=1}^{n} I_i \subseteq P$, entonces $I = \bigcap_{i=1}^{n+1} I_i$, donde $I_{n+1} = P$. Tenemos

$$\bigcap_{i=1}^{n} P_i = r\left(\bigcap_{i=1}^{n} I_i \right) = r(I) = r\left(\bigcap_{i=1}^{n} I_i \right) \cap r(P) = r\left(\bigcap_{i=1}^{n} I_i \right) \cap P \subseteq P.$$

Y como $\prod_{i=1}^{n} P_i \subseteq \bigcap_{i=1}^{n} P_i$, se tiene que existe $k = 1, \ldots, n$ tal que $P_k \subseteq P$. □

Proposición 5.2.2. Sea $I = \bigcap_{i=1}^{n} I_i$ una descomposición primaria minimal de I, con $P_i = r(I_i)$. Entonces $\bigcup_{i=1}^{n} P_i = \{x \in A \ / \ (I : x) \neq I\}$.

Demostración: Supongamos $x \notin \bigcup P_i \Longrightarrow x \notin P_i$ para todo i. Entonces $(I_i : x) = I_i$ para todo i. Tenemos $I = \bigcap_{i=1}^{n}(I_i : x) = (\bigcap_{i=1}^{n} I_i : x) = (I : x)$. Lo cual implica que $x \notin \{x \in A \,/\, (I : x) \neq I\}$. Para ver que $\bigcup_{i=1}^{n} P_i \subseteq \{x \in A \,/\, (I : x) \neq I\}$, usaremos indiccuón en n. Para $n = 1$, $r(I) = P$. Luego $x \in P$ implica $(I : x) = A$ si $x \in I$. Si $x \in P \backslash I$ entonces $(I : x)$ es P-primario. Así $I \neq P = (I : x)$. Supongamos que el resultado se cumple para $n - 1$. Sea $I = \bigcap_{i=1}^{n} I_i$ con $r(I_i) = P_i$. Sea $I' = \bigcap_{i=1}^{n-1} I_i$. Note que $\bigcap_{i\neq j}^{n-1} I_i \not\subseteq I_j$ y $r(I_i) \neq r(I_j)$. Tenemos $(I' : x) \supsetneqq I'$. Así,

$$\begin{aligned}(I : x) &= \left(\bigcap_{i=1}^{n} I_i : x\right) = \bigcap_{i=1}^{n}(I_i : x) \\ &= \bigcap_{i=1}^{n-1}(I_i : x) \cap (I_n : x) = \left(\bigcap_{i=1}^{n-1} I_i : x\right) \cap (I_n : x) \\ &= (I' : x) \cap (I_n : x) \supsetneqq I' \cap I_n = I.\end{aligned}$$

□

Si $\langle 0\rangle$ es descomponible, entonces $\langle 0\rangle = \bigcap_{i=1}^{n} I_i$. Sean $P_i = r(I_i)$. Tenemos que $\bigcup_{i=1}^{n} P_i = \{x \in A \,/\, (\langle 0\rangle : x) \neq \langle 0\rangle\}$ es el conjunto de los divisores de cero en A. Sea $\mathcal{N}$ el conjunto de los elementos nilpotentes, entonces $\mathcal{N} = \bigcap_{i=1}^{n} P_i$. Note que $\langle 0\rangle = I \subseteq P$, así $P_i \subseteq P$.

Proposición 5.2.3. Sea S un conjunto multiplicativamente cerrado e I un ideal P-primario de un anillo A. Entonces:

(1) $S \cap P \neq \emptyset \Longrightarrow S^{-1}I = S^{-1}A$.

(2) $S \cap P = \emptyset \Longrightarrow S^{-1}I$ es $S^{-1}P$-primario.

Demostración:

(1) Sea $s \in S \cap P$. Luego existe $n \in \mathbb{N}$ tal que $s^n \in I$. Luego $1 = \frac{s^n}{s^n} \in (S^{-1}I) \cap U(S^{-1}A)$. Por lo que $S^{-1}I = S^{-1}A$.

(2) Primero veamos que $S^{-1}P$ es primo. Supongamos $x/s \cdot /t \in S^{-1}P$. Luego existen $p \in P$ y $u \in S$ tales que $xy/st = p/u$. De donde existe $v \in S$ tal que $uvxy = vstp \in P$. Se sigue que $xy \in P$. Como P es primo, nos queda $x \in P$ o $y \in P$. Por lo que $x/s \in S^{-1}P$ o $y/t \in S^{-1}P$. Si $p/s \in S^{-1}P$, entonces $p \in P$ y luego $p^n \in I$. Entonces $p^n/s^n \in S^{-1}I$ y $p/s \in r(S^{-1}I)$.

□

Proposición 5.2.4. Sea S un subconjunto multiplicativamente cerrado de A. La contracción de in ideal primario I en $S^{-1}A$ es un ideal primario en A.

Demostración: Sea I un ideal primario en $S^{-1}A$. Considere la proyección $f : A \ni a \mapsto a/1 \in S^{-1}A$. Probemos que $f^{-1}(I)$ es primario en A. Si $xy \in f^{-1}(I)$ entonces $f(x)f(y) = f(xy) \in I$. Como I es primario, se tiene $f(x) \in I$ o $f(y) \in r(I)$, es decir $x \in f^{-1}(I)$ o $y \in f^{-1}(r(I)) = r(f^{-1}(I))$. □

Si I es un ideal en A, entonces $S^{-1}I$ es un ideal en $S^{-1}A$. La contracción de $S^{-1}I$ en A se denota por $S(I) := f^{-1}(S^{-1}I)$. Tenemos que $I \subseteq S(I)$. Además, note que si I es primario entonces $S(I)$ es también primario.

Proposición 5.2.5. Sean S un subconjunto multiplicativamente cerrado en A, e I un ideal descomponible, con $I = \bigcap_{i=1}^{n} I_i$ una descomposición primaria minimal de I ($r(I_i) = P_i$). Si $S \cap P_i = \emptyset$ para todo $i = 1, \ldots, m$, y $S \cap P_i \neq \emptyset$ para todo $i = m+1, \ldots, n$, entonces $S^{-1}I = \bigcap_{i=1}^{m} S^{-1}I_i$ y $S(I) = \bigcap_{i=1}^{m} I_i$ son ambas descomposiciones primarias minimales.

Demostración: Note que $S^{-1}I = S^{-1}\left(\bigcap_{i=1}^{n} I_i\right) = \bigcap_{i=1}^{n} S^{-1}I_i$. Tenemos $S^{-1}I_i = S^{-1}A$ si $i = m+1, \ldots, n$. Entonces $S^{-1}I = \bigcap_{i=1}^{m} S^{-1}I_i$. Ahora veamos que $S(I) = f^{-1}(S^{-1}I) = \bigcap_{i=1}^{m} I_i$. Sea $x \in S(I)$. Entonces $x/1 = f(x) \in S^{-1}I = \bigcap_{i=1}^{m} I_i$. Esto implica $x \in \bigcap_{i=1}^{m} I_i$. Ahora sea $x \in \bigcap_{i=1}^{m} I_i$. Luego $x \in I_i$ para todo i. Se sigue $f(x) \in S^{-1}I_i$ para todo i. De donde $f(x) \in \bigcap_{i=1}^{m} S^{-1}I_i = S^{-1}I$, es decir $x \in S(I)$. Por lo tanto, $S(I) = \bigcap_{i=1}^{m} I_i$ es una descomposición primaria. Veamos que es minimal. Si no lo fuera, existe $1 \leq j \leq m$ tal que $I_j \supseteq \bigcap_{i \neq j}^{m} I_i \supseteq \bigcap_{i=1}^{n} I_i$ (contradicción). Recuerde que P primo $\implies S^{-1}P$ primo si $S \cap P = \emptyset$. Note que $r(S^{-1}I_i) = S^{-1}P_i$ y que $S^{-1}I_i$ es $S^{-1}P_i$-primario. Supongamos $S^{-1}I_j \supseteq \bigcap_{i \neq j}^{m} I_i S^{-1}I_i$. Luego para todo $y \in \bigcap_{i=1}^{m} I_i$, $y/1 \in \bigcap_{i=1}^{m} S^{-1}I_i \subseteq S^{-1}I_j$. De donde $y/1 = y_j/s_j$, es decir $P_j \not\ni us_j y = uy_j \in I_j$. Luego, $y \in I_j$ (contradicción). Tenemos que para toto $i \neq j$, $r(S^{-1}I_i) = S^{-1}P_i \neq S^{-1}P_j = r(S^{-1}I_j)$. Si $S^{-1}P_i = S^{-1}P_j$ entonces $p_i/1 = p_j/s_j$. Luego $tp_i s_j = tp_j \in P_j$, donde $ts_j \notin P_j$. Esto implica que $p_i \in P_j$ (contradicción). □

Definición 5.2.2. Los **ideales primos de un ideal** I son los radicales de los ideales I_i que aparecen en una descomposición primaria minimal de I ($I = \bigcap_{i=1}^{n} I_i$, $P_i = r(I_i)$). Un conjunto Σ de ideales primos que pertenecen a I se dice **aislado** si satisface la siguiente condición: Sea P' un ideal primo perteneciente a I contenido en un ideal $P \in \Sigma$, entonces $P' \in \Sigma$.

Sea Σ el conjunto aislado de los ideales primos de I. Entonces $S = A \setminus \bigcup_{P \in \Sigma} P$ es un subconjunto multiplicativamente cerrado de A. Si $x, y \in S$ entonces $x, y \notin P$ para todo $P \in \Sigma$. Luego $xy \notin P$ para todo $P \in \Sigma$ por ser P primo. Entonces $xy \in S$.

Lema 5.2.4. Sean $P_1 \ldots, P_n$ ideales primos e I un ideal tal que para todo $j = 1, \ldots, n$, $I \not\subseteq P_j$. Entonces $I \not\subseteq \bigcup_{j=1}^{n} P_j$.

Demostración: Usemos inducción sobre n. El caso $n = 1$ es inmediato. Supongamos que el resultado es cierto para $n-1$ y que $I \not\subseteq P_j$ para $j = 1, \ldots, n$. Luego, $I \not\subseteq \bigcup_{i \neq 1}^{n} P_i$, $\ldots$, $I \not\subseteq \bigcup_{i \neq n}^{n} P_i$. De donde, existe $x_1 \in I$ tal que $x_1 \notin P_2, \ldots, P_n$, $\ldots$, $x_n \in I$ tal que $x_n \notin P_1, \ldots, P_{n-1}$. Si algún x_i no pertenece a P_i, entonces $x_i \in I$ y $x_i \notin \bigcup_{j=1}^{n} P_j$. Si para todo i, $x_i \in P_i$, entonces para todo i, $y_i = x_1 \cdots x_{i-1} \cdot x_{i+1} \cdots x_n \notin P_i$. Así, $\sum_{i=1}^{n} y_i \notin \bigcup_{i=1}^{n} P_i$. □

Proposición 5.2.6. Para cada ideal primo P' perteneciente a I, se tiene:

(1) $P' \in \Sigma \Longrightarrow P' \cap S = \emptyset$.

(2) $P' \notin \Sigma \Longrightarrow P' \cap S \neq \emptyset$.

Demostración: Para (1), si $P' \in \Sigma$, se tiene $P' \cap S = P' \cap \left(A \backslash \bigcup_{P\in\Sigma} P\right) = \emptyset$. Ahora probemos (2). Tenemos

$$P' \cap S = P' \cap \left(A \backslash \bigcup_{P\in\Sigma} P\right) = P' \cap \left(\bigcup_{P\in\Sigma} P\right)^c = P' \cap \left(\bigcap_{P\in\Sigma} P^c\right) = \bigcap_{P\in\Sigma} (P' \cap P^c).$$

Luego $P' \notin \Sigma$ implica que para todo $P \in \Sigma$, se tiene $P' \not\subseteq P$. Se sigue $P' \not\subseteq \bigcup_{P\in\Sigma} P$, por el lema anterior. Así,

$$P' \cap S = P' \cap \left(A \backslash \bigcup_{P\in\Sigma} P\right) \neq \emptyset.$$

□

Teorema 5.2.2 (Segundo Teorema de Unicidad)**.** Sea $I = \bigcap_{i=1}^{n} I_i$ una descomposición primaria minimal y $\{P_{i_1}, \ldots, P_{i_m}\}$ el conjunto aislado de ideales primos de I. Entonces los P_{i_1}, …, P_{i_m} son independientes de la descomposición.

CAPÍTULO 6

CONDICIONES DE CADENA

6.1 Módulos Noetherianos y Artinianos

Definición 6.1.1. Recordemos que un conjunto no vacío $(\Sigma, \leq)$ se dice **parcialmente ordenado** si:

(1) Para todo $x \in \Sigma$, $x \leq x$.

(2) Para todo $x, y, z \in \Sigma$, $x \leq y$ e $y \leq z \Longrightarrow x \leq z$.

(3) PAra todo $x, y \in \Sigma$, $x \leq y$ e $y \leq x \Longrightarrow x = y$.

El conjunto $(\Sigma, \leq)$ se dice **totalmente ordenado** si además satisface:

(4) Para todo $x, y \in \Sigma$, $x \leq y$ o $y \leq x$.

Ejemplo 6.1.1.

(1) Los conjuntos $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, con la relación $\leq$ de "menor o igual", son totalmente ordenados.

(2) Si A es un conjunto no vacío, entonces $(P(A), \subseteq)$ y $(P(A), \supseteq)$ son parcialmente ordenados.

Proposición 6.1.1. En un conjunto parcialmente ordenado $(\Sigma, \leq)$, las siguientes condiciones son equivalentes:

(1) Todo subconjunto no vacío de Σ tiene elemento maximal.

(2) Toda sucesión creciente $x_1 \leq x_2 \leq \cdots$ de elementos de Σ es **estacionaria**, es decir que existe $n \in \mathbb{N}$ tal que para todo $k \in \mathbb{N}$, se tiene $x_n = x_{n+k}$.

Demostración:

- (1) $\Longrightarrow$ (2): Sea $x_1 \leq x_2 \leq \cdots$ una sucesión creciente no vacía de Σ. El conjunto $\{x_i : i \in \mathbb{N}\}$ tiene un elemento maximal, es decir que existe $n \in \mathbb{N}$ tal que $x_i \leq x_n$ para todo $i \in \mathbb{N}$. Por lo tanto para todo $k \in \mathbb{N}$, se tiene $x_{n+k} \leq x_n \leq x_{n+k}$.

- (2) $\Longrightarrow$ (1): Sea $T \subseteq \Sigma$ un subconjunto no vacío. Supongamos que T no posee elemento maximal. Contruímos la siguiente sucesión creciente en T: tomamos $x_1 \in T$. Como x_1 no es maximal, se toma $x_2 \in T \backslash \{x_1\}$ tal que $x_1 \leq x_2$. Como x_2 no es maximal, se toma $x_3 \in T \backslash \{x_1, x_2\}$ tal que $x_2 \leq x_3$. Así sucesivamente, se obtiene una sucesión creciente de elementos de T distintos entre sí, obteniendo así una contradicción.

□

Sea M un A-módulo. Considere el conjunto parcialmente ordenado $(\Sigma, \subseteq)$ de los submódulos de M. Si Σ satisface una de las dos condiciones equivalentes de la proposición anterior, diremos que M es un módulo **Noetheriano**. Es decir, si $N_1 \subseteq N_2 \subseteq \cdots$ es una sucesión creciente de submódulos de M, entonces existe $n \in \mathbb{N}$ tal que para todo $k \in \mathbb{N}$, $N_n = N_{n+k}$. Es este caso, (1) es llamada **condición de cadena ascendente (c.c.a)**. Ordenando parcialmente a $\Sigma = \{N \subseteq M : N \text{ es un submódulo de } M\}$ con $\supseteq$, si $(\Sigma, \supseteq)$ satisface (1) o (2) (es decir, para toda cadena descendente $N_1 \supseteq N_2 \supseteq \cdots$ existe $k \in \mathbb{N}$ tal que $N_k = N_{n+k}$ para todo $n \in \mathbb{N}$), entonces M satisface la **condición de cadena descendente (c.c.d)**, y en este caso diremos que M es un módulo **Artiniano**.

Ejemplo 6.1.2.

(1) Todo A-módulo finito es Noetheriano y Artiniano.

(2) El conjunto $\mathbb{Z}$, como $\mathbb{Z}$-módulo es Noetheriano pero no Artiniano. Los submódulos de $\mathbb{Z}$ son sus ideales y estos son principales. Consideremos una cadena ascendente $I_1 = \langle x_1 \rangle \subseteq I_2 = \langle x_2 \rangle \subseteq \cdots$. Entonces el ideal $I = \bigcup_{i=1}^{\infty} I_i = \langle y \rangle$ es principal. Luego $y \in I_k = \langle x_k \rangle = I$, por lo que $\mathbb{Z}$ es Noetheriano. Para ver que $\mathbb{Z}$ no es Artiniano, basta considerar la cadena descendente $\langle 2 \rangle \supsetneq \langle 2^2 \rangle \supsetneq \langle 2^3 \rangle \supsetneq \cdots$, que no es estacionaria.

Proposición 6.1.2. Un módulo M es Noetheriano si, y sólo si, todo submódulo de M es finitamente generado.

Demostración: Suponga que existe un submódulo $N \subseteq M$ que no es finitamente generado. Tome $n_1 \in N$ tal que $N \neq \langle n_1 \rangle$. Luego tome $n_2 \in N \backslash \langle n_1 \rangle$, $N \supsetneq \langle n_1, n_2 \rangle$. Tome $n_3 \in N \backslash \langle n_1, n_2 \rangle$, $N \supsetneq \langle n_1, n_2, n_3 \rangle$. Así obtenemos una sucesión creciente no estacionaria $\langle n_1 \rangle \subsetneq \langle n_1, n_2 \rangle \subsetneq \langle n_1, n_2, n_3 \rangle \subseteq \cdots$. Para probar la otra implicación, consideremos una sucesión creciente $N_1 \subseteq N_2 \subseteq N_3 \subseteq \cdots$ de submódulos de M. Luego $\bigcup_{i=1}^{\infty} N_i$ es un submódulo de M, el cual es finitamente generado: $\bigcup_{i=1}^{\infty} N_i = \langle x_1, \ldots, x_k \rangle$. Existe $m \in \mathbb{N}$ tal que $x_1, \ldots, x_k \in N_m$, lo cual implica que la sucesión anterior es estacionaria. □

Proposición 6.1.3. Sea $0 \longrightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \longrightarrow 0$ una sucesión exacta de A-módulos. Entonces:

(1) M es Noetheriano si, y sólo si, M' y M'' son Noetherianos.

(2) M es Artiniano si, y sólo si, M' y M'' son Artinianos.

Demostración: Sólo probaremos la parte (1). Supongamos que M es un anillo Noetheriano. Sea $N_1' \subseteq N_2' \subseteq \cdots$ una sucesión creciente de submódulos de M'. Entonces $\alpha(N_1') \subseteq \alpha(N_2') \subseteq \cdots$ es una sucesión creciente de submódulos de M. Como M es Noetheriano, existe $k \in \mathbb{N}$ tal que $\alpha(N_k') = \alpha(N_{k+j}')$ para todo $j \in \mathbb{N}$. Por ver que $N_{k+j}' \subseteq N_k$, para todo j. Sea $n' \in N_{k+j}'$. Entonces $\alpha(n') \in \alpha(N_k')$, por lo que existe $n_0 \in N_k'$ tal que $\alpha(n') = \alpha(n_0)$, es decir $\alpha(n' - n_0) = 0$. Como α es injectiva, se tiene $n' = n_0 \in N_k'$. Ahora supongamos que M' y M'' son Noetherianos. Sea $N_1 \subseteq N_2 \subseteq \cdots$ una cadena ascendente de submódulos de M. Entonces $\alpha^{-1}(N_1) \subseteq \alpha^{-1}(N_2) \subseteq \cdots$ y $\beta(N_1) \subseteq \beta(N_2) \subseteq \cdots$ son cadenas ascendentes de submódulos de M' y M'', respectivamente. Luego, existen k' y k'' en $\mathbb{N}$ tales que para todo $j \in \mathbb{N}$, se tiene $\alpha^{-1}(N_{k'}) = \alpha^{-1}(N_{k'+j})$ y $\beta(N_{k''}) = \beta(N_{k''+j})$. Sea $k = k' + k''$. Para todo $j \in \mathbb{N}$, se tiene $\alpha^{-1}(N_k) = \alpha^{-1}(N_{k+j})$ y $\beta(N_k) = \beta(N_{k+j})$. Falta probar que $N_{k+j} \subseteq N_k$. Si $n \in N_{k+j}$, entonces $\beta(n) \in \beta(N_k)$. Por lo que existe $n_1 \in N_k$ tal que $\beta(n) = \beta(n_1)$. Luego, $n - n_1 \in \mathrm{Ker}(\beta) = \mathrm{Im}(\alpha)$. Por lo que existe $n' \in M'$ tal que $\alpha(n') = n - n_1 \in N_{k+j}$. De donde $n' \in \alpha^{-1}(N_{k+j}) = \alpha(N_k)$. Así, $n = \alpha(n') + n_1 \in N_k$. □

Ejercicio 6.1.1. En la proposición anterior, probar la parte (2) y lo que falta de la parte (1).

Corolario 6.1.1. Si $M_1, \ldots, M_n$ son A-módulos Noetherianos (o Artinianos) entonces $\bigoplus_{i=1}^n M_i$ es Noetheriano (resp. Artiniano).

Demostración: Para $n = 1$ es inmediato. Supongamos que el resultado es cierto para $n - 1$. Luego $\bigoplus_{i=1}^{n-1} M_i$ es Noetheriano (Artiniano). Tenemos la sucesión exacta

$$0 \longrightarrow M_n \xrightarrow{\alpha} \bigoplus_{i=1}^{n} M_i \xrightarrow{\beta} \bigoplus_{i=1}^{n-1} M_i \longrightarrow 0,$$

donde $\alpha(m_n) = (0, 0, \ldots, 0, m_n)$ y $\beta(m_1, \ldots, m_n) = (m_1, \ldots, m_{n-1})$. Como M_n y $\bigoplus_{i=1}^{n-1} M_i$ son Noetherianos (resp. Artinianos), se tiene por la Proposición anterior que $\bigoplus_{i=1}^n M_i$ también lo es. □

Definición 6.1.2. Un anillo A se dice **Noetheriano** (resp. **Artiniano**) si es Noetheriano (resp. Artiniano) como A-módulo.

Proposición 6.1.4. Si A es Noetheriano (resp. Artiniano) y M es un A-módulo finitamente generado, entonces M es un módulo Noetheriano (resp. Artiniano).

Demostración: Sea $M = \langle f_1, \ldots, f_n \rangle$. Considere la aplicación $A^n \xrightarrow{\beta_0} M$ dada por $\beta_0(0, \ldots, 1, \ldots, 0) = f_i$, si 1 está en la i-ésima posición. Se tiene que $M \cong A^n/\mathrm{Ker}(\beta_0)$. Como A^n es Noetheriano (resp. Artiniano), se sigue que M también lo es. □

6.2 Longitud

Recordemos que una **cadena** de submódulos de un A-módulo M es una sucesión de submódulos de M:

$$\langle 0\rangle = M_0 \subsetneqq M_1 \subsetneqq M_2 \subsetneqq \cdots \subsetneqq M_n = M.$$

La **longitud** de una cadena como ésta es n. Una **cadena maximal** es una cadena a la que no se le pueden añadir submódulos, es decir que para todo $i = 1, \ldots, n$ si $J \subseteq M$ es un submódulo de M y $M_{i-1} \subseteq J \subseteq M_i$, entonces $M_{i-1} = J$ o $M_i = J$. O equivalentemente, el A-módulo M_i/M_{i-1} no tiene submódulos diferentes de los triviales, para todo i. Una cadena maximal se llama **serie de composición**.

Definición 6.2.1. La longitud de un A-módulo M se define como el mínimo de las longitudes de todas las series de composición de M, si M tiene series de composición. De lo contrario diremos que M posee longitud infinita. Denotaremos la longitud de M por $l(M)$.

Lema 6.2.1. Sea M un A-módulo de longitud finita $l(M) < \infty$. Si M es un submódulo de N, entonces $l(N) \leq l(M)$.

Demostración: Sea $l(M) = n$ y $\langle 0\rangle = M_0 \subsetneqq M_1 \subsetneqq \cdots \subsetneqq M_n = M$ una serie de composición de longitud mínima. Considere $\langle 0\rangle = N \cap M_0 \subseteq N \cap M_1 \subseteq \cdots \subseteq N \cap M_n = N$. Se define para cada $i = 1, \ldots, n$, $f : N \cap M_i / N \cap M_{i-1} \longrightarrow M_i/M_{i-1}$ por $f(m + N \cap M_{i-1}) = m + M_{i-1}$. Consideremos el diagrama

$$\begin{array}{ccc} m_1 + N \cap M_{i-1} & \xrightarrow{=} & m_2 + N \cap M_{i-1} \\ \Big\downarrow f & & \Big\downarrow f \\ m_1 + M_{i-1} & \xrightarrow[=]{} & m_2 + M_{i-1} \end{array}$$

Note que $m_1 - m_2 \in N \cap M_{i-1} \subseteq M_{i-1}$. Entonces f está bien definida. Es claro que f es un homomorfismo de A-módulos. Veamos que f es inyectiva. Supongamos que $f(m + N \cap M_{i-1}) = m + M_{i-1} = 0 + M_{i-1}$, donde $m \in M_{i-1}$. Tenemos $m \in N \cap M_i \Longrightarrow m \in N$. Así $m \in N \cap M_{i-1} \Longrightarrow m + N \cap M_{i-1} = 0 + N \cap M_{i-1}$. Tenemos que M_i/M_{i-1} sólo tiene submódulos triviales. Por lo tanto $M_i/M_{i-1} \cong f\,(N \cap M_i / N \cap M_{i-1})$. Si $M_i/M_{i-1} = \langle 0\rangle$ entonces $N \cap M_i = N \cap M_{i-1}$. En caso contrario $N \cap M_i / N \cap M_{i-1}$ no tiene submódulos triviales, y no hay submódulos entre $N \cap M_{i-1}$ y $N \cap M_i$. Elimimando los términos repetidos en $\langle 0\rangle = N \cap M_0 \subseteq N \cap M_1 \subseteq \cdots \subseteq N \cap M_n = N$. Así se tiene una serie de composición de N de longitud menor o igual que $l(M)$. Por lo tanto $l(N) \leq l(M)$. □

Lema 6.2.2. Sea M un A-módulo con $l(M) = n < \infty$. Si $N \subsetneqq M$ es un submódulo de M entonces $l(N) < l(M)$.

Demostración: Si $l(N) = l(M)$ entonces la serie de composición de N ontenida por la eliminación de términos idénticos en $\langle 0\rangle = N \cap M_0 \subseteq N \cap M_1 \subseteq \cdots \subseteq N \cap M_n = N$ tiene longitud n y no hay términos iguales. Entonces $\langle 0\rangle = N \cap M_0 = M_0$ implica que $\langle 0\rangle = M_0 \subseteq N \cap M_1 \subseteq M_1$. De donde $N \cap M_1 = M_0 = \langle 0\rangle$ (lo cual no es posible), o $N \cap M_1 = M_1$. Se sigue $N \cap M_1 = M_1 \subseteq N \cap M_2 \subseteq M_2$.

De esto se tiene $N \cap M_2 = M_2$, y así sucesivamente. Hasta que obtenemos $N \cap M_n = M_n = M \subseteq N$, obteniendo una contradicción. $\square$

Lema 6.2.3. Si M es un A-módulo de longitud n, entonces toda cadena en M tiene longitud menor o igual que n.

Demostración: Sea $\langle 0 \rangle = M_0 \subsetneqq M_1 \subsetneqq \cdots \subsetneqq M_k = M$ una cadena de M. Por el lema anterior, $0 = l(M_0) < l(M) = n$. Además $l(M_0) < l(M)$ pues $M_0 \subsetneqq M_1$. De manera similar, $l(M_0) < l(M_1) < l(M_2)$ hasta obtener $l(M_0) < l(M_1) < l(M_2) < \cdots < l(M_k) = l(M) = n$. Entonces $k \leq l(M_k) = n$. $\square$

Teorema 6.2.1. Sea M un A-módulo de longitud n. Entonces toda serie de composición de M tiene longitud n.

Demostración: Si $\langle 0 \rangle = M_0 \subsetneqq M_1 \subsetneqq \cdots \subsetneqq M_n = M$ y $\langle 0 \rangle = M'_0 \subsetneqq M'_1 \subsetneqq \cdots \subsetneqq M'_k = M$ son dos series de composición de M, donde la primera es de longitud mínima. Por el lema anterior, $k \leq n$. Por otro lado, $l(M) = n$ es el mínimo de las longitudes de las series de composición de M, por lo que $n \leq k$. $\square$

Corolario 6.2.1. Sea M un A-módulo de longitud finita $l(M) = n$. A toda cadena se le pueden añadir submódulos hasta convertirla en una serie de composición.

Demostración: Sea $\langle 0 \rangle = M_0 \subsetneqq M_1 \subsetneqq \cdots \subsetneqq M_k = M$ $(*)$. Si para todo $1 \leq i \leq k$ vale la condición: para todo submódulo $J \subseteq M$ tal que $M_{i-1} \subseteq J \subseteq M_i \Longrightarrow M_{i-1} = J$ o $M_i = J$, entonces $(*)$ es una serie de composición. En caso contrario, existe $1 \leq i \leq k$ y un submódulo $J \subseteq M$ tal que $M_{i-1} \subsetneqq J \subsetneqq M_i$. Luego $\langle 0 \rangle = M_0 \subsetneqq M_1 \subsetneqq \cdots \subsetneqq M_{i-1} \subsetneqq J \subsetneqq M_i \subsetneqq \cdots \subsetneqq M_k = M$ $(**)$ es una cadena de longitud $k+1$. Si $k+1 = n$, la cadena es una serie de composición. Si no, se puede añadir submódulos tal que $(**)$ es una serie de composición y $k+1 = n$. Procediendo así, cuando la cadena obtenida al añadir submódulos tenga longitud n, esto es una serie de composición, pues en caso contrario, se puede añadir a esta cadena de longitud n otros submódulos, con lo cual se tendría una cadena de longitud $n+1$, lo que contradice el lema anterior. $\square$

Teorema 6.2.2. Sea M un A-módulo. Entonces $l(M) \leq n < \infty$ si, y sólo si, M es Noetheriano y Artiniano.

Demostración: Supongamos primero que $M_1 \subsetneqq M_2 \subsetneqq \cdots$ es una cadena ascendente de submódulos de M. Luego, $\langle 0\rangle = M_0 \subsetneqq M_1 \subsetneqq \cdots \subsetneqq M_k \subsetneqq M$ $(*)$ no puede tener más de $n-1$ submódulos, pues en caso contrario la cadena tendría más de $l(M) = n$ submódulos (contradicción).

Para probar la otra implicación, sea $M = M_0$ y consideremos el conjunto Σ de submódulos de M. Sea M_1 un submódulo maximal de Σ. Tenemos $M_0 \supsetneqq M_1$. Si $M_1 \neq \langle 0\rangle$, entonces consideremos un elemento maximal de $\Sigma_1 = \{N \subsetneqq M_1 : N \text{ es submódulo de } M_1\}$. Luego existe un submódulo maximal M_2 en Σ. Procediendo de esta manera, se obtiene una cadena ascendente estacionaria $M_0 \supsetneqq M_1 \supsetneqq M_2 \supsetneqq \cdots \supsetneqq M_n = \langle 0\rangle$, que es una serie de composición. Por lo que $l(M) = n < \infty$. □

Teorema 6.2.3. Para un $\mathbb{K}$-espacio vectorial V, las siguientes condiciones son equivalentes:

(1) $\dim(V) = n < \infty$.

(2) $l(V) = n < \infty$.

(3) V es Noetheriano.

(4) V es Artiniano.

Demostración:

- (1) $\Longrightarrow$ (2): Todas las series de composición de V $\langle 0\rangle = V_0 \subsetneqq V_1 \subsetneqq \cdots \subsetneqq V_k = V$ tienen longitud menor o igual que n, pues en caso contrario, tomando $v_1 \in V_1 \backslash V_0$, $v_2 \in V_2 \backslash (V_1 \cup V_0)$, $\ldots$, $v_k \in V_k \backslash \left(\bigcup_{i=1}^{k-1} V_i\right)$, $\{v_1, \ldots, v_k\}$ es un conjunto linealmente independiente con más de n elementos.
- (2) $\Longrightarrow$ (3) y (4): Ya fue probado.
- (3) $\Longrightarrow$ (1): Si existe un conjunto infinito linealmente independiente entonces existe uno numerable $\{v_i\}_{i\in\mathbb{N}}$ linealmente independiente. Así $\langle 0\rangle = V_0 \subsetneqq \langle v_1\rangle \subsetneqq \langle v_1, v_2\rangle \subsetneqq \cdots$ es una cadena ascendente no estacionaria, por lo que V no sería Noetheriano.
- (4) $\Longrightarrow$ (1): Supongamos que existe $\beta = \{v_i\}_{i\in\mathbb{N}}$ linealmente independiente. Entonces tenemos que $\langle\beta\rangle \supsetneqq \langle\beta\backslash\{v_1\}\rangle \supsetneqq \langle\beta\backslash\{v_1, v_2\}\rangle \supsetneqq \cdots$ es una cadena descendente no estacionaria, por lo que V no sería Artiniano.

□

6.3 Anillos Noetherianos

Proposición 6.3.1. Sea $f : A \longrightarrow B$ un homomorfismo de anillos sobreyectivo. Si A es Noetheriano entonces B también lo es.

Demostración: Sea $J_1 \subseteq J_2 \subseteq \cdots$ una cadena ascendente de ideales en B. Entonces $f^{-1}(J_1) \subseteq f^{-1}(J_2) \subseteq \cdots$ es una cadena ascendente de ideales en A. Por lo que existe $n \in \mathbb{N}$ tal que $f^{-1}(J_n) = f^{-1}(J_{n+k})$, para todo $k \in \mathbb{N}$. Como f es sobreyectivo, se tiene $J_n = f(f^{-1}(J_n)) = f(f^{-1}(J_{n+k})) = J_{n+k}$, para todo $k \in \mathbb{N}$. □

Si A es un subanillo de B entonces B deviene en un A-módulo con su suma y con el producto de B restringido $A \times B \longrightarrow B$ dado por $a \cdot b \in B$.

Proposición 6.3.2. Sea A es un subanillo de B. Si A es Noetheriano y B es finitamente generado como A-módulo, entonces B es Noetheriano como anillo.

Demostración: Por resultados anteriores, tenemos que B es Noetheriano como A-módulo. Por otro lado, toda cadena ascendente de ideales de B es también una cadena ascendente de submódulos de B como A-módulos. Por lo que tiene que ser estacionaria y por ende B es Noetheriano. □

Ejemplo 6.3.1. Considere $\mathbb{Z}[i] = \{a + bi \ / \ a, b \in \mathbb{Z}\}$. Note que $\mathbb{Z}$ es un subanillo de $\mathbb{Z}[i]$. Como $\mathbb{Z}$ es Noetheriano y $\mathbb{Z}[i]$ un $\mathbb{Z}$-módulo finitamente generado, se tiene que $\mathbb{Z}[i]$ es un anillo Noetheriano.

Proposición 6.3.3. Si A es un anillo Noetheriano y S es un subconjunto de A multiplicativamente cerrado, entonces $S^{-1}A$ es un anillo Noetheriano.

Demostración: Sea $J_1 \subseteq J_2 \subseteq \cdots$ una cadena ascendente de ideales de $S^{-1}A$. Consideremos la proyección $f : A \longrightarrow S^{-1}A$ dad por $a \mapsto a/1$. Tenemos que $f^{-1}(J_1) \subseteq f^{-1}(J_2) \subseteq \cdots$ es una cadena ascendente de ideales en A. Por lo que existe $n \in \mathbb{N}$ tal que $f^{-1}(J_n) = f^{-1}(J_{n+k})$ para todo $k \in \mathbb{N}$. Como f es sobreyectivo, se tiene que $J_n = J_{n+k}$ para todo $k \in \mathbb{N}$. □

Corolario 6.3.1. Si A es un anillo Noetheriano y P es un ideal primo de A, entonces A_P es Noetheriano.

Teorema 6.3.1 (Teorema de la Base de Hilbert)**.** Si A es un anillo Noetheriano, entonces $A[x]$ es Noetheriano.

Demostración: Basta probar que todo ideal de $A[x]$ es finitamente generado. Sea J un ideal de $A[x]$ y sea $I = \{a \in A \ / \ \text{existe } p(x) \in J \text{ con } p(x) = a_0 + a_1x + \cdots + ax^n\}$. Veamos que I es un ideal de A. Primero, note que $I \neq \emptyset$ pues $0 \in I$. Sean $a.b \in I$. Luego existen $p(x), q(x) \in J$ tales que $p(x) = a_0 + a_1x + \cdots + ax^n$ y $q(x) = b_0 + b_1x + \cdots + bx^m$. Si $m \geq n$, $x^{m-n}p(x) = a_0x^{m-n} + a_1x^{m-n+1} + \cdots + ax^m$ y $x^{m-n}p(x) - q(x) = \cdots + (a-b)x^m \in J$, así, $a - b \in I$. Ahora supongamos que $a \in I$ y $b \in A$. Luego existe $p(x) = a_0 + a_1x + \cdots + ax^n \in J$. Tenemos $bp(x) = ba_0 + ba_1x + \cdots + bax^n \in J$ y así

$ab \in I$. Como A es Noetheriano, se tiene que I es finitamente generado. Supongamos $I = \langle a_1, \ldots, a_n \rangle$. Luego existen $p_1(x), \ldots, p_n(x) \in J$ con $p_i(x) = a_0^i + a_1^i x + \cdots + a_i x^{r_i}$. Sea $r = \max(r_i)$. Luego, $J = (J \cap \langle 1, x, \ldots, x^{r-1} \rangle) + \langle p_1(x), \ldots, p_n(x) \rangle$, donde el primer sumando es finitamente generado, porque $\langle 1, x, \ldots, x^{r-1} \rangle$ es un A-módulo finitamente generado y A es Noetheriano. Sea $f(x) \in J$ el polinomio $c_0 + c_1 x + \cdots + c_m x^m$. Si $m \geq r$, $c_m \in I = \langle a_1, \ldots, a_n \rangle$. Luego $c_m = a_1 y_1 + \cdots + a_n y_n$. Tenemos

$$y_i x^{m-r_i} p_i(x) = \cdots + y_i a_i x^m \in J$$

$$f(x) - \sum_{i=1}^{n} y_i x^{m-r_i} p_i(x) = \cdots + \left(c_m - \sum_{i=1}^{n} y_i a_i \right) x^m, \text{ donde } \sum_{i=1}^{n} y_i a_i = 0.$$

Por lo tanto $f(x) - \sum_{i=1}^{n} y_i x^{m-r_i} p_i(x) \in J$ y tiene grado menor o igual que $m-1$. Ahora, si el grado de $f(x) - \sum_{i=1}^{n} y_i x^{m-r_i} y_i p_i(x)$ es mayor o igual que r, se aplica una vez más el procedimiento anterior para reducir el grado. Procediendo así, en algún momento se tiene que $h(x) = f(x) - \sum_{i=1}^{n} q_i(x) p_i(x) \in J$ y grado$(h(x)) < m$. Por lo tanto, $f(x) = h(x) + \sum_{i=1}^{n} q_i(x) p_i(x) \in J \cap \langle x, \ldots, x^{r-1} \rangle + J$. □

Corolario 6.3.2. Si A es un anillo Noetheriano entonces $A[x_1, \ldots, x_n]$ también lo es.

6.4 Anillos Artinianos

Proposición 6.4.1. En un anillo Artiniano todo ideal primo es maximal.

Demostración: Sea P un ideal primo. Entonces A/P es un dominio entero. Sea $x + P \in A/P \backslash \{0 + P\}$. Luego $\langle x + P \rangle \supseteq \langle x^2 + P \rangle \supseteq \cdots \langle x^n + P \rangle \supseteq \cdots$. Como A es Artiniano, existe $n \in \mathbb{N}$ tal que $\langle x^n + P \rangle = \langle x^{n+j} + P \rangle$, para todo $j \in \mathbb{N}$. En particular, $\langle x^n + P \rangle = \langle x^{n+1} + P \rangle$. Así, $x^n + P = (y + P)(x^{n+1} + P)$, para algún $y \in A$. De donde $(x^n + P)(1 - yx + P) = x^n - yx^{n+1} + P = 0 + P$. Como A/P es un dominio entero y $x^n + P \neq 0 + P$, se tiene $1 - yx + P = 0 + P$. De esto se sigue que $(x + P)(y + P) = 1 + P$. □

Corolario 6.4.1. En un anillo Artiniano A, el nilradical $\mathcal{N}$ es igual al radical de Jacobson $\mathcal{R}$.

Proposición 6.4.2. Un anillo Artiniano tiene un número finito de ideales maximales.

Demostración: Recordemos que si $I_1, \ldots, I_n$ son ideales de A y P es un ideal primo de A, entonces $\bigcap_{i=1}^{n} I_i \subseteq P \Longrightarrow I_j \subseteq P$ para algún $1 \leq j \leq n$. Sea $\mathcal{M}_1$ un ideal maximal de A. Si no hay otro ideal maximal, la prueba termina aquí. De haber otro ideal maximal $\mathcal{M}_2$, se tiene $\mathcal{M}_1 \supseteq \mathcal{M}_1 \cap \mathcal{M}_2$. De haber otro ideal maximal $\mathcal{M}_3$, se tiene $\mathcal{M}_1 \supseteq \mathcal{M}_1 \cap \mathcal{M}_2 \supseteq \mathcal{M}_1 \cap \mathcal{M}_2 \cap \mathcal{M}_3$. Continuando de esta manera obtenemos una cadena descendente $\mathcal{M}_1 \supsetneq \mathcal{M}_1 \cap \mathcal{M}_2 \cap \mathcal{M}_3 \supsetneq \cdots$. Como A es Artiniano, existe $n \in \mathbb{N}$ tal que $\bigcap_{i=1}^{n} \mathcal{M}_i = \bigcap_{i=1}^{n+1} \mathcal{M}_i \subseteq \mathcal{M}_{n+1}$. Luego, existe $j = 1, \ldots, n$ tal que $\mathcal{M}_j \subseteq \mathcal{M}_{n+1}$. Como $\mathcal{M}_i$ es maximal, nos queda $\mathcal{M}_i = \mathcal{M}_{n+1}$. De donde se sigue el resultado. □

Proposición 6.4.3. Si A es un anillo Artiniano entonces el nilradical $\mathcal{N}$ es nilpotente.

Demostración: Tenemos una cadena $\mathcal{N} \supseteq \mathcal{N}^2 \supseteq \cdots \supseteq \mathcal{N}^k = \mathcal{N}^{k+1} = I$, para algún $k \in \mathbb{N}$. Basta probar que $I = 0$. Supongamos lo contrario. El conjunto $\Sigma = \{J \subseteq A \ / \ J \text{ es un ideal de } A \text{ y } J \cdot I \neq 0\}$ es no vacío. Como A es Artiniano, tenemos que Σ posee un elemento minimal. De donde existe $J \in \Sigma$ minimal. Sea $x \in J \backslash \{0\}$ tal que $x \cdot I \neq \langle 0 \rangle$. Entonces $\langle x \rangle \cdot I \neq \langle 0 \rangle$. De donde $\langle x \rangle \in \Sigma$ y $\langle x \rangle \subseteq J \implies J = \langle x \rangle$. Luego, $(x \cdot I) \cdot I = x \cdot I^2 = x \cdot I \neq \langle 0 \rangle$ implica que $x \cdot I \in \Sigma$. Como $x \cdot I \subseteq \langle x \rangle$, nos queda $x \cdot I = \langle x \rangle$. Se tiene $x = x \cdot y$, para algún $y \in \mathcal{N}^k = \subseteq \mathcal{N}$. Sea $m \in \mathbb{N}$ tal que $y^m = 0$. Se tiene $x = x \cdot y = x \cdot y^2 = \cdots = x \cdot y^m = x \cdot 0 = 0$ (contradicción). $\square$

Corolario 6.4.2. Sea A un anillo Artiniano en el que el ideal nulo es producto de ideales maximales (quizás repetidos), $\langle 0 \rangle = \mathcal{M}_1 \cdots \mathcal{M}_n$. Entonces A es Noetheriano si, y sólo si, A es Artiniano.

Demostración: Se considera para todo $i = 1, \ldots, n$ a $\frac{\mathcal{M}_1 \cdots \mathcal{M}_{i-1}}{\mathcal{M}_1 \cdots \mathcal{M}_i}$ como un $A/\mathcal{M}_1$-espacio vectorial, el cual es Noetheriano si, y sólo si, es Artiniano. Las operaciones en $\frac{\mathcal{M}_1 \cdots \mathcal{M}_{i-1}}{\mathcal{M}_1 \cdots \mathcal{M}_i}$ como A-módulo son: $+$ es la misma como espacio vectorial, y el producto $\cdot$ está dado por $a \cdot \overline{m} = \overline{am} = \overline{a} \cdot \overline{m}$. Note que U es un subespacio de $\frac{\mathcal{M}_1 \cdots \mathcal{M}_{i-1}}{\mathcal{M}_1 \cdots \mathcal{M}_i}$ si, y sólo si, U es un submódulo del A-módulo $\frac{\mathcal{M}_1 \cdots \mathcal{M}_{i-1}}{\mathcal{M}_1 \cdots \mathcal{M}_i}$. Por lo tanto $\frac{\mathcal{M}_1 \cdots \mathcal{M}_{i-1}}{\mathcal{M}_1 \cdots \mathcal{M}_i}$ es un A-módulo Noetheriano si, y sólo si, $\frac{\mathcal{M}_1 \cdots \mathcal{M}_{i-1}}{\mathcal{M}_1 \cdots \mathcal{M}_i}$ es Noetheriano como $A/\mathcal{M}_1$-espacio vectorial. Esto equivale a que $\frac{\mathcal{M}_1 \cdots \mathcal{M}_{i-1}}{\mathcal{M}_1 \cdots \mathcal{M}_i}$ es un $A/\mathcal{M}_1$-espacio vectorial Artiniano, o lo que es igual $\frac{\mathcal{M}_1 \cdots \mathcal{M}_{i-1}}{\mathcal{M}_1 \cdots \mathcal{M}_i}$ es un A-módulo Artiniano. De la exactitud de la sucesión exacta corta

$$0 \longrightarrow \mathcal{M}_1 \hookrightarrow A \longrightarrow A/\mathcal{M}_1 \longrightarrow 0,$$

se sigue que A es Noetheriano (Artiniano) si, y sólo si $A/\mathcal{M}_1$ y $\mathcal{M}_1$ son Noetherianos (resp. Artinianos). De la exactitud de

$$0 \longrightarrow \mathcal{M}_1 \cdot \mathcal{M}_2 \hookrightarrow \mathcal{M}_1 \longrightarrow \frac{\mathcal{M}_1}{\mathcal{M}_1 \cdot \mathcal{M}_2} \longrightarrow 0$$

se sigue que $\mathcal{M}_1$ es Noetheriano (resp. Artiniano) si, y sólo si, $\mathcal{M}_1 \cdot \mathcal{M}_2$ y $\frac{\mathcal{M}_1}{\mathcal{M}_1 \cdot \mathcal{M}_2}$ son Noetherianos (resp. Artinianos). Procediendo así, A es Noetheriano (Artiniano) si, y sólo si, $\mathcal{M}_1 \cdots \mathcal{M}_{i-2}$ y $\frac{\mathcal{M}_1 \cdots \mathcal{M}_{i-2}}{\mathcal{M}_1 \cdots \mathcal{M}_{i-1}}$ son Noetherianos (resp. Artinianos). De la sucesión exacta

$$0 \longrightarrow \mathcal{M}_1 \cdots \mathcal{M}_i \hookrightarrow \mathcal{M}_1 \cdots \mathcal{M}_{i-1} \longrightarrow \frac{\mathcal{M}_1 \cdots \mathcal{M}_{i-1}}{\mathcal{M}_1 \cdots \mathcal{M}_i} \longrightarrow 0,$$

se tiene que A es Noetheriano (Artiniano) si, y sólo si, $\mathcal{M}_1 \cdots \mathcal{M}_i$ y $\frac{\mathcal{M}_1 \cdots \mathcal{M}_{i-1}}{\mathcal{M}_1 \cdots \mathcal{M}_i}$ son Noetherianos (resp. Artinianos). Procedemos de esta manera hasta llegar a la equivalencia anterior para $i = n$, de donde se sigue el resultado. $\square$

Dada una cadena de ideales primos de A, $P_0 \subsetneqq P_1 \subsetneqq \cdots \subsetneqq P_n$ de longitud n. Se define la **dimensión** de A como

$$\dim(A) := \sup\{l(\mathcal{C}) \ / \ \mathcal{C} \text{ es una cadena de ideales primos en } A\} = \left\{ \begin{array}{l} n \in \mathbb{N} \cup \{0\}\,, \\ \infty \end{array} \right.$$

Teorema 6.4.1. A es Artiniano si, y sólo si, A es Noetheriano y $\dim(A) = 0$.

Lema 6.4.1. Si A es un anillo Noetheriano entonces todo ideal de A es intersección finita de ideales irreducibles.

Demostración: Supongamos falsa la tesis. Entonces

$$\Sigma = \{I \subseteq A \ / \ I \text{ es un ideal de } A \text{ que no es intersección finita de irreducibles}\} \neq \emptyset.$$

Como A es Noetheriano, se tiene que existe $\mathcal{M} \in \Sigma$ maximal en Σ. Note que $\mathcal{M}$ no puede ser irreducible. Si $\mathcal{M} = I \cap J$ entonces $I \subsetneqq \mathcal{M}$ y $J \subsetneqq \mathcal{M}$. Pero $\mathcal{M} = \mathcal{M} \cap A$ y $\mathcal{M} \subsetneqq \mathcal{M}$ (contradicción). □

Lema 6.4.2. Si A es un anillo Noetheriano y $\langle 0 \rangle$ es irreducible entonces $\langle 0 \rangle$ es primario.

Demostración: Supongamos $xy \in \langle 0 \rangle$, donde $x \neq 0$. Luego $\text{Ann}(x) \subseteq \text{Ann}(x^2) \subseteq \cdots$. Como A es Noetheriano, existe $n \in \mathbb{N}$ tal que $\text{Ann}(x^n) = \text{Ann}(x^{n+j})$ para todo $j \in \mathbb{N}$. Note que $\langle x^n \rangle \cap \langle y \rangle = \langle 0 \rangle$. Si $ax^n = by$ entonces $ax^{n+1} = byx = 0$. Luego $a \in \text{Ann}(x^{n+1}) = \text{Ann}(x^n)$ implica que $ax^n = 0$. Como $\langle 0 \rangle$ es irreducible y $\langle 0 \rangle = \langle x^n \rangle \cap \langle y \rangle$, donde $\langle y \rangle \neq \langle 0 \rangle$, se tiene que $\langle x^n \rangle = \langle 0 \rangle$. Entonces $x^n = 0 \in \langle 0 \rangle$. □

Corolario 6.4.3. Si A es un anillo Noetheriano e I es un ideal irreducible entonces I es primario.

Demostración: Supongamos $xy \in I$ y $y \notin I$. En A/I, $\langle 0 + I \rangle$ es irreducible. Si $\langle 0 + I \rangle = J \cap K$ entonces $I = \pi^{-1}(J) \cap \pi^{-1}(K)$, donde $\pi : A \longrightarrow A/I$ es la proyección canónica. Se sigue que $I = \pi^{-1}(J)$ o $I = \pi^{-2}(K)$. Por el lema anterior, $\langle 0 + I \rangle$ es primario. Luego, $xy \in I$ e $y \notin I$ implican $xy + I = 0 + I$ e $y + I \neq 0 + I$. Al ser $\langle 0 + I \rangle$ primario, se tiene que existe $n \in \mathbb{N}$ tal que $x^n + I \in \langle 0 + I \rangle$. De donde $x^n \in I$. □

Corolario 6.4.4. Si A es un anillo Noetheriano entonces todo ideal tiene una descomposición primaria.

Demostración: Por el Lema 6.4.1, todo ideal es intersección finita de ideales irreducibles. Como A es Noetheriano, todo irreducible es primario. De esto se sigue el resultado. □

Prueba del Teorema 6.4.1:

($\Longrightarrow$) Supongamos que A es Artiniano. Todo ideal primo es maximal y entonces $\dim(A) = 0$. Sean $\mathcal{M}_1$, $\ldots$, $\mathcal{M}_n$ los ideales maximales de A. Luego $\mathcal{N} = \bigcap_{i=1}^{n} \mathcal{M}_i$, $\prod_{i=1}^{n} \mathcal{M}_i^k \subseteq (\bigcap_{i=1}^{n} \mathcal{M}_i)^k = \mathcal{N}^k = \langle 0 \rangle$. Esto implica que $\langle 0 \rangle = \prod_{i=1}^{n} \mathcal{M}_i$, lo cual quiere decir que A es Noetheriano si, y sólo si, A es Artiniano. Luego, I es irreducible y $I = J \cap K \Longrightarrow I = J$ o $I = K$.

($\Longleftarrow$) Supongamos que A es Noetheriano y $\dim(A) = 0$. El ideal $\langle 0 \rangle$ tiene una descomposición primaria $\langle 0 \rangle = \bigcap_{i=1}^{n} I_i$, donde I_i es primario y $r(I_i) = P_i$ es el menor ideal primo que contiene a I_i, para cada $i = 1, \ldots, n$. Como $\dim(A) = 0$, se tiene que $P_i = \mathcal{M}_i$ es maximal. Entonces $\mathcal{M}_1$, $\ldots$, $\mathcal{M}_n$ son todos los ideales primos de A. De haver otro ideal maximal $\mathcal{M}$, $\langle 0 \rangle = \mathcal{M}_1 \cdots \mathcal{M}_n \subseteq \mathcal{M}$. Así $\mathcal{M}_j \subseteq \mathcal{M}$, para algún $j = 1, \ldots, n$ y por tanto $\mathcal{M}_j = \mathcal{M}$. Tenemos $\mathcal{N} = \bigcap_{i=1}^{n} \mathcal{M}_i$ y $\prod_{i=1}^{n} \mathcal{M}_i \subseteq (\bigcap_{i=1}^{n} \mathcal{M}_i)^k = \mathcal{N}^k = 0$. Por lo tanto, $\langle 0 \rangle = \prod_{i=1}^{n} \mathcal{M}_i^k$.

□

BIBLIOGRAFÍA

[1] Atiyah, M. F.; MacDonald, I. G. *Introduction to Commutative Algebra*. Addison-Wesley Publishing Co. (1969).

[2] Hartly, B; Hawkes, T. 0. *Rings, Modules and Linear Algebras*. Chapman and Hall. (1970).