UNIVERSIDAD NACIONAL
AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS

DESCOMPOSICIÓN PRIMARIA Y TERCIARIA DE IDEALES Y MÓDULOS

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

M A T E M Á T I C O

PRESENTA:

MARIO ALBERTO HERNÁNDEZ SERRANO

DIRECTOR DE TESIS:
Dr. JAIME CASTRO PÉREZ

CIUDAD DE MÉXICO 2019

1.Datos del alumno
Hernández
Serrano
Mario Alberto
5532417561
Universidad Nacional Autónoma de México
Facultad de Ciencias
Matemáticas
306270301

2.Datos del tutor
Dr.
Jaime
Castro
Pérez

3.Datos del sinodal 1
Dra.
Bertha María
Tomé
Arreola

4.Datos del sinodal 2
Dra.
Martha Lizbeth Shaid
Sandoval
Miranda

5.Datos del sinodal 3
Dr.
José
Ríos
Montes

6.Datos del sinodal 4
Dr.
Alejandro
Alvarado
García

7.Datos del trabajo escrito
Descomposición primaria y terciaria de ideales y módulos
66p
2019

Agradecimientos

A mis padres Mario y María y a mi hermano Luis las personas más importantes y que más quiero, por todo el amor y apoyo, por ser un pilar en mi vida para poder ser la persona que soy ahora, por inculcarme tantos valores, por ayudarme a levantarme cuando he tropezado y porque sin su apoyo no habría logrado concluir mis estudios.

A mi tío Kiko, una persona muy generosa por apoyarme en lo que necesité y a mi tía Lourdes que igualmente me brindó su apoyo.

A mi novia Karina, la persona más amorosa y amable, por todos los consejos y por estar a mi lado en las buenas y las malas, por demostrarme que siempre se pueden alcanzar las metas que uno se pone, eres y serás la mujer más importante en mi vida, cuenta conmigo siempre.

A toda mi familia, que siempre me han brindado una sonrisa.

A mi tutor de tesis, el Dr Jaime Castro por toda la ayuda que me brindó, fue uno de los mejores profesores que he tenido.

Le agradezco a todos los sinodales por sus comentarios en especial a la Dra Lizbeth Sandoval.

Al profesor Tonatiuh Valdez, por su amistad y por ayudarme tanto en mi desarrollo como docente.

A la UNAM y a la Facultad de Ciencias.

Finalmente, a todos mis amigos por todo su apoyo y gracias a Dios.

Índice general

Introducción

En esta tesis se desarrollan principalmente los temas de la Descomposición Primaria de Ideales y Módulos sobre un anillo conmutativo. La descomposición primaria para ideales es la generalización del hecho conocido de que un número entero se descompone como producto de potencias de números primos. En anillos neterianos conmutativos cada ideal tiene una descomposición primaria. Es también importante mencionar que el concepto de descomposición primaria también se extiende a la descomposición primaria de un módulo sobre un anillo conmutativo. Para módulos sobre un anillo conmutativo se define lo que es un submódulo primario y en este contexto se obtienen los resultados equivalentes a los obtenidos cuando se trabaja con ideales del anillo.

Es también de gran importancia mencionar que la descomposición primaria va más allá de los anillos conmutativos. En [4] los autores definen la descomposición terciaria de un módulo que en el caso neteriano conmutativo coincide con la descomposición primaria. Además en [6] se menciona que la descompocición terciaria es una razonable generalización de la descomposición primaria la cual fue probada por [6]. Adicionalmente en [6] se aborda una descomposición primaria para anillos no conmutativos, sin embargo los resultados que se obtienen no son tan satisfactorios como los que se obtienen de la descomposición terciaria. También en [2] se da otra descomposición primaria en términos de C-módulos.

En el capítulo 1 damos los preliminares, y hablamos del concepto ideal primo que en la teoría de anillos es una generalización importante del concepto de número primo. En ese mismo capítulo trataremos temas como el radical de un ideal. Mostraremos que el radical de un ideal I es la intersecćon de los ideales primos que contienen a I. Damos también la definición de contracción y extensión de ideales a través de morfismos de anillos. Por último en este mismo capítulo se introduce el tema de anillos de fracciones que son una generalización del campo de fracciones para el álgebra conmutativa.

En el capítulo 2 se desarrollará el tema de descomposición primaria de ideales que es uno de los temas principales de esta tesis. Llegaremos finalmente a los dos teoremas de unicidad.

En el capítulo 3 se utilizará la descomposición primaria de ideales y se la aplicamos a una clase importante de anillos dentro de la teoría del álgebra conmutativa, los anillos neterianos conmutativos. Daremos la descomposición primaria de los ideales de un anillo neteriano conmutativo.

En el capítulo 4 se extiende el concepto de descomposición primaria de ideales a descomposición primaria de submódulos, donde desarrollamos completamente la teoría correspondiente a la descomposición primaria de submódulos de un módulo dado. Obtenemos también los teoremas de unicidad correspondientes al contexto de submódulos.

Finalmente, en el capítulo 5 hablaremos de la descomposición terciaria de módulos. En este capítulo el anillo no es un anillo neteriano conmutativo. Se hace notar que esta descomposición generaliza la descomposición primaria en anillos neterianos conmutativos, vista en el capitulo 3.

Capítulo 1

Preliminares

En el capítulo 1 daremos los preliminares, se desarrollaran conceptos importantes para los temas de descomposición primaria de ideales y módulos.

1.1. Ideales Primos

El concepto de ideal primo es una generalización importante del concepto de número primo.

Definición 1.1.1. *Si A es un anillo conmutativo, un ideal $P \neq A$ es ideal primo si siempre que $xy \in P \Rightarrow x \in P$ o $y \in P$.*

Ejemplos 1.1.2.

1) Si $A = \mathbf{Z}$, entonces los ideales primos son de la forma $p\mathbf{Z}$ donde p es un número entero primo. Note también que el ideal cero es primo.

2) Si $A = \mathbf{Z}_6$ los enteros módulo 6. El ideal $P = 2\mathbf{Z}_6$ es un ideal primo de A. En efecto si $a, b \in A$ tal que $ab \in 2\mathbf{Z}_6$, entonces $ab \equiv 0\ mod(6)$ o $ab \equiv 2\ mod(6)$ o $ab \equiv 4\ mod(6)$, en cualquier caso 2 divide a ab, por lo tanto $a \in 2\mathbf{Z}_6$ o $b \in 2\mathbf{Z}_6$.

Proposición 1.1.3. *Sea A un anillo conmutativo y $Q \neq A$, entonces Q es ideal primo si y solo sí A/Q es dominio entero.*

Demostración $\Rightarrow\rfloor$Sean $x + Q$, $y + Q$ elementos de A/Q tales que $(x+Q)(y+Q) = 0+Q$, entonces $xy+Q = 0+Q$. Por lo tanto $xy \in Q$. Como Q es ideal primo, entonces $x \in Q$ o $y \in Q$. Así tenemos que $x + Q = 0 + Q$ o $y + Q = 0 + Q$. Por lo tanto A/Q es dominio entero.

$\Leftarrow\rfloor$Ahora supongamos que A/Q es dominio entero. Sean $x, y \in A$ tal que $xy \in Q$ entonces $0 + Q = xy + Q = (x + Q)(y + Q)$. Como A/Q es dominio entero, entonces $x + Q = 0 + Q$ o $y + Q = 0 + Q$. Por lo tanto $x \in Q$ o $y \in Q$. Así tenemos que Q es ideal primo. ■

Definición 1.1.4. *Sea A un anillo conmutativo, un ideal $M \neq A$ es máximo si no existe ideal I de A tal que $M \subsetneq I \subsetneq A$.*

Proposición 1.1.5. *Si A es un anillo conmutativo y M es un ideal máximo, entonces M es un ideal primo.*

Demostración. Sean $a, b \in A$ tal que $ab \in M$. Si $a \notin M$ entonces $Aa + M = A$, así existe $r \in A$ y $m \in M$ tal que $ra + m = 1$. Ahora multiplicando por b tenemos que $rab + mb = b$ pero $ab \in M$ entonces $rab \in M$ y como $m \in M$ entonces $mb \in M$ por lo tanto $b \in M$. ■

Note que el inverso de esta proposición es falso, por ejemplo en $\mathbf{Z}$ el ideal cero es primo, pero el ideal cero no es máximo.

Teorema 1.1.6. *Todo anillo conmutativo con 1 tiene al menos un ideal máximo.*

Demostración. La demostración se realizará aplicando el lemma de Zorn. Sea Σ el conjunto de todos los ideales distintos de A, donde Σ es un conjunto parcialmente ordenado por la inclusión y $\Sigma \neq \emptyset$ ya que $0 \in \Sigma$. Para aplicar el lemma de Zorn tenemos que probar que toda cadena ascendente en Σ esta acotada superiormente en Σ.
Sea $\{I_\alpha\}$ una cadena de ideales en Σ, tal que para cualquier par de indices α, β tenemos que $I_\alpha \subseteq I_\beta$ o $I_\alpha \supseteq I_\beta$. Sea $J = \bigcup_\alpha I_\alpha$ donde J es un ideal y además 1 no pertenece a J ya que 1 no pertenece a cada I_α para toda α. Por lo tanto $J \in \Sigma$, y J es una cota superior de la cadena. Por lo tanto por el lemma de Zorn Σ tiene un elemento máximo. ■

Corolario 1.1.7. *Si $I \neq A$ es un ideal en un anillo A, entonces existe un ideal máximo de A que contiene a I.*

Demostración. Sea Π el conjunto de todos los ideales de A que contienen a I, $\Pi \neq \emptyset$ ya que el anillo A pertenece a este conjunto. Π es un conjunto parcialmente ordenado por la inclusión, entonces para aplicar el lemma de Zorn tenemos que probar que toda cadena ascendente en Π está acotada superiormente en Π.

Sea $\{I_\alpha\}$ una cadena de ideales en Π, es decir que para cualquier par de indices α, β, $I_\alpha \subseteq I_\beta$ o $I_\alpha \supseteq I_\beta$. Sea $M = \bigcup_\alpha I_\alpha$, donde M es un ideal y además 1 no pertenece a M ya que 1 no pertenece a cada I_α. Como M pertenece a Π y además M es cota superior de la cadena, entonces por el lemma de Zorn Π tiene un elemento máximo. ■

Corolario 1.1.8. *Si A es anillo conmutativo con 1, entonces toda no unidad en A está contenida en un ideal máximo.*

Demostración. Sea $a \in A$ no unidad. Consideremos Aa el ideal generado por a, entonces $Aa \neq A$, así por el corolario anterior tenemos que existe un ideal máximo M en A, tal que $Aa \subseteq M$. Por lo tanto $a \in M$. ■

Proposición 1.1.9. *Sea A un anillo conmutativo con 1, sean $I_1, I_2, ..., I_n$ ideales de A. Si P es un ideal primo de A tal que $\bigcap_{j=1}^n I_j \subseteq P$. Entonces $I_j \subseteq P$ para algún j. Si además $\bigcap_{j=1}^n I_j = P$ entonces $I_j = P$.*

Demostración. Supongamos que $I_j \nsubseteq P$ para toda j, entonces para cada j, existe $x_j \in I_j$ tal que $x_j \notin P$. Ya que P es primo, entonces $\prod_{j=1}^n x_j \notin P$. Por otra parte sabemos que $I_1 I_2 ... I_n \subseteq I_1 \cap I_2 \cap ... \cap I_n$ y como $\prod_{j=1}^n x_j \in I_1 I_2 ... I_n$, entonces $\bigcap I_j \nsubseteq P$ lo cual es una contradicción. Finalmente, si $P = \bigcap I_j$, entonces $P \subseteq I_j$ para todo j. Así tenemos que $P = I_j$ para algún j. ■

1.2. Radical

En teoría de anillos el concepto de radical nos muestra ciertas propiedades de los ideales parte importante para la descomposición primaria.

Proposición 1.2.1. *Si I es un ideal en un anillo A, entonces el conjunto $r(I) = \{x \in A : x^n \in I \text{ para algún entero } n > 0\}$ es un ideal.*

Demostración. Si $x \in r(I)$, entonces $x^n \in I$ para cierto $n > 0$. Es claro que $\alpha x \in r(I)$ $\forall \alpha \in A$, ya que $(\alpha x)^n = \alpha^n x^n$ e I un ideal. Sean $x, y \in r(I)$, luego $x^m \in I$, $y^n \in I$. Por el teorema binomial (que es válido ya que A es conmutativo), $(x+y)^{n+m+1}$ es suma de enteros multiplicados por productos $x^r y^s$, donde $r + s = m + n + 1$; esto implica que $r \geq m$ o $s \geq n$, entonces cada uno de estos productos está en I. Por lo tanto $(x+y)^{m+n+1} \in I$. Así obtenemos que $x + y \in r(I)$, entonces $r(I)$ es un ideal. ■

Definición 1.2.2. *Sea I un ideal en un anillo A. El radical (o nilradical) de I es el ideal $r(I) = \{x \in A : x^n \in I \text{ para algún entero } n > 0\}$.*

Proposición 1.2.3. *Si I es un ideal en un anillo A, el radical de I es la intersección de todos los ideales primos que contienen a I.*

Demostración. Sea $H = \bigcap\{P \subseteq A \mid P \text{ es ideal primo e } I \subseteq P\}$ la intersección de todos los ideales primos P que contienen a I. Si $x \in r(I)$ y P es un ideal primo tal que $I \subseteq P$, entonces $x^n \in I \subseteq P$ para algún $n > 0$, por lo tanto $x \in P$, entonces $x \in H$. Así $r(I) \subseteq H$.

Recíprocamente, supongamos que $x \in H$ y que $x \notin r(I)$. Sea Λ el conjunto de los ideales J con la propiedad de que $I \subseteq J$ y $x^n \notin J$ para todo $n > 0$ con n número natural. Λ es no vacío porque $r(I) \in \Lambda$. Como Λ es un conjunto parcialmente ordenado por inclusión, se puede aplicar el Lema de Zorn. Por lo tanto Λ tiene un elemento máximo. Sea P' un elemento máximo de Λ. Probaremos que P' es primo.
Sean $y, z \notin P'$, entonces los ideales $< y > +P'$, $< z > +P'$ contienen propiamente a P', entonces no pertenecen a Λ. Por lo tanto $x^m \in < y > +P'$, $x^n \in < z > +P'$ para ciertos $m, n > 0$. Entonces $x^{n+m} \in < yz > +P'$. Así el ideal $< yz > +P' \notin \Lambda$ y por lo tanto $yz \notin P'$. De aquí obtenemos que P' es primo. Entonces tenemos un ideal primo P' tal que $x \notin P'$, por lo tanto $x \notin H$, esto es una contradicción. Así probamos que $\forall x \notin r(I)$ implica $x \notin H$. Por lo tanto $H \subseteq r(I)$, así $H = r(I)$. ■

Proposición 1.2.4. *Si $I, I_1, I_2, ..., I_n$ son ideales en un anillo A, entonces:*

i) $I \subseteq r(I) = r(r(I))$

ii) $r(I_1 I_2 ... I_n) = r(\bigcap_{j=1}^{n} I_j) = \bigcap_{j=1}^{n} r(I_j)$

iii) $r(I) = A \Leftrightarrow I = A$

iv) $r(I_1 + I_2) = r(r(I_1) + r(I_2))$

v) Si P es un ideal primo, entonces $r(P^n) = P$ para todo $n > 0$.

Demostración. (i) Las inclusiones $I \subseteq r(I) \subseteq r(r(I))$ son consecuencia directa de la definición de radical. Si $x \in r(r(I))$, entonces existe $n > 0$ tal que $x^n \in r(I)$ y entonces $x^{nm} = (x^n)^m \in I$ para algún $m > 0$. Por lo tanto, $x \in r(I)$ y $r(r(I)) \subseteq r(I)$.

ii) Si $x \in \bigcap_{j=1}^{n} r(I_j)$ entonces existen $m_1, m_2, ..., m_n > 0$ tal que $x^{m_j} \in I_j$ para cada $j = 1, 2, ..., n$. Si $m = m_1 + m_2 + ... + m_n$ entonces $x^m = x^{m_1}x^{m_2}...x^{m_n} \in I_1I_2...I_n$, por lo tanto $\bigcap_{j=1}^{n} r(I_j) \subseteq r(I_1I_2...I_n)$. Como $I_1I_2...I_n \subseteq \bigcap_{j=1}^{n} I_j$, entonces tenemos que
$r(I_1I_2...I_n) \subseteq r(\bigcap_{j=1}^{n} I_j)$.
Finalmente, si $x \in r(\bigcap_{j=1}^{n} I_j)$, existe un $n > 0$ tal que $x^n \in \bigcap_{j=1}^{n} I_j$, entonces para cada $j = 1, 2, ..., n, x^n \in I_j$, así $x \in r(I_j)$ para toda $j = 1, 2, ..., n$. Por lo tanto $x \in \bigcap_{j=1}^{n} r(I_j)$. Así tenemos que $r(\bigcap_{j=1}^{n} I_j) \subseteq \bigcap_{j=1}^{n} r(I_j)$. Por lo tanto $r(\bigcap_{j=1}^{n} I_j) \subseteq \bigcap_{j=1}^{n} r(I_j) \subseteq r(I_1I_2...I_n) \subseteq r(\bigcap_{j=1}^{n} I_j)$ lo cual prueba el resultado.

iii) Sea $r(I) = A$, entonces para todo $x \in A$, existe un $n > 0$ tal que $x^n \in I$, en particular $1 = 1^n \in I$, por lo tanto $I = A$. La otra implicación es trivial.

iv) De (i) se deduce que $I_1 + I_2 \subseteq r(I_1) + r(I_2)$ y entonces $r(I_1 + I_2) \subseteq r(r(I_1)+r(I_2))$. Para probar la otra contención, tomemos $x \in r(r(I_1)+r(I_2))$ entonces existe $n > 0$ tal que $x^n \in (r(I_1) + r(I_2))$, luego tenemos que $x^n = x_1 + x_2$ donde $x_1 \in r(I_1)$ y $x_2 \in r(I_2)$ o sea existen $n_1, n_2 > 0$, tales que $x^{n_1} \in I_1$ y $x^{n_2} \in I_2$, por el teorema binomial, $(x^n)^{n_1+n_2+1} = (x_1 + x_2)^{n_1+n_2+1}$ es una suma de enteros multiplicados por productos de $x_1^r x_2^s$, donde $r + s = n_1 + n_2 + 1$; no podemos tener que $r < n_1$ y $s < n_2$ así que $r \geq n_1$ o $s \geq n_2$, entonces cada uno de estos productos están en I_1 o en I_2, por lo tanto $x^{n(n_1+n_2+1)} \in I_1 + I_2$ y $x \in r(I_1 + I_2)$.

v) Sea P un ideal primo, por (i) e (ii) $P \subseteq r(P) = r(P^n)$. Solo falta probar que $r(P) \subseteq P$. Sea $x \in r(P)$ y sea n el menor entero positivo tal que $x^n \in P$, como P es un ideal primo, entonces $x \in P$ o $x^{n-1} \in P$. Como n es el mínimo tal que $x^n \in P$, entonces $x^{n-1} \notin P$, así que lo único que puede suceder es que $x \in P$. ■

1.3. Ideal Cociente

Definición 1.3.1. *Si I, J son ideales en un anillo A, su ideal cociente es $(I : J) = \{x \in A : xJ \subseteq I\}$ el cual es un ideal. En particular $(0 : J)$ es llamado el anulador de J y se indica como $Ann(J)$.*

Observación: Si J es el ideal principal $< x >= Ax$, escribiremos $(I : x)$ en lugar de $(I : Ax)$ y $Ann(x)$ en lugar de $Ann(Ax)$. Con esta notación el conjunto de los divisores de cero en A es $D = \bigcup_{x \neq 0} Ann(x)$.

Proposición 1.3.2. *Si $I, J, I_1, I_2, ..., I_n$ son ideales del anillo A, entonces:*

i) $I \subseteq (I : J)$

ii) $(\bigcap_{k=1}^{n} I_k : J) = \bigcap_{k=1}^{n} (I_k : J)$.

Demostración. *i)* Si $x \in I$ entonces tenemos que $xJ \subseteq I$ por ser I ideal de A por lo tanto $x \in (I : J)$. Así $I \subseteq (I : J)$.

ii) Sea $x \in (\bigcap_{k=1}^{n} I_k : J)$ entonces $xJ \subseteq \bigcap_{k=1}^{n} I_k$. Así xJ está incluido en cada I_k y por tanto $x \in (I_k : J)$ para cada $k = 1, 2, ..., n$. Recíprocamente si $x \in \bigcap_{k=1}^{n} (I_k : J)$ entonces para cada k tenemos que $xJ \subseteq I_k$. Luego $xJ \subseteq \bigcap_{k=1}^{n} I_k$ y por esto $x \in (\bigcap_{k=1}^{n} I_k : J)$. ■

En general, se puede definir el radical $r(E)$ de cualquier subconjunto E de A como el conjunto de los $x \in A$ tales que $x^n \in E$ para cierto entero $n > 0$. Generalmente no es un ideal. En efecto si E es un subconjunto de A que no contiene al cero, entonces 0 no pertenece a $r(E)$ y por lo tanto $r(E)$ no es un ideal.

Proposición 1.3.3. *Sea A un anillo y $\{E_\alpha\}$ una familia de subconjuntos de A, entonces $r(\bigcup_\alpha E_\alpha) = \bigcup_\alpha r(E_\alpha)$.*

Demostración. Sea $x \in r(\bigcup_\alpha E_\alpha)$ entonces existe $n > 0$ tal que $x^n \in \bigcup_\alpha E_\alpha$. Por lo tanto existe α tal que $x^n \in E_\alpha$. Así $x \in r(E_\alpha)$, por lo tanto $r(\bigcup_\alpha E_\alpha) \subseteq \bigcup_\alpha r(E_\alpha)$.

Ahora si $x \in \bigcup_\alpha r(E_\alpha)$ entonces $x \in r(E_\alpha)$ para alguna α, entonces existe $n > 0$ tal que $x^n \in E_\alpha$. Así $x^n \in \bigcup_\alpha E_\alpha$, por lo tanto obtenemos que $x \in r(\bigcup_\alpha E_\alpha)$. ■

Proposición 1.3.4. *Sea D el conjunto de los divisores de cero de A, entonces $D = r(D) = \bigcup_{x \neq 0} r(Ann(x))$.*

Demostración. Ya tenemos que $D \subseteq r(D)$, ahora demostraremos que $r(D) \subseteq D$. Sea $x \in r(D)$, si $x \in D$ entonces ya terminamos. Si $x \notin D$, entonces existe $n > 1$ mínimo tal que $x^n \in D$. Por lo tanto existe $y \neq 0$ tal que $x^n y = 0$. Como $x^{n-1} \notin D$, entonces $x^{n-1} y \neq 0$, pero $0 = x^n y = x(x^{n-1} y)$. Por lo tanto $x \in D$ es una contradicción. Así hemos demostrado que $r(D) \subseteq D$, por lo tanto $D = r(D)$. Ahora sabe-

mos que $D = \bigcup_{x\neq 0} Ann(x)$, entonces por la Proposición 8 tenemos que $r(D) = r(\bigcup_{x\neq 0} Ann(x)) = \bigcup_{x\neq 0} r(Ann(x))$. ■

1.4. Extensión y Contracción

En álgebra conmutativa la extensión y la contracción de ideales son operaciones realizadas a partir de los morfimos de anillos.

Definición 1.4.1. *Sea $f : A \longrightarrow B$ un morfismo de anillos. Si I es un ideal en A, se define la extensión I^e de I como el ideal $Bf(I)$ generado por $f(I)$, en forma más explícita se puede definir I^e como el conjunto de todas las sumas $\sum y_i f(x_i)$ donde $x_i \in I, y_i \in B$. Si J es un ideal de B, entonces $f^{-1}(J)$ es siempre un ideal de A, llamado la contracción de J y se denota J^c.*

Note que en general la imagen de un ideal no siempre es un ideal. Por ejemplo consideramos el morfismo inclusión de los enteros $\mathbf{Z}$ en los racionales $\mathbf{Q}$; $f : \mathbf{Z} \to \mathbf{Q}$. Tenemos que $f(2\mathbf{Z}) = 2\mathbf{Z}$ no es un ideal de $\mathbf{Q}$.

Proposición 1.4.2. *Sea $f : A \to B$ un morfismo de anillos y $J \subseteq B$ un ideal primo, entonces la contracción J^c es ideal primo en A.*

Demostración. Sean $x, y \in A$ tal que $xy \in J^c$. Por lo tanto $f(xy) \in J$, como f es morfismo de anillos, entonces $f(xy) = f(x)f(y)$, y como J es ideal primo y $f(x)f(y) \in J$, entonces $f(x) \in J$ o $f(y) \in J$. Así obtenemos que $x \in J^c$ o $y \in J^c$. Por lo tanto J^c es ideal primo de A. ■

Proposición 1.4.3. *Sea $f : A \longrightarrow B$ un morfismo de anillos y sean I ideal de A, y J_1, J_2, J ideales en B, entonces:*

i) $I \subseteq I^{ec}$, $J^{ce} \subseteq J$

ii) $J^c = J^{cec}$, $I^e = I^{ece}$

iii) $(J_1 \cap J_2)^c = J_1^c \cap J_2^c$.

Demostración. i) Sabemos que $I^e = Bf(I)$ y como $f(I) \subseteq Bf(I)$, entonces $f(I) \subseteq Bf(I) = I^e$, por lo tanto $f^{-1}(f(I)) \subseteq f^{-1}(I^e)$. Además es claro que $I \subseteq f^{-1}(f(I))$. Así hemos probado que $I \subseteq f^{-1}(I^e) = I^{ec}$.

Ahora probaremos que $J^{ce} \subseteq J$. Tenemos que $J^c = f^{-1}(J)$, por lo tanto $J^{ce} = (f^{-1}(J))^e = Bf(f^{-1}(J))$. Por otra parte es claro que $f(f^{-1}(J)) \subseteq J$,

por lo tanto $Bf(f^{-1}(J)) \subseteq BJ = J$. Así hemos demostrado que $J^{ce} \subseteq J$.

ii) Por el inciso (i) tenemos que $J^{ce} \subseteq J$, por lo tanto $f^{-1}(J^{ce}) \subseteq f^{-1}(J)$. Como $f^{-1}(J^{ce}) = J^{cec}$ y $f^{-1}(J) = J^c$, entonces $J^{cec} \subseteq J^c$. Ya que $J^c \subset A$, entonces por (i) tenemos que $J^c \subseteq (J^c)^{ec} = J^{cec}$. Por lo tanto tenemos que $J^{cec} \subseteq J^c \subseteq J^{cec}$. Así obtenemos que $J^c = J^{cec}$.

Ahora demostraremos que $I^e = I^{ece}$. Por inciso (i) tenemos que $I \subseteq I^{ec}$, por lo tanto $f(I) \subseteq f(I^{ec})$, de donde obtenemos que $Bf(I) \subseteq Bf(I^{ec})$. Por lo tanto $I^e \subseteq I^{ece}$. Por otra parte tenemos que $I^e \subseteq B$ y por inciso (i) tenemos que $(I^e)^{ce} \subseteq I^e$, es decir $I^{ece} \subseteq I^e$, por lo tanto $I^e \subseteq I^{ece} \subseteq I^e$, así obtenemos que $I^e = I^{ece}$.

iii) Sabemos que $f^{-1}(J_1 \cap J_2) = f^{-1}(J_1) \cap f^{-1}(J_2)$. Por lo tanto $(J_1 \cap J_2)^c = J_1^c \cap J_2^c$. ■

1.5. Módulos

En esta subsección A denota un anillo no necesariamente conmutativo.

Definición 1.5.1. *Un $A-$módulo izquierdo consiste en un grupo abeliano M y una operación $A \times M \to M$ denotada $(a, x) \to ax$ tal que*

1) $a(x + y) = ax + ay$

2) $(a + b)x = ax + bx$

3) $(ab)x = a(bx)$

4) $1x = x$

Si en lugar de (3) se cumple 3′) $x(ab) = (ax)b$ se dice que M es un $A-$módulo derecho.

Si A es un anillo conmutativo, las condiciones (3) y (3′) coinciden y, por tanto, todo módulo izquierdo es derecho. Si A es un campo, M se llama un espacio vectorial.

Se denotará con 0 el módulo cuyo grupo es trivial.

Definición 1.5.2. *Sean M y N dos $A-$módulos. Una función $f : M \to N$ se llama un A-homomorfismo de M en N si:*

1) $f(x+y) = f(x) + f(y)$,

2) $f(ax) = af(x)$, $a \in A$, $x, y \in M$.

La transformación idéntica de M en M es un A-homomorfismo que se denotará con 1_M. Al conjunto de todos los A-homomorfismos de M en N se le denotará $Hom_A(M, N)$ y éste se vuelve un grupo abeliano si se define la operación con la fórmula $(f+g)(x) = f(x)+g(x)$, $(f, g \in Hom_A(M, N)$, $x \in M)$.

El cero de este grupo, es decir, la función que transforma todo elemento en 0 se denotará también con 0.

Si A es conmutativo, $Hom_A(M, N)$ se puede considerar como un $A-$*módulo* izquierdo, definiendo $(af)(x) = a(f(x))$, $(a \in A$, $f \in Hom_A(M, N)$, $x \in M)$.

En el caso no conmutativo af puede no ser un A-homomorfismo.

Definición 1.5.3. *Si $f : M \to N$ y $g : N \to P$ son A-homomorfismos, su composición $gf : M \to P$ lo es también.*

Note que la composición determina una aplicación
$Hom_A(M, N) \times Hom_A(N, P) \to Hom_A(M, P)$ tal que $(f, g) \to gf$ la cual es bilineal, es decir, $(g_1 + g_2)f = g_1f + g_2f$ y $g(f_1 + f_2) = gf_1 + gf_2$.

Si, además, A es conmutativo, la bilinealidad significa también que vale $g(af) = (ag)f = a(gf)$, donde $a \in A$.

Si $f \in Hom_A(M, N)$, se escribirá también $f : M \to N$. Por otra parte se tiene que $(fg)h = f(gh)$.
En el caso de que $M = N = P$ esta composición define una multiplicación en $Hom_A(M, M)$ con la cual este grupo resulta ser un anillo con elemento unitario 1_M.

Definición 1.5.4. *Un $A-$módulo N es un submódulo de un $A-$módulo M si*

1) *N es un subgrupo de M,*

2) *La inclusión de N en M es un A-homomorfismo.*

Si $f : M \to N$ es un A-homomorfismo de módulos, el *núcleo* de f denotado por $Kerf$ es el $A-$*submódulo* de M formado por los elementos $x \in M$ tales que $f(x) = 0$ y la imagen de f, denotada Imf es el $A-$*submódulo* de N que consta de los elementos $y \in N$ de la forma $y = f(x)$ con $x \in M$.

El homomorfismo $f : M \to N$ se llama monomorfismo (respectivamente epimorfismo), si f es una función inyectiva (respectivamente suprayectiva). Se dice que f es un isomorfismo si existe un A-homomorfismo $g : N \to M$ tal que $gf = 1_M$, $fg = 1_N$. Evidentemente f es un monomorfismo (respectivamente epimosrfismo) si y sólo si $Kerf = 0$ (respectivamente $Imf = N$). Un homomorfismo es isomorfismo si y sólo si es monomorfismo y epimorfismo.

Definición 1.5.5 *Una sucesión $M' \to^f M \to^g M''$ de A-homomorfismos de módulos se dice que es exacta si $Imf = Kerg$.*

Por ejemplo $f : M' \to M$ es monomorfismo si y sólo si la sucesión $0 \to M' \to M$ es exacta, en donde $0 \to M'$ es el único A-homomorfismo posible de 0 en M'. Análogamente $g : M \to M''$ es un epimorfismo si y sólo si la sucesión $M \to^g M'' \to 0$ es exacta, siendo $M'' \to 0$ el único posible A-homomorfismo de M'' en 0.

Una sucesión $M_1 \to^{f_1} M_2 \to^{f_2} ... \to^{f_n} M_{n+1}$ de A-homomorfismos de módulos es exacta si $Imf_i = Kerf_{i+1}$, $(1 \leq i \leq n)$.

1.6. Módulos cociente

La estructura de cociente que se estudia en anillos también es válida para módulos.

Definición 1.6.1. *Sea M un $A-$módulo y M' un submódulo de M. El módulo cociente M/M' de M con respecto a M' es el $A-$módulo cuyos elementos son las clases de equivalencia de M determinadas por la relación $x \sim y$ si $x - y \in M'$, con las operaciones inducidas por las de M.*

El A-homomorfismo $g : M \to M/M'$ definido por $g(x) = x + M' = \bar{x}$ la clase de equivalencia de x, es llamado proyección canónica.

Proposición 1.6.2. *Sea* $0 \to M' \to^f M \to^g M'' \to 0$ *una sucesión exacta de A-homomorfismos. Entonces, para cada A-homomorfismo* $h : M \to N$ *tal que* $hf = 0$*, existe un A-homomorfismo único* $\bar{h} : M'' \to N$ *tal que* $\bar{h}g = h$*.*

Demostración. Sea $y \in M''$; por ser g suprayectiva existe $x \in M$ tal que $y = g(x)$. Si también $y = g(x')$ se tiene que $g(x) = g(x')$, de donde $g(x - x') = 0$ y por ser la sucesión exacta $x - x' \in Imf$. Puesto que $hf = 0$, $h(x - x') = 0$, es decir, $h(x) = h(x')$. Esto demuestra que podemos definir la función $\bar{h} : M'' \to N$ con la formula $\bar{h}(y) = \bar{h}(g(x)) = h(x)$.

Ahora probaremos que esta función es un A-homomorfismo:

$\bar{h}(y_1 + y_2) = \bar{h}(g(x_1) + g(x_2)) = \bar{h}(g(x_1 + x_2)) = h(x_1 + x_2) = h(x_1) + h(x_2) = \bar{h}(y_1) + \bar{h}(y_2)$;

$\bar{h}(ay) = \bar{h}(ag(x)) = \bar{h}(g(ax)) = h(ax) = ah(x) = a\bar{h}(y)$.

Unicidad: Sean $\bar{h_1} : M'' \to N$, $\bar{h_2} : M'' \to N$ dos *A-homomorfismos* tales que $\bar{h_1}g = h$, $\bar{h_2}g = h$. Entonces, ya que g es epimorfismo resulta que $\bar{h_1} = \bar{h_2}$; en efecto, si $y \in M''$, $y = g(x)$ y se tiene $\bar{h_1}(y) = \bar{h_1}(g(x)) = \bar{h_2}(g(x)) = \bar{h_2}(y)$ con lo cual queda probada la unicidad de $\bar{h}$. ■

1.7. Teoremas de isomorfismos

Los teoremas de isomorfismos son tres resultados importantes que relacionan módulos y módulo cociente.

Teorema 1.7.1. *(Primer teorema de isomorfismo) Consideremos la sucesión exacta* $0 \to M' \to^i M \to^g M/M'$*, donde* i *es la inclusión y* g *la proyección canónica. Si* $h : M \to M''$ *es un epimorfismo con núcleo* M'*, entonces existe un isomorfismo* $f : M/M' \to M''$ *tal que* $fg = h$*.*

Demostracón. Por la Proposición 1.6.2, existen $f : M/M' \to M''$, $f' : M'' \to M/M'$ tales que $fg = h$ y $f'h = g$, de donde, $ff'h = h$ y $f'fg = g$. Pero como g y h son epimorfismos, se tiene que $f'f = 1_{M/M'}$ y $ff' = 1_{M''}$. ■

Note que si $(N_i)_{i\in I}$ es una familia de submódulos de $A - modulo\ M$, la intersección $\bigcap_{i\in I} N_i$ es un submódulo de M. Si S es un subconjunto de M, el submódulo generado por S es la intersección de todos los submódulos de

M que contienen a S. En particular $\sum_{i\in I} N_i$ denota el submódulo generado por la unión $\bigcup_{i\in I} N_i$. En el caso de dos submódulos, el generado por $N \cup N'$ se denota $N + N'$. En el caso de los elementos de $N + N'$ son de la forma $x + x'$ con $x \in N$ y $x' \in N'$.

Proposición 1.7.2. *(Segundo teorema de isomorfismo.) Si N y N' son submódulos de un $A-$ módulo M, entonces la composición de A-homomorfismos $N \to^f N + N' \to^g (N + N')/N'$ (donde f es la inclusión y g es la proyección canónica) es un epimorfismo con núcleo $N \cap N'$. Por lo tanto $N/(N \cap N') \cong (N + N')/N'$.*

Demostración. Sea $y \in (N + N')/N'$. Por ser g suprayectiva existen $x \in N$ y $x' \in N'$ tales que $y = g(x + x')$, de donde, $y = g(x) + g(x')$. Pero $g(x') = x' + N' = \bar{0}$. Por lo tanto $y = g(x)$ y como f es la inclusión entonces $y = g(f(x))$. Es decir, gf es suprayectiva. Ahora supongamos que $(gf)(x) = 0$, para $x \in N$. Como $(gf)(x) = g(f(x)) = f(x) + N' = 0$, entonces $f(x) \in N'$. Ya que f es la inclusión entonces $x = f(x) \in N'$. Por lo tanto $x \in N \cap N'$. Inversamente, si $x \in N \cap N'$, $(gf)(x) = 0$, ya que $f(x) \in N'$. ■

Ahora consideremos $0 \to M' \to^f M \to^g M'' \to 0$ una sucesión exacta de $A-$ *módulos*. Si N'' es un submódulo de M'', $g^{-1}(N'')$ es un submódulo de M y se tiene:

Proposición 17.3. *(Tercer teorema de isomorfismo.)*

a) *La correspondencia $N'' \to g^{-1}(N'')$ es un isomorfismo de la retícula de submódulos de M'' en la retícula de submódulos de M que contienen a M'.*

b) *Si N es un submódulo de M que contiene a M', entonces la composición de los epimorfismos canónicos $M \to M/M' \to (M/M')/(N/M')$ es un epimorfismo con núcleo N. Por tanto $M/N \cong (M/M')/(N/M')$.*

Note que: a) Significa que la correspondencia es biyectiva y conserva las inclusiones.

b) Es consecuencia de los teoremas de isomorfismo.

1.8. Productos y sumas directas

En esta sección para una familia de A-módulos vámos a definir el producto y la suma directa.

Definición 1.8.1. *Sea $\{M_\alpha\}_{\alpha\in I}$ una familia de $A-$módulos izquierdos. El producto directo $\prod M_\alpha$ $(\alpha \in I)$ de la familia $\{M_\alpha\}$ es el $A-$módulo izquierdo cuyos elementos son las funciones $u : I \to \bigcup M_\alpha$ $(\alpha \in I)$ tales que $u(\alpha) \in M_\alpha$ (es decir, los elementos del producto cartesiano) con las operaciones:*

i) $(u + v)(\alpha) = u(\alpha) + v(\alpha)$,

ii) $(au)(\alpha) = au(\alpha)$ $(u, v \in M,\ a \in A,\ \alpha \in I)$.

Para cada α se tiene el A-homomorfismo $\rho_\alpha : \prod M_\alpha \to M_\alpha$ es llamado *proyección*, definido por $\rho_\alpha(u) = u(\alpha)$.

Proposición 1.8.2. *(Propiedad universal del producto directo.) Para cada $A-$módulo N y cada familia $f_\alpha : N \to M_\alpha$ $(\alpha \in I)$ de A-homomorfismos existe un A-homomorfismo único $f : N \to \prod M_\alpha$ tal que $\rho_\alpha f = f_\alpha$.*

Demostración. La función $f : N \to \prod M_\alpha$ definida por $f(x)(\alpha) = f_\alpha(x)$ $x \in N$, $\alpha \in I$ es un A-homomorfismo:

i) $f(x + y)(\alpha) = f_\alpha(x + y) = f_\alpha(x) + f_\alpha(y) = f(x)(\alpha) + f(y)(\alpha) = (f(x) + f(y))(\alpha)$,

ii) $f(ax)(\alpha) = f_\alpha(ax) = af_\alpha(x) = a(f(x)(\alpha)) = (af(x))(\alpha)$.

Además $(\rho_\alpha f)(x) = \rho_\alpha(f(x)) = f(x)(\alpha) = f_\alpha(x)$, o sea, $\rho_\alpha f = f_\alpha$ para cada α.

Ahora probaremos la unicidad de f. Sea $g : N \to \Pi M_\alpha$ tal que $\rho_\alpha g = f_\alpha$ entonces, $g(x)(\alpha) = \rho_\alpha(g(x)) = f_\alpha(x) = \rho_\alpha(f(x)) = f(x)(\alpha)$, de donde $g(x) = f(x)$. ■

La propiedad universal del producto directo suele expresarse diciendo que para definir un homomorfismo en un producto directo basta definir homomorfismos en sus factores.

Proposición 1.8.3. *La propiedad universal caracteriza al producto di-*

recto.

Demostración. Sea M' un módulo y $\rho'_\alpha : M' \to M_\alpha$ homomorfismos tales que para todo módulo N y toda familia de homomorfismos $g_\alpha : N \to M_\alpha$ existe un homomorfismo $g : N \to M'$ único tal que $\rho'_\alpha g = g_\alpha$.

Según la propiedad universal de ΠM_α y las hipótesis sobre M' existen entonces $h : M' \to \Pi M_\alpha$ y $h' : \Pi M_\alpha \to M'$ tales que $\rho_\alpha h = \rho'_\alpha$ y $\rho'_\alpha h' = \rho_\alpha$, de donde, $\rho_\alpha hh' = \rho_\alpha = \rho_\alpha 1_{M'}$ y $\rho'_\alpha h'h = \rho'_\alpha = \rho'_\alpha 1_M$. De acuerdo con las unicidades, $hh' = 1_M$ y $h'h = 1_{M'}$ por lo cual M' y $\prod M_\alpha$ son isomorfos. ■

Definición 1.8.4. *La suma directa $M = \bigoplus M_\alpha$ $(\alpha \in I)$ de la familia $\{M_\alpha\}$ es el $A-$submódulo de $\prod M_\alpha$ cuyos elementos son las funciones $u : I \to \bigcup M_\alpha$ tales que para todo α excepto un número finito de ellos $u(\alpha) = 0$.*

En este caso, para cada α existe un A-homomorfismo $i_\alpha : M_\alpha \to \bigoplus M_\alpha$ llamado *inclusión* dado por $i_\alpha(x_\alpha)(\beta) = 0$ si $\beta \neq \alpha$, $i_\alpha(x_\alpha)(\beta) = x_\alpha$, si $\beta = \alpha$, $(\alpha, \beta \in I,\ x_\alpha \in M_\alpha)$.

Nótese que si el conjunto de indices I es finito, la suma, directa coincide con el producto directo.

La notación en estos casos será $M_1 \times M_2 \times ... \times M_n$, o $M_1 \bigoplus M_2 \bigoplus ... \bigoplus M_n$.

Proposición 1.8.5 *(Propiedad universal de la suma directa) Para cada $A-$módulo N y cada familia de homomorfismos $v_\alpha : M_\alpha \to N$ $(\alpha \in I)$ existe un homomorfismo $v : \bigoplus M_\alpha \to N$ único tal que $vi_\alpha = f_\alpha$.*

Demostración. Para $f = (f_\alpha) \in \bigoplus_{\alpha \in I} M_\alpha$ se define v de la siguiente manera: $v(f) = 0$ si $f = 0$ y $v(f) = \sum_{j \in I_f} v_j(f_j)$ si $f \neq 0$. Afirmación v es un A-homomorfismo. En efecto, sean $f = (f_\alpha)$, $g = (g_\alpha) \in \bigoplus_{\alpha \in I} M_\alpha$. Si $f = 0$ o $g = 0$, entonces se tiene que $v(f+g) = v(f)+v(g)$. Supongamos que $f \neq 0$ y $g \neq 0$ y sea $h = (h_\alpha) = f+g$. Si $h = 0$, entonces $g_\alpha = -f_\alpha$ para cada $\alpha \in I$ y entonces se tiene $v(h) = 0 = \sum_{j \in I} v_j(f_j) + \sum_{j \in I} v_j(g_j) = v(f) + v(g)$. Si $h \neq 0$, entonces $v(h) = \sum_{j \in I} v_j(h_j) = \sum_{j \in I} v_j(f_j + g_j) = \sum_{j \in I} v_j(f_j) + \sum_{j \in I} v_j(g_j) = v(f) + v(g)$. De manera análoga se prueba que para $f \in \bigoplus_{\alpha \in I} M_\alpha$, $a \in A$ y $b \in N$, $v(fa) = v(f)a$ y $v(bf) = bv(f)$. sea ahora $m \in M_j$, entonces $vi_j(m) = v(f)$, donde $f = (f_\alpha)$ con $f_j = m$ y $f_\alpha = 0$ para $\alpha \neq j$. De aquí resulta que $v(f) = v_j(f_j)$, es decir, $vi_j = v_j$, para cada $j \in I$.

Probemos ahora la unicidad del homomorfismo v. Sea v' un

$A-homomorfismo$ de $\bigoplus_{\alpha\in I} M_\alpha$ en M tal que $v'i_\alpha = v_\alpha$ para cada $\alpha \in I$ y $f = (f_\alpha) \in \bigoplus_{\alpha\in I} M_\alpha$. Si $f = 0$, entonces $v'(f) = v(f)$. Si $f \neq 0$, entonces $v'(f) = \sum_{j\in I} v'_j(f_j) = \sum_{j\in I}(v'_j i)(f_j) = \sum_{j\in I} v_j(f_j) = v(f)$. ■

La propiedad universal de la suma directa se expresa diciendo que para definir un homomorfismo desde una suma directa, basta definirla desde cada uno de los sumandos.

Proposición 1.8.6. *Sea $M_1, ..., M_n$ una familia de submódulos de un $A-$módulo M. Entonces se cumplen las condiciones:*

1) $M_1 + ... + M_n = M$,

2) $M_k \cap (M_1 + ... + M_{k-1} + M_{k+1} + ... + M_n) = 0$, $(1 \leq k \leq n)$,

si y solamente si el homomorfismo de la suma directa $M_1 \bigoplus ... \bigoplus M_n \to M$ que determina las inclusiones $M_i \to M$ es un isomorfismo.

Demostración. $\Rightarrow$) Usando la propiedad universal de la suma directa. En efecto si llamamos θ_i a la composición del isomorfismo de $M_i \to M_i$ con la inclusión de $M_i \to M$ tenemos que existe un único homomorfismo $\theta : \bigoplus_{i\in I} M_i \to M$ tal que $\theta((x_i)_{i\in I}) = \sum_{i\in I} \theta(x_i)$.
Ahora como tenemos que $\theta(M_i) = M_i$ y por hipótesis tenemos que $M = M_1, ..., M_n$, entonces tenemos que θ es sobre. Además si $\theta((x_i)_{i\in I}) = 0$, entonces $\theta_i(x_i) = 0$ para todo i. Por lo tanto como θ_i es un isomorfismo entonces θ es inyectiva.

$\Leftarrow$) Por hipótesis se tiene que $M_1 \bigoplus ... \bigoplus M_n \to M$ es un isomorfismo, entonces si $x \in M_k \cap (M_1 + ... + M_{k-1} + M_{k+1} + ... + M_n)$ podemos escribir a $x = \sum_{i\in I} m'_i$, donde $m_j = x$ y $m'_i = 0$ para todo $i \neq j$, pero además $x = \sum_{i\in I} m''_i$ con $m''_j = 0$ y $m''_i \in M_i$ para todo $i \neq j$. Por lo tanto se tiene que $x = m''_j = m'_j = 0$.
Por ultimo como tenemos que $m \cong \bigoplus_{i=1}^n M_i$, entonces cada $m \in M$ se puede escribir de manera única de la forma $m = m_1, ..., m_n$. por lo tanto $M = M_1 + ... + M_n$. ■

Bajo las hipótesis de la proposición anterior, cada elemento x de M puede escribirse en forma única como $x = x_1 + ... + x_n$, con $x_k \in M_k$.

Podemos entonces definir los A-endomorfismos $p_k : M \to M$ $(1 \leq k \leq n$, haciendo $p_k(x) = x_k$. Estos endomorfismos tienen las tres propiedades siguientes:

1) $p_j p_k = 0$ si $j \neq k$,

2) $p_k p_k = p_k$,

3) $p_1 + ... + p_n = 1_M$.

Definición 1.8.7. *Se dice que la sucesión exacta de $A-$ módulos $0 \to M' \to^f M \to^g M'' \to 0$ se escinde si existe un $A-$ homomorfismo $h : M'' \to M$ tal que $gh = 1_{M''}$.*

Por ejemplo, si $M = M' \bigoplus M''$ es una suma directa de $A-$ *módulos*, la sucesión exacta $0 \to M' \to^{i'} M' \bigoplus M'' \to^{p''} M'' \to 0$ (en donde i' es la inclusión y p'' la proyección respectivas) se escinde, ya que la inclusión $i'' : M'' \to M$ es un $A-homomorfismo$ tal que $p''i'' = 1_{M''}$. Inversamente, es valida la

Proposición 1.8.8. *Si $0 \to M' \to^f M \to^g M'' \to 0$ es una sucesión exacta que se escinde y $h : M'' \to M$ es el morfismo tal que $gh = 1_{M''}$, entonces los morfismos $h : M'' \to M$, $f : M' \to M$ inducen un isomorfismo $M' \bigoplus M'' \to M$ dado por $(x, y) \to f(x) + h(y)$.*

Demostración. Sea $x \in M'$ y $y \in M''$ tal que $f(x) + h(y) = 0$, entonces se tiene que $0 = gf(x) + gh(y) = y$. Por tanto, $f(x) = 0$, de donde $x = 0$. Sea ahora $z \in M$. Tenemos que $z = z - hg(z) + hg(z)$. Pero $g(z - hg(z)) = g(z) - gh(g(z)) = g(z) - g(z) = 0$ y según la exactitud $z - hg(z) = f(x)$ para cierta $x \in M'$. Por lo tanto, $z = f(x) + h(y)$ con $y = g(z)$. ■

1.9. Anillos de fracciones

En álgebra conmutativa es importante el concepto de anillo de fracciones que es una generalización del concepto de campo de fracciones.

Definición 1.9.1 *Sea A un anillo conmutativo con 1. Un subconjunto multiplicativamente cerrado de A, es un subconjunto S de A tal que $1 \in S$ y S es cerrado respecto a la multiplicación: en otras palabras, S es un subsemigrupo del semigrupo multiplicativo de A.*

Definimos una relación $\equiv$ en $A \times S$ como sigue:

$(a, s) \equiv (b, t) \Leftrightarrow (at - bs)u = 0$ para algún $u \in S$.

Proposición 1.9.2 *Si A es un anillo conmutativo con 1 y S es un conjunto multiplicativamente cerrado de A, entonces la relación $\equiv$ es de equivalencia.*

Demostración. (Reflexiva) Hay que probar que $(a, s) \equiv (a, s)$, pero dado $u \in S$ tenemos que $(as - as)u = 0u = 0$, así se prueba que es reflexiva.

(Simetría) Es claro que si $(a, s) \equiv (b, t)$ entonces $(b, t) \equiv (a, s)$

(Transitividad) Para probar que es transitiva, supongamos que $(a, s) \equiv (b, t)$ y $(b, t) \equiv (c, u)$. Entonces existen $v, w \in S$ tales que $(at - bs)v = 0$ y $(bu - ct)w = 0$. Multiplicando la primera ecuación por uw y a la segunda por sv y sumandolas se tiene que $(au - cs)tvw = 0$. Ya que S es cerrado respecto a la multiplicación, se tiene $tvw \in S$, por lo tanto $(a, s) \equiv (c, u)$. Así se tiene una relación de equivalencia. ■

Denotamos por a/s a la clase de equivalencia de (a, s), y por $S^{-1}A$ el conjunto de la clases de equivalencia. Se da una estructura de anillo a $S^{-1}A$ definiendo una adición y una multiplicación de estas fracciones de la misma manera que en el álgebra elemental, es decir:

1) $(a/s) + (b/t) = (at + bs)/st$,

2) $(a/s)(b/t) = ab/st$.

El anillo $S^{-1}A$ se denomina el *anillo de fracciones* de A con respecto a S. Además $S^{-1}A$ es anillo conmutativo con 1.

Note que $S^{-1}A$ es anillo cero $\Leftrightarrow 0 \in S$.

Note además que tenemos un morfismo natural de anillos $f : A \longrightarrow S^{-1}A$ definido por $f(a) = a/1$. Si además A es dominio entero y $S = A - \{0\}$, entonces $S^{-1}A$ es el campo de fracciones de A.

Ejemplo: 1.9.3. Sea P un ideal primo de un anillo A, entonces $S = A - P$ es multiplicativamente cerrado (de hecho $A - P$ es multiplicativamente cerrado si y solo sí P es primo). Escribimos A_P en lugar de $S^{-1}A$ para este caso. Los elementos de la forma a/s con $a \in P$ forman un ideal M en A_P. Si $b/t \notin M$ entonces $b \notin P$, por lo tanto $b \in S$ y además b/t es una unidad en A_P. Resulta que si a es un ideal en A_P y $a \nsubseteq M$, entonces a contiene

una unida y es por lo tanto todo el anillo. Por lo tanto M es el único ideal máximo en A_P.

La construcción de $S^{-1}A$ puede llevarse a cabo utilizando $A-$*módulos* en lugar del anillo A, de la siguiente forma.

Sea M un $A-$*módulo*, definimos la relación $\equiv$ en el conjunto $M \times S$, diremos que $(m,s) \equiv (m',s') \Leftrightarrow \exists t \in S$ tal que $t(sm'-s'm)=0$, donde este $0 \in M$.

De forma completamente análoga como en el caso del anillo A tenemos que $\equiv$ es una relación de equivalencia en $M \times S$.

Nuevamente denotamos por m/s a la clase de equivalencia de (m,s) y $S^{-1}M$ el conjunto de clases de equivalencia.

Ahora demostraremos que $S^{-1}M$ es un $S^{-1}A-$*módulo* con las siguientes operaciones:

$1)(m/s)+(m'/s')=(s'm+sm')/ss'$

$2)(\alpha/\sigma)(m/s)=(\alpha m/\sigma s)$, donde $(\alpha/\sigma) \in S^{-1}A$.

Primero probaremos que la suma no depende de los representantes.

Supongamos que $m/s = x/y$ y $m'/s' = x'/y'$. Por lo tanto $(x/y) + (x'/y') = (y'x+yx'/yy'$. Ahora debemos probar que las clases de equivalencia $(s'm+sm'/ss'$ y $(y'x+yx'/yy'$ son iguales, es decir debemos probar que $(s'm+sm')/ss' = (y'x+yx'/yy'$. Así lo que debemos probar es que existe $t \in S$, tal que $t(ss'(y'x+yx')-yy'(s'm+sm'))=0$.

En efecto tenemos que $t(ss'(y'x+yx')-yy'(s'm+sm')) =$
$t(ss'(y'x+yx')-yy'(s'm+sm')) = t(ss'y'x+ss'yx'-yy's'm-yy'sm') =$
$t(ss'y'x-yy's'm+ss'yx'-yy'sm') = t(s'y'(sx-ym)+sy(s'x'-y'm'))$.

Por otra parte sabemos que $m/s = x/y$ y $m'/s' = x'/y'$, entonces existe t_1 y t_2 tal que $t_1(sx-ym)=0$ y $t_2(s'x'-y'm'=0$. Por lo tanto si tomamos $t=t_1t_2$, tenemos que $t(s'y'(sx-ym)+sy(s'x'-y'm')) =$
$t_1t_2(s'y'(sx-ym)+sy(s'x'-y'm')) = (t_1t_2s'y'(sx-ym)+t_1t_2sy(s'x'-y'm')) =$
$(t_2s'y'[t_1(sx-ym)]+t_1sy[t_2(s'x'-y'm')])=0$.
Así hemos probado que la suma esta bien definida.

Ahora probaremos que el producto no depende de los representantes y lo haremos en dos casos.

Primer caso.
Supongamos que, si $\alpha/\sigma = a/s$ (en $S^{-1}A$) y $m'/s' \in S^{-1}M$, entonces debemos probar que $\alpha m'/\sigma s' = am'/ss'$. Así debemos probar que existe $t \in S$ tal que $t(\sigma s'am' - ss'\alpha m') = 0$.

En efecto tenemos que $t(\sigma s'am' - ss'\alpha m') = t(s'(\sigma a - s\alpha)m')$.

Por otra parte sabemos que $\alpha/\sigma = a/s$, por lo tanto existe $t_1 \in S$ tal que $t_1(s\alpha - \sigma a) = 0$. Por lo tanto si tomamos $t = -t_1$, tenemos que $t(\sigma s'am' - ss'\alpha m') = -t_1(s'(\sigma a - s\alpha)m') = s'(t_1(s\alpha - \sigma a)m') = 0$.

Segundo caso.
Supongamos que si $m'/s' = m''/s''$ (en $S^{-1}M$) y $\alpha/\sigma \in S^{-1}A$, entonces debemos probar que $(\alpha/\sigma)(m'/s') = (\alpha/\sigma)(m''/s'')$. Pero esta demostración es completamente análoga a la prueba del primer caso. Así hemos demostrado que el producto de elementos del anillo $S^{-1}A$ por elementos de $S^{-1}M$ esta bien definido.

Ahora procederemos a demostrar que $S^{-1}M$ es un módulo sobre el anillo de fracciones $S^{-1}A$.

i) $0/s$ es el elemento neutro para cualquier $s \in S$
Vamos a demostrar que para todo $m/s \in S^{-1}M$ se tiene que $(0/s)+(m/s) = m/s$. Es decir $(0/s) + (m/s) = (s0 + sm)/ss = m/s$, entonces debemos probar que existe $t \in S$ tal que $t(s(sm) - ss(m)) = 0$. Pero $t(s(sm) - ss(m)) = t(s(sm - sm)) = t(0) = 0$. pro lo tanto para cualquier $t \in S$ se tiene lo que de quiere probar.

ii) Para todo $m/s \in S^{-1}M$ existe $(-m)/s \in S^{-1}M$ tal que $(m/s) + (-m/s) = 0/s$.
Tenemos que $(m/s) + (-m/s) = (sm + s(-m))/ss = 0/s$, por lo que tenemos que probar que existe $t \in S$ tal que $t(s(sm+s(-m)) - ss(0)) = 0$, pero tenemos que $t(s(sm+s(-m)) = t(s(s(m-m) - ss(0)) = t(s(0)) = t(0) = 0$ por lo tanto para cualquier $t \in S$ se tiene lo que se quiere demostrar.

iii) Asociatividad de la suma, $(m/s) + [(m'/s') + (m''/s'')] = [(m/s) + (m'/s')] + (m''/s'')$.
Por un lado tenemos que $(m/s) + [(m'/s') + (m''/s'')] = (m/s) + [m's'' +$

$m's''/s's''] = (s's''m + s[m's'' + m's'']/ss's'')$ y $[(m/s) + (m'/s')] + (m''/s'') = [ms' + m's/ss'] + (m''/s'') = (s''[ms' + m's] + ss'm''/ss's'')$, entonces hay que demostrar que $(s's''m + s[m's'' + m's'']/ss's'') = (s''[ms' + m's] + ss'm''/ss's'')$ es decir hay que demostrar que existe $t \in S$ tal que $t(ss's''(s's''m + s[m's'' + m's'']) - ss's''((s''[ms' + m's] + ss'm'')) = 0$

Pero $t(ss's''(s's''m + s[m's'' + m's'']) - ss's''((s''[ms' + m's] + ss'm'')) = t(ss's''(s's''m + sm's'' + sm's'' - s's''m + sm's'' + sm's'')) = t(ss's''(0)) = t(0) = 0$. Por lo tanto para cualquier $t \in S$ se tiene lo que se quería probar.

iv) Conmutatividad, $(m/s) + (m'/s') = (m'/s') + (m/s)$.
Hay que demostrar que $(s'm + sm')/ss' = (sm' + s'm)/s's$. Es decir tenemos que probar que existe $t \in S$ tal que $t(s's[s'm + sm'] - ss'[sm' + s'm]) = 0$. Pero tenemos que $t(s's[s'm + sm'] - ss'[sm' + s'm]) = t([s'm + sm'](ss' - s's)) = t([s'm + sm'](0)) = t(0) = 0$. Por lo tanto se tiene que para cualquier $t \in S$ $t(s's[s'm + sm'] - ss'[sm' + s'm]) = 0$.

v) El producto distribuye a la suma, $(\alpha/\sigma)[(m/s) + (m'/s')] = (\alpha/\sigma)(m/s) + (\alpha/\sigma)(m'/s')$.
Vamos a demostrar que:
$(\alpha[s'm + sm'])/ss'\sigma = [(\sigma s')(\alpha m) + (\sigma s)(\alpha m')]/\sigma s\sigma s']$. Es decir que existe $t \in S$ tal que
$t([\sigma s\sigma s'][(\alpha(s'm + sm'))] - [\sigma ss'][(\sigma s')(\alpha m) + (\sigma s)(\alpha m')]) = 0$, pero tenemos que
$t([\sigma s\sigma s'][(\alpha(s'm + sm'))] - [\sigma ss'][(\sigma s')(\alpha m) + (\sigma s)(\alpha m')]) =$
$t([\sigma s\sigma s'][\alpha s'm + \alpha sm'] - [\sigma ss'][\sigma s'\alpha m + \sigma s\alpha m'] =$
$t([\sigma ss'][\sigma s'\alpha m + \sigma s\alpha m'] - [\sigma ss'][\sigma s'\alpha m + \sigma s\alpha m']) = t(0) = 0$. Por lo tanto se tiene que para cualquier t, $t([\sigma s\sigma s'][(\alpha(s'm + sm'))] - [\sigma ss'][(\sigma s')(\alpha m) + (\sigma s)(\alpha m')]) = 0$.
Para el caso $[(\alpha/\sigma) + (\alpha'/\sigma')](m/s) = (\alpha/\sigma)(m/s) + (\alpha'/\sigma')(m/s)$ es análoga a la demsotración anterior.

vi) Asociatividad del producto,
$[(\alpha/\sigma)(\alpha'/\sigma')](m/s) = (\alpha/\sigma)[(\alpha'/\sigma')(m/s)]$.

Se tiene que probar que $[\alpha\alpha']m/[\sigma\sigma']s = \alpha[\alpha'm]/\sigma[\sigma's]$. Por demostrar que existe $t \in S$ tal que $t((\sigma[\sigma's])([\alpha\alpha']m) - ([\sigma\sigma']s)(\alpha[\alpha'm)) = 0$. Pero tenemos que
$t((\sigma[\sigma's])([\alpha\alpha']m) - ([\sigma\sigma']s)(\alpha[\alpha'm)) = t((\sigma[\sigma's])([\alpha\alpha']m) - (\sigma[\sigma's])([\alpha\alpha']m))$
$= t(0) = 0$. Entonces se tiene que dada cualquier $t \in S$, $t((\sigma[\sigma's])([\alpha\alpha']m) - ([\sigma\sigma']s)(\alpha[\alpha'm)) = 0$. Por lo tanto se tiene la igualdad que se quería.

vii) Multiplicar por el $1 = (s/s) \in S^{-1}A$ por los elementos de $S^{-1}M$, es decir $(s/s)(m/s) = (m/s)$.
Tenemos que demostrar que $(sm/ss) = (m/s)$, es decir que existe $t \in S$ tal que $t(s[sm] - ss[m]) = 0$. Pero es obvio que $t(s[sm] - ss[m]) = t(ssm - ssm) = t(0)$. Por lo tanto dada cualquier $t \in S$ se tiene lo que se quería demostrar.

Proposición 1.9.4. *Sea A anillo conmutativo con 1 y S un conjunto multiplicativamente cerrado. Si $f : A \to S^{-1}A$ es el morfismo de anillos tal que $f(a) = a/1$ e I es un ideal de A, entonces su extensión I^e en $S^{-1}A$ es $S^{-1}I$.*

Demostración. Sabemos que $I^e = (S^{-1}A)f(I)$, entonces cada elemento $x \in I^e$ es de la forma
$x = (\sum_{i=1}^{n} \alpha_i/s_i)(\sum_{j=1}^{m} f(x_j)) = (\sum_{i=1}^{n} \alpha_i/s_i)(\sum_{j=1}^{m} x_j/1)$. Por lo tanto el elemento x es de la forma $x = \sum_{k=1}^{r}(\alpha_k x_k)/s_k$, donde $\alpha_k \in A$, $x_k \in I$, $s_k \in S$. Por otra parte sabemos que los elementos de $S^{-1}I$ son de esta misma forma. Así tenemos que $I^e = S^{-1}I$. ■

Proposición 1.9.5. *Sea A un anillo conmutativo con 1 y S un conjunto multiplicativamente cerrado. Si $f : A \to S^{-1}A$ es el morfismo de anillos tal que $f(a) = a/1$, entonces:*

i) Cada ideal J en $S^{-1}A$ es un ideal extendido.

ii) Si I es un ideal en A entonces $I^{ec} = \bigcup_{s\in S}(I : s)$. Además $I^e = A$ si y solo si $I \cap S \neq \emptyset$.

iii) El operador S^{-1} conmuta con intersecciones y radicales.

Demostración. *i)* Sea J un ideal en $S^{-1}A$, y sea $x/s \in J$. Como $s/1 \in S^{-1}A$ y J es ideal, entonces $(x/s)(s/1) = x/1 \in J$. Por lo tanto $x \in J^c$. Ya que $J^{ce} = S^{-1}A(f(J^e))$, entonces $x/s \in J^{ce}$. Así hemos probado que $J \subseteq J^{ce}$. Por el inciso (i) de la Proposición 1.4.3 tenemos que $J^{ec} \subseteq J$. Por lo tanto $J^{ec} = J$, es decir J es el ideal extendido de J^c.

ii) Por la Proposición 1.9.2 sabemos que $I^e = S^{-1}A$. Por lo tanto $x \in I^{ec} \Leftrightarrow x \in (S^{-1}A)^c$. Así $f(x) = x/1 \in S^{-1}A \Leftrightarrow x/1 = r/s$ para algún $r \in I, s \in S \Leftrightarrow (sx-r)t = 0$ para algún $t \in S \Leftrightarrow xts \in I \Leftrightarrow x \in \bigcup_{s\in S}(I : s)$. Ahora si $I^e = S^{-1}A$ entonces $I^{ec} = A$. Por lo tanto $1 \in I^{ec} = \bigcup_{s\in S}(I : s)$. Así existe $s \in S$ tal que $1 \in (I : s)$ de donde $s \in I$. Por lo tanto $I \cap S \neq \emptyset$. Ahora probaremos el inverso. Sea $s \in i \cap S$, entonces $I^e = (S^{-1}A)f(I)$.

Como $s \in I$, entonces $f(s) = s/1$ y si tomamos $1/s \in S^{-1}A$, tenemos que $(1/s)(s/1) = s/s = 1/1 \in S^{-1}A$. Por lo tanto $I^e = (S^{-1}A)f(I) = S^{-1}A$.

iii) Primero demostraremos que $S^{-1}r(I) \subseteq r(S^{-1}I)$. Sea $x/s \in S^{-1}r(I)$, entonces $x \in r(I)$ y $s \in S$. Por lo tanto existe $n > 0$ tal que $x^n \in I$. Como $s \in S$, entonces $x^n/s \in S^{-1}I$. Como $S^{-1}I$ es ideal de $S^{-1}A$ entonces $(x^n/s)(1/s^{n-1}) = x^n/s^n \in S^{-1}I$. Por lo tanto $(x/s)^n \in S^{-1}I$. Así tenemos que $x/s \in r(S^{-1}I)$.

Ahora demostraremos que $r(S^{-1}I) \subseteq S^{-1}r(I)$. Sea $x/s \in r(S^{-1}I)$ entonces existe $n > 0$ tal que $(x/s)^n \in S^{-1}I$. Por lo tanto $x^n/s^n \in S^{-1}I$. Como $S^{-1}I$ es ideal de $S^{-1}A$, entonces $(x^n/s^n)(s^{n-1}/1) = x^n/s \in S^{-1}I$. Así obtenemos que $x^n \in I$. Por lo tanto $x \in r(I)$. De donde $x/s \in S^{-1}r(I)$.

Para el caso de la intersección lo probaremos sólo para cuando tenemos dos ideales, se extiende fácilmente si tienen más. Dados I, J dos ideales en A, probaremos que $S^{-1}(I \cap J) = (S^{-1}I) \cap (S^{-1}J)$. Si $x/s = y/t$ donde $x \in I$, $y \in J$ y $s, t \in S$, entonces $u(tx - sy) = 0$ para algún $u \in S$, por lo tanto $w = utx = usy \in I \cap J$, y por tanto $x/s = w/stu \in S^{-1}(I \cap J)$. En consecuencia $S^{-1}I \cap S^{-1}J \subseteq S^{-1}(I \cap J)$. La otra contención es clara. ■

Capítulo 2

Descomposición Primaria

2.1. Descomposición Primaria de ideales

En esta sección A denotara un anillo conmutativo con uno.

La descomposición de un ideal en ideales primarios es un pilar tradicional dentro de la teoría de ideales. Esto proporciona la fundamentación algebraica para la descomposición de una variedad algebraica en sus componentes irreducibles. Otro punto que aborda la descomposición primaria es la generalización de la factorización de un número entero en su producto de potencias de primos.

Definición 2.1.1 *Un ideal Q en un anillo A es primario si $Q \neq A$ y si $xy \in Q \Rightarrow x \in Q$ o $y^n \in Q$ para algún entero $n > 0$. Equivalentemente si $x \notin Q$ entonces $y^n \in Q$ para alguna $n > 0$.*

Note que un ideal primo es la generalización de un número primo.

Proposición 2.1.2. *Q es primario $\Leftrightarrow$ $A/Q \neq 0$ y todo divisor de cero en A/Q es nilpotente.*

Demostración. $\Rightarrow$) Si Q es primario entonces $A/Q \neq 0$. Ahora sea $z+Q \in A/Q$ un divisor de cero, entonces existe $w+Q \in A/Q$ y $w \notin Q$, tal que $(z+Q)(w+Q) = Q$, y $(z+Q)(w+Q) = zw+Q = Q$. Así tenemos que $zw \in Q$. Como Q es primario sabemos que $w \notin Q$, entonces existe un entero $n > 0$ tal que $z^n \in Q$.
Por lo tanto, $Q = z^n + Q = (z+Q)^n$; lo que prueba que $z+Q$ es nilpotente.

$\Leftarrow$) Supongamos que $A/Q \neq \emptyset$ y que todo divisor de cero en A/Q es nilpotente. Es claro que $Q \neq A$. Sean $x, y \in A$ tal que $xy \in Q$. Si x no

pertenece a Q, entonces $x+Q \neq Q$ y $(x+Q)(y+Q) = xy+Q = Q$. Por lo tanto $y+Q$ es un divisor de cero en A/Q. Por lo tanto $y+Q$ es nilpotente en A/Q. Así por hipótesis existe un entero $n > 0$ tal que $(y+Q)^n = y^n+Q = Q$ entonces $y^n \in Q$. Por lo tanto Q es primario. ■

Proposición 2.1.3. *Si A es un anillo y Q un ideal primo de A, entonces Q es primario.*

Demostración. Sea Q un ideal primo en un anillo A y sean $x, y \in A$ tal que $xy \in Q$ como Q es un ideal primo se tiene que $x \in Q$ o $y \in Q$. Ahora si $x \notin Q$ entonces $y \in Q$ es decir existe un entero $n = 1$ tal que $y^1 \in Q$ por lo tanto Q es primario. ■

Proposición 2.1.4. *La contracción de un ideal primario Q es primario.*

Demostración. Sea $f : A \longrightarrow B$ un morfismo de anillos y sea Q un ideal primario de B. Ahora sean $x, y \in A$ tal que $xy \in f^{-1}(Q)$ entonces,
$f(xy) = f(x)f(y) \in Q$.
Q es primario, entonces $f(x) \in Q$ o $[f(y)]^n \in Q$. Como f es un morfismo de anillos entonces $[f(y)]^n = f(y^n)$. De aquí tenemos que $f(y^n) \in Q$ para algún entero $n > 0$. Así $x \in f^{-1}(Q)$ o $y^n \in f^{-1}(Q)$. Por lo tanto $f^{-1}(Q)$ es primario. ■

Proposición 2.1.5. *Sea Q un ideal primario de un anillo A, entonces $r(Q)$ es el ideal primo mas pequeño que contiene a Q.*

Demostración. Sea Q un ideal primario de A, por el resultado de la Proposición 1.2.3 tenemos que $r(Q)$ es la intersección de todos los ideales primos que contienen a Q. Ahora demostraremos que $r(Q)$ es primo. Sean $x, y \in A$ tal que $xy \in r(Q)$, entonces existe $m \geq 1$ tal que $(xy)^m = x^m y^m \in Q$ pero como Q es primario se tiene que $x^m \in Q$ o $(y^m)^n \in Q$ para algún entero $n > 0$, entonces $x^m \in Q$ o $y^{mn} \in Q$ por lo que se tiene que $x \in r(Q)$ o $y \in r(Q)$. En consecuencia $r(Q)$ es primo. Así $r(Q)$ es el ideal primo mas pequeño que contiene a Q. ■

Definición 2.1.6. *Sea Q un ideal primario y P un ideal primo de un anillo A. Si $P = r(Q)$, entonces diremos que Q es $P-$primario.*

Ejemplos. 2.1.7.

1) Sea $\mathbf{Z}$ el anillo de los números enteros, entonces los ideales primarios de $\mathbf{Z}$ son $0\mathbf{Z}$ y $p^i\mathbf{Z}$, donde i es un número natural positivo y p es un número

primo.

Demostración *i*) El ideal cero $0\mathbf{Z}$ es ideal primo, entonces por la Proposición 2.1.3 tenemos que $0\mathbf{Z}$ es primario.

ii) Sea $m + p^i\mathbf{Z} \in \mathbf{Z}/p^i\mathbf{Z}$ un elemento divisor de cero tal que $m \notin p^i\mathbf{Z}$, entonces existe $k + p^i\mathbf{Z} \in \mathbf{Z}/p^i\mathbf{Z}$ con $k \notin p^i\mathbf{Z}$, tal que $(m + p^i\mathbf{Z})(k + p^i\mathbf{Z}) = mk + p^i\mathbf{Z} = p^i\mathbf{Z}$ por lo tanto se tiene que $mk \in p^i\mathbf{Z}$ es decir $mk = p^i a$ con $a \in \mathbf{Z}$.
Como $k \notin p^i\mathbf{Z}$, entonces $k \neq p^i z$ para toda $z \in \mathbf{Z}$. Ya que $p^i \mid mk$, de donde $m = p^j b$ y $k = p^l c$ con $0 < j < i$ y $0 < l < i$. Así existe un entero $s > 0$ tal que $sj > i$. De esta forma tenemos $(m)^s = (p^j b)^s = p^{sj} b^s$, entonces $(m + p^i\mathbf{Z})^s = m^s + p^i\mathbf{Z} = p^i\mathbf{Z}$ lo que implica que $m + p^i\mathbf{Z}$ es un elemento nilpotente de $\mathbf{Z}/p^i\mathbf{Z}$. Ahora por la Proposición 2.1.2 tenemos que $p^i\mathbf{Z}$ es primario.

Ahora sea Q un ideal primario de $\mathbf{Z}$, entonces $Q = m\mathbf{Z}$, para un entero $m > 1$. Supongamos que m no es una potencia de un número primo, entonces $m = p^i q$ donde p es un número primo, $q > 1$ es un entero que tal que $p \nmid q$ e $i > 0$.
Afirmamos que el elemento $p + m\mathbf{Z} \in \mathbf{Z}/Q$ es un divisor de cero. En efecto el elemento $p^{i-1}q + m\mathbf{Z} \neq \bar{0}$ y $(p + m\mathbf{Z})(p^{i-1}q + m\mathbf{Z}) = p^i q + m\mathbf{Z} = \bar{0}$. Ya que Q es primario entonces por la Proposición 2.1.2, tenemos que $p + m\mathbf{Z}$ es nilpotente en $\mathbf{Z}/Q$. Por lo tanto existe un entero $n > 0$ tal que $(p + m\mathbf{Z})^n = \bar{0}$. De donde tenemos que $p^n \in m\mathbf{Z}$. De aquí obtenemos que $m \mid p^n$, así existe $r \in \mathbf{Z}$ tal que $mr = p^n$. Esto implica que m es una potencia de p. Lo que es una contradicción.

2) Sea $A = F[x, y]$ con F un campo y sea $Q =< x, y^2 >= Ax + Ay^2 = (F[x, y])x + (F[x, y])y^2$. Definimos el siguiente morfismo $\Phi : A \to F[y]/F[y]y^2$ como $\Phi(p(x, y)) = p(0, y) + F[y]y^2$. Sabemos que $ker\Phi = \{p(x, y) \in A \mid \Phi(p(x, y)) \in F[y]y^2\} = \{p(x, y) \in A \mid p(0, y) \in F[y]y^2\}$.

Por otra parte claramente tenemos que x, y^2 pertenecen al kernel de Φ ya que $\Phi(x) = 0 + F[y]y^2 = F[y]y^2$ y $\Phi(y^2) = y^2 + F[y]y^2 = F[y]y^2$, De donde se tiene $Q \subseteq ker(\Phi)$.
Ahora si $p(x, y) \in ker(\Phi)$ entonces $p(x, y) = p_1(y) + xp_2(x, y)$ y aplicando el morfismo tenemos $\Phi(p(x, y)) = p_1(y) + 0p_2(0, y) + F[y]y^2 = p_1(y) + F[y]y^2 = F[y]y^2$ lo que implica que $p_1(y) \in F[y]y^2$ por lo tanto $p_1(y) \in F[y]$ y $p_2(x, y) \in F[x, y]$, entonces $xp_2(x, y) \in x(F[x, Y]) = F[x, y]x$. Así tenemos que $p(x, y) \in < x, y^2 >= Q$. Por lo que se tiene que $ker(\Phi) = Q$. De donde por el primer teorema de ismorfismos se tiene que $A/ker(\Phi) \cong Im(\Phi)$

es decir $A/Q \cong F[y]/F[y]y^2$. En consecuencia los divisores de cero son de la forma $ay + F[y]y^2$. Pero estos elementos son nilpotentes, entonces todos los divisores de cero de A/Q son nilpotntes por lo cual Q es primario.

Además note que el ideal $P =< x, y >= xA + yA$ es ideal primo y $P^2 \nsubseteq Q \nsubseteq P$. Es decir Q no es potencia de un ideal primo y si es primario.

3) Sea $A = F[x, y, z]$, donde F es un campo y tomamos $I = (xy - z^2)A, B = A/I, P =< x + I, z + I >= (x + I)B + (z + I)B$. Afirmación: P es un ideal primo de B, y P^2 no es primario.

Demostración. Sea $\phi : A \to F[y]$ tal que $\phi(p(x, y, z)) = p(0, y, 0)$, entonces ϕ es un morfismo de anillos.
Por otra parte $\phi(xy - z^2) = 0y - 0^2 = 0$ de donde $xy - z^2 \in ker(\phi)$. Como $I = (xy - z^2)A$, entonces se tiene que $I \subseteq ker(\phi)$. Se sigue que ϕ induce un morfismo de anillos $\varphi : B \longrightarrow F[y]$ donde $\varphi(p(x, y, z) + I) = \phi(p(x, y, z))$ es decir $\varphi(p(x, y, z)+I) = p(0, y, 0)$. Así tenemos que $\varphi(x+I) = 0, \varphi(z+I) = 0$, entonces $x + I, z + I \in ker\varphi$. En conclusión $P \subseteq ker\varphi$.

Ahora sea $p(x, y, z) + I \in ker(\varphi)$ y escribimos $p(x, y, z) = p_1(y) + xp_2(x, y)+zp_3(x, y, z)$ para algún $p_1(y) \in F[y], p_2(x, y) \in F[x, y], p_3(x, y, z) \in F[x, y, z]$. Ahora si $\bar{0} = \varphi(p(x, y, z)+I) = \phi(p(x, y, z)) = p(0, y, 0) = p_1(y)+ 0p_2(x, y) + 0p_3(x, y, z) = p_1(y)$, entonces $p_1(y) \in I = (xy - z^2)F[x, y, z]$. Por lo tanto $p_1(y) = 0$. Así obtenemos que $p(x, y, z) = 0 + xp_2(x, y) + zp_3(x, y, z) \in < x+I, z+I >$. Así tenemos que $p(x, y, z)+I \in < x+I, z+I >= P$. Por lo tanto $ker(\varphi) = P$. Entonces por el primer teorema de isomorfismos $B/ker(\varphi) \cong Im(\varphi)$. Así $B/P \cong F[y]$ por lo tanto B/P es un dominio entero ya que $F[y]$ lo es, lo cual prueba que P es un ideal primo.

Ahora demostraremos que P^2 no es primario. Observe que $(x + I)(y + I) = xy + I = xy - (xy - z^2) + I = z^2 + I = (z + I)^2 \in P^2$,. Por lo tanto $P^2 =< x^2 + I, xz + I, z^2 + I >$. Supongamos que P^2 es primario. Como $(x + I)(y + I) \in P^2$, entonces $x + I \in P^2$ o $y^k + I = (y + I)^k \in P^2$ para algún entero $k \geq 1$. Por lo tanto x o $y^k \in < x^2, xz, z^2, xy - z^2 >$ lo cual es imposible ya que $< x^2, xz, z^2, xy - z^2 >= \alpha x^2 + \beta xz + \gamma z^2 + \delta(xy - z^2)$ con α, β, γ, $\delta \in A$. Por lo tanto P^2 no es primario.

Porposición 2.1.8. *Sea Q un ideal de un anillo A y supongamos que $r(Q)$ es ideal máximo, entonces:*

i) Q es primario

ii) Si M es ideal máximo de A, entonces M^t es primario y M^t es $M-$primario para toda t un número natural.

Demostración. i) Supongamos que Q es un ideal de A, y sea $M = r(Q)$ tal que M es máximo. Por la Proposición 1.2.3 sabemos que M es la intersección de todos los idales primos de A que contienen a Q. Como M es ideal máximo, entonces por la Proposición 1.1.5 tenemos que M es ideal primo y por lo tanto M es el único ideal primo de A que contiene a Q.
Ahora por la correspondencia biyectiva tenemos que M/Q es el único ideal máximo (por lo tanto primo) de A/Q. Por el Corolario 1.1.7 tenemos que cualquier ideal propio de A/Q esta contenido en M/Q.

Afirmación: cada elemento de A/Q es unidad o es nilpotente. En efecto sea $a + Q \in A/Q$ no unidad, entonces por Corolario 1.1.8 tenemos que $a + Q \in M/Q$. Así existe $m \in M$ tal que $a + Q = m + Q$. De donde $a - m \in Q$. Pero $Q \subseteq r(Q) = M$. En consecuencia $a - m \in M$. Por lo tanto $a \in M$. Ahora por la Definición 1.2.2, tenemos que existe un entero $n > 0$ tal que $a^n \in Q$. Por lo tanto $(a + Q)^n = a^n + Q = \bar{0}$, es decir $a + Q$ es nilpotente en A/Q. De aquí tenemos que cada divisor de cero en A/Q es nilpotente. Por lo tanto, por la Proposición 2.1.2, esto es equivalente a Q sea primario.

ii) Sea t un número natural. Tomamos M un ideal máximo. Probaremos que $r(M^t) = M$. Sea $x \in r(M^t)$, entonces existe n tal que $x^n \in M^t$. Como $M^t \subseteq M$, entonces $x^n \in M$. Ya que $x^n = x(x^{n-1})$, entonces $x(x^{n-1}) \in M$. Como M es primo entonces $x \in M$ o $x^{n-1} \in M$, repitiendo el proceso llegaremos a que $x \in M$. Por lo tanto $r(M^t) \subseteq M$. Ahora sea $x \in M$, entonces $x^t \in M^t$. Por lo tanto $M \subseteq r(M^t)$. Así hemos demostrado que $r(M^t) = M$, De donde M^t es $M-primario$. ■

Proposición 2.1.9. *Sea P un ideal primo y $Q_1, Q_2, ..., Q_n$ ideales $P-$primarios en un anillo A, entonces $Q = \bigcap_{i=1}^{n} Q_i$ es P-primario.*

Demostración. Por la Proposición 1.2.4 inciso (ii), tenemos que $r(Q) = r(\bigcap_{i=1}^{n} Q_i) = \bigcap_{i=1}^{n} r(Q_i) = \bigcap P = P$. Solo falta probar que Q es primario. Supongamos que $x, y \in A$ tal que $xy \in Q$. Como $Q = \bigcap_{i=1}^{n} Q_i$, entonces $xy \in Q_i$ para alguna $1 \leq i \leq n$. Si $x \notin Q$, entonces $x \notin Q_j$ para alguna $1 \leq j \leq n$. Como Q_j es primario, entonces tenemos que $y^n \in Q_j$ para un entero $n > 0$. Por lo tanto $y \in r(Q_j) = P$. Como $r(Q) = P$ y $y \in P$, entonces existe un entero $m > 0$ tal que $y^m \in Q$. Por lo tanto Q es $P-primario$. ■

Definición 2.1.10. *Sea Q un ideal en un anillo A y $x \in A$, definimos*

$(Q : x) = \{y \in A \mid xy \in Q\}$.

Proposición 2.1.11. *Sea P un ideal primo de un anillo A y Q un ideal $P-$primario. Si $x \in A$. Entonces:*

i) $x \in Q \Rightarrow (Q : x) = A$.

ii) Si $x \notin Q$ *entonces* $(Q : x)$ *es* $P-$*primario y por lo tanto* $r((Q : x)) = P$.

iii) Si $x \notin P$ *entonces* $(Q : x) = Q$.

Demostración. i) Supongamos que $x \in Q$, entonces $Ax \subseteq Q$ ya que Q es un ideal de A. Así tenemos que para todo $y \in A$, $yx \in Q$. Por lo tanto $A \subseteq (Q : x)$. Como $(Q : x) \subseteq A$, entonces tenemos que $(Q : x) = A$.

ii) Suponemos que $x \notin Q$, si $y \in (Q : x)$ entonces $xy \in Q$ pero como Q es primario y tenemos que $x \notin Q$, entonces existe un entero $k > 0$ tal que $y^k \in Q$. Así $y \in r(Q)$. Además por hipótesis tenemos que $r(Q) = P$. Por lo tanto $y \in P$. Así tenemos que $(Q : x) \subseteq P$. Pero $Q \subseteq (Q : x)$, entonces $Q \subseteq P$. Se tiene que el radical respeta contenciones, entonces $r(Q) \subseteq r((Q : x)) \subseteq r(P)$, pero $r(P) = P$ y $r(Q) = P$, entonces $P = r(Q) \subseteq r(((Q : x)) \subseteq r(P) = P$ por lo tanto $r((Q : x)) = P$.

Ahora sólo falta probar que $(Q : x)$ es primario. Claramente $1 \notin (Q : x)$, entonces $(Q : x) \neq A$, ahora sean $a, b \in A$ tal que $ab \in (Q : x)$. Supongamos que $b^j \notin (Q : x)$ para todo $j > 0$, entonces por definición del radical tenemos que $b \notin r((Q : x)) = P$. Además como $ab \in (Q : x)$, entonces $abx \in Q$ es decir tenemos que $ax \in Q$ o existe $l > 0$ tal que $b^l \in Q$ por ser Q un ideal primario. Si se tiene que $b^l \in Q$ entonces $b \in r(Q) = P$ lo cual es una contradicción. Así $ax \in Q$ de donde tenemos que $a \in (Q : x)$. Por lo tanto $(Q : x)$ es primario.

iii) Supongamos que $x \notin P$. Claramente tenemos que $Q \subseteq (Q : x)$. Ahora demostraremos que $(Q : x) \subseteq Q$. Supongamos que existe $y \in (Q : x)$ y $y \notin Q$. Como $y \in (Q : x)$, entonces $xy \in Q$. Ya que $y \notin Q$, y Q es primario, entonces existe un entero $m > 0$ tal que $x^m \in Q$. Por lo tanto $x \in r(Q)$. Pero por hipótesis Q es $P-primario$, por lo tanto $r(Q) = P$. Así tenemos que $x \in P$ y esto es una contradicción. Por lo tanto $(Q : x) \subseteq Q$. de donde $(Q : x) = Q$. ■

Definición 2.1.12. *Una descomposición primaria de un ideal I en un*

anillo A es una intersección finita de ideales primarios es decir $I = \bigcap_{i=1}^{n} Q_i$ donde Q_i es ideal primario para $1 \leq i \leq n$.

En general una descomposición primaria no necesariamente existe para cada ideal, sin embargo nos centraremos en los ideales que si tienen descomposición primaria.

Note que los ideales distintos de cero de $\mathbf{Z}$ son de la forma $n\mathbf{Z}$. Ahora si descomponemos a n en sus factores primos $n = p_1^{m_1} p_2^{m_2} ... p_k^{m_k}$, entonces una descomposición primaria de $n\mathbf{Z}$ es $n\mathbf{Z} = \bigcap_{i=1}^{k} (p_i\mathbf{Z})^{m_i} = \bigcap_{i=1}^{k} p_i^{m_i}\mathbf{Z}$.

Definición 2.1.13 *Llamaremos a la descomposición primaria de la Definición 2.1.12 mínima o irredundante si:*

i) $r(Q_1), r(Q_2), ..., r(Q_n)$, son distintos entre si.

ii) $\bigcap_{j \neq i} Q_j \nsubseteq Q_i$ para $1 \leq j \leq n$.

Note que la descomposición $n\mathbf{Z} = \bigcap_{i=1}^{k} p_i^{m_i}\mathbf{Z}$ es mínima.

Proposición 2.1.14 *Cualquier descomposición primaria puede ser remplazada por una descomposición primaria mínima.*

Demostración. Si $I = \bigcap_{j=1}^{n} Q_j$ con cada Q_j primario y algún Q_i contiene a $\bigcap_{j \neq i} Q_j$, entonces $I = \bigcap_{j \neq i} Q_j$ es también una descomposición primaria. Eliminado todos los Q_i que resulten superfluos y cambiando los índices tenemos que $I = \bigcap_{j=1}^{k} Q_j$ con ningún Q_i que contenga la intersección de los otros Q_j. Sean $P_1, ..., P_r$ los ideales primos distintos en el conjunto $\{r(Q_1), ..., r(Q_k)\}$. Sea Q_i' $(1 \leq i \leq r)$ la intersección de todos los $Q_j \in \{Q_1, ..., Q_n\}$ que son P_i-primarios. Por la Proposición 2.1.9 tenemos que Q_i' es P_i-primario. Así para cada $i = 1, 2, ..., r$. $Q_1, Q_2, ..., Q_r$ son P_i-primarios respectivamente. Por lo tanto $I = \bigcap_{j=1}^{n} Q_j = \bigcap_{j=1}^{r} Q_j'$ es una descomposición primaria mínima de I. ■

Definición 2.1.15. *Si I es un ideal en un anillo A, diremos que I es descomponible si I tiene una descomposición primaria.*

Teorema 2.1.16. *(Primer teorema de unicidad) Sea I un ideal descomponible en un anillo A. Sea $I = \bigcap_{i=1}^{n} Q_i$ una descomposición primaria mínima de I. Si $r(Q_i) = P_i$ para $1 \leq i \leq n$, entonces*
$\{P_1, P_2, ..., P_n\} = \{P \mid P$ es primo y $\exists x \in A$ tal que $r((I : x)) = P\}$.

Demostración. Sea $x \in A$ tal que $r((I : x))$ es el ideal primo P. Como $I = \bigcap_{i=1}^{n} Q_i$ entonces $r((I : x)) = r((\bigcap_{i=1}^{n} Q_i) : x)$. Por la Proposición 1.3.2, tenemos que $((\bigcap_{i=1}^{n} Q_i) : x) = \cap_{i=1}^{n}(Q_i : x)$. Así tenemos que $r((\bigcap_{i=1}^{n} Q_i) : x) = r(\cap_{i=1}^{n}(Q_i : x))$. Ahora por Proposición 1.2.4 tenemos que $r(\bigcap_{i=1}^{n}(Q_i : x)) = \bigcap_{i=1}^{n} r((Q_i : x))$. Por lo tanto $\bigcap_{i=1}^{n} r((Q_i : x) = r((I : x)) = P$. Como P es primo, entonces por [1,Proposición 1.11 inciso (ii)] tenemos que existe $1 \leq j \leq n$ tal que $r((Q_j : x)) = P$. Ya que $r((Q_j : x)) = P_j$, entonces $P_j = P$. Por lo tanto hemos probado que $\{P \mid P$ es primo y $\exists x \in A$ tal que $r((I : x)) = P\} \subseteq \{P_1, P_2, ..., P_n\}$.

Ahora demostraremos la otra contención. Como la descomposición primaria de I es mínima, entonces para cada $1 \leq i \leq n$ existe $x_i \in (\bigcap_{j \neq i} Q_j)$ y $x_i \notin Q_i$. Ahora por la Proposición 2.1.11 (ii) tenemos que $r((Q_i : x)) = P_i$. Por otra parte tenemos que $r((I : x_i)) = r((\bigcap_{j=1}^{m} Q_j) : x_i) = r(((\bigcap_j Q_j) \cap Q_i) : x_i) = r((\bigcap_j Q_j) : x_i) \cap r((Q_i : x_i))$. Como $x_i \in \bigcap_{j \neq i} Q_j$, entonces $r((\bigcap_{j \neq i} Q_j) : x_i) = A$. Por lo tanto $r((I : x_i)) = A \cap P_i = P_i$. ■

El teorema anterior asegura que los ideales P_i, $1 \leq i \leq n$ son independientes de la descomposición de I

Note que si A es un anillo y Q es un ideal primario de A que contiene al ideal I, entonces el ideal Q/I es un ideal primario del anillo A/I. En efecto si $x + I, y + I \in A/I$, tal que $(x + I)(y + I) \in Q/I$, entonces $xy + I \in Q/I$, de donde obtenemos que $xy \in Q$. Como Q es primario, entonces $x \in Q$ o existe un entero $m > 0$ tal que $y^m \in Q$. Por lo tanto $x + I \in Q/I$ o $(y + I)^m \in Q/I$. Lo que prueba que Q/I es ideal primario en A/I.

Ahora si $\bigcap_{i=1}^{n} Q_i$ es una descomposición primaria del ideal I. Afirmamos que $\bigcap_{i=1}^{n}(Q_i/I)$ es una descomposición primaria de $\bar{0}$ en el anillo A/I. En efecto, sabemos que Q_i/I es primario en el anillo A/I. Como $I = \cap_{i=1}^{n} Q_i$, entonces $\bar{0} = I/I = (\cap_{i=1}^{n} Q_i)/I = \cap_{i=1}^{n}(Q_i/I)$. Inversamente si $\bar{0}$ tiene una descomposición primaria en A/I, entonces I tiene una descomposición primaria en A. Además si $r(Q_i) = P_i$, entonces $r(Q_i/I) = P_i/I$.

Sean $\{P_1, ..., P_n\}$ los ideales primos del Teorema 2.1.16. Estos ideales se dice que son pertenecientes a I o asociados a I.

Nótese que el ideal I es primario si y solo si tiene un único ideal primo asociado.

Los elementos mínimos del conjunto $\{P_1, ..., P_n\}$ son llamados primos mínimos o primos aislados pertenecientes a I. Los otros son llamados idea-

les primos inmersos.

Ejemplo 2.1.17. Sea $A = F[x, y]$ donde F es un campo, y sea $I =< x^2, xy >= x^2A + xyA = x(xA + yA)$. Observe que $I =< x > \cap < x, y >^2 = (xA) \cap (xA + yA)^2$, además que $I =< x > \cap < x^2, y >$. Claramente $< x >= xA$ es primo en A, además $< x, y >$ es máximo en A y por lo tanto por la Proposición 2.1.8 $< x, y >^2$ es primario en A.

Note que $r(< x >) =< x >$ y $r(< x, y >^2) =< x, y >$.
Los ideales primos asociados a I son los ideales $< x >$ y $< x, y >$. Además $r(I) = r(< x > \cap < x, y >^2) = r(< x >) \cap r(< x, y >^2) =< x > \cap < x, y >=< x >$. Por lo tanto $r(I) =< x >= Ax$ es un ideal primo, pero no es ideal máximo porque $< x >\subseteq< x, y >$. También tenemos que I no es ideal primario ya que el elemento $x(x + y) = (x^2 + xy) \in I$, pero $x \notin I$,y ninguna potencia de $(x + y)$ pertenece a I.

Porposición 2.1.18. *Sea I un ideal descomponible en un anillo A y sea P un ideal primo de A tal que $I \subseteq P$. Entonces P contiene un ideal primo mínimo perteneciente a I.*

Demostración. Sea $I = \bigcap_{i=1}^{n} Q_i$ una descomposición primaria mínima de I y $P_i = r(Q_i)$ para $1 \leq i \leq n$. Como P es primo se tiene que $P = r(P)$. Pero por hipótesis $I \subseteq P$ entonces $r(I) \subseteq r(P) = P$. Por otra parte tenemos que $r(I) = \bigcap_{i=1}^{n} r(Q_i) = \bigcap_{i=1}^{n} P_i$ entonces $\bigcap_{i=1}^{n} P_i \subseteq P$ y por [1, Proposición 1.11] $P_j \subseteq P$ para alguna j. Por lo tanto P contiene un primo mínimo que pertenece a I.

Ya que para cada $I \subseteq A$se tiene que $I \subseteq r(I)$. Por lo tanto si I es descomponible, entonces $I \subseteq r(I) = r(\bigcap_{i=1}^{n} Q_i) = \bigcap_{i=1}^{n} P_i$. Así I esta contenido en cada uno de los ideales primos P_i. Por lo tanto el conjunto de los idales primos mínimos que contienen a I es el mismo conjunto de ideales mínimos pertenecientes a I. ■

Note que en general es falso que todas las componentes primarias son independientes de la descomposición. En el ejemplo 2.1.17 $I =< x^2, xy >=< x > \cap < x, y >^2 =< x > \cap < x^2, y >$ son dos descomposiciones primarias mínimas distintas.

Proposición 2.1.19. *Sea I un ideal descomponible en un anillo A, sea $I = \bigcap_{i=1}^{n} Q_i$ una mínima descomposición primaria y sea $r(Q_i) = P_i$. Entonces $\bigcup_{i=1}^{n} P_i = \{x \in A \mid (I : x) \neq I\}$.*

Demostración Por la nota anterior sabemos que si I es un ideal de A descomponible, entonces $\bar{0}$ es ideal de A/I descomponible. Además una descomposición primaria de $\bar{0}$ es $\bigcap_{i=1}^{n}(Q_i/I)$, es decir $\bar{0} = \bigcap_{i=1}^{n}(Q_i/I)$. Ahora solo debemos demostrar que $\bigcup_{i=1}^{n}(P_i/I) = \{\bar{x} \in A/I \mid (\bar{0}, \bar{x}) \neq \bar{0}\}$.
Sea $\bar{D}$ el conjunto de los divisores de cero en A/I por [1, Proposición 1.15] tenemos que $\bar{D} = \bigcup_{\bar{x}\neq\bar{0}} r(Ann(\bar{x})) = \bigcup_{\bar{x}\neq\bar{0}} r((\bar{0} : \bar{x}))$. Como $\bar{0} = \bigcap_{i=1}^{n}(Q_i/I)$, entonces si $\bar{x} \neq \bar{0}$ tenemos que $r((\bar{0} : \bar{x})) = r(\bigcap_{i=1}^{n}(Q_i/I) : \bar{x}) = \bigcap_{i=1}^{n} r((Q_i/I) : \bar{x})$. Ahora como $\bar{x} \neq \bar{0} = \bigcap_{i=1}^{n}(Q_i/I)$, entonces existe $1 \leq j \leq n$ tal que $\bar{x} \notin (Q_j/I)$, entonces por Proposición 2.1.11, tenemos que $r((Q_j/I) : \bar{x}) = P_j/I$. Por lo tanto $r((\bar{0} : \bar{x})) \subseteq P_j/I$ para alguna $1 \leq j \leq n$. Así obtenemos que $r((\bar{0} : \bar{x})) \subseteq \bigcup_{i=1}^{n}(P_i/I)$ para toda $\bar{x} \neq \bar{0}$. Por lo tanto $\bar{D} = \bigcup_{\bar{x}\neq\bar{0}} r((\bar{0} : \bar{x})) \subseteq \bigcup_{i=1}^{n}(P_i/I)$.

Por otra parte sabemos que $\bar{D} = \{\bar{x} \in A/I \mid (\bar{0}, \bar{x}) \neq \bar{0}\}$. Por lo tanto $\bar{D} \subseteq \bigcup_{i=1}^{n}(P_i/I)$. Ahora por el Teorema 2.1.16 sabemos que cada ideal P_i/I es de la forma $r((\bar{0} : \bar{x}))$ para alguna $\bar{x} \in A/I$. Por lo tanto $\bigcup_{i=1}^{n}(P_i/I) \subseteq \bar{D}$. Así hemos demostrado que $\bigcup_{i=1}^{n}(P_i/I) = \bar{D} = \{\bar{x} \in A/I | (\bar{0} : \bar{x}) \neq \bar{0}\}$. ■

Note que si A es un anillo y el ideal cero es descomponible, entonces por la Proposición 2.1.19, el conjunto D de divisores de cero de A es la unión de ideales primos pertenecientes a 0. Por otra parte también sabemos $r(0) = \{x \in A | x^n = 0\}$ es el conjunto de los elementos nilpotentes de A. Por lo tanto si el cero es descomponible, $0 = \bigcap_{j=1}^{n} Q_j$, entonces $r(0) = r(\bigcap_{j=1}^{n} Q_j) = \bigcap_{j=1}^{n} r(Q_j)$. Con esto probamos que el conjunto de elementos nilpotentes de A es igual a la intersección de los ideales primos pertenecientes a 0.

Proposición 2.1.20. *Sea S un subconjunto multiplicativamente cerrado de A, sea P un ideal primo y Q un ideal P-primario. Entonces:*

i) Si $S \cap P \neq \emptyset$ entonces $S^{-1}Q = S^{-1}A$

ii) Si $S \cap P = \emptyset$ entonces $S^{-1}Q$ es $S^{-1}P$-primario y $(S^{-1}Q)^c = Q$

Demostración. i) Sea $x \in S \cap P$. Como S es multiplicativamente cerrado y $P = r(Q)$ entonces existe un entero $n \geq 1$ tal que $x^n \in S \cap Q$. Así el elemento $\frac{x^n}{1} \in S^{-1}Q$. Pero este elemento es una unidad del anillo $S^{-1}A$, ya que $(\frac{x^n}{1})(\frac{1}{x^n}) = 1$. Por lo tanto $S^{-1}Q = S^{-1}A$.

ii) Ahora supongamos que $S \cap P = \emptyset$ y sea $s \in S$. Afirmación si $a \in A$ es tal que $as \in Q$, entonces $a \in Q$. En efecto si $a \notin Q$, entonces por Proposición

2.1.11 tenemos que $(Q : a) = P$. Como $as \in Q$, entonces $s \in (Q : a) = P$. Así $s \in S \cap P = \emptyset$ esto es una contradicción. Por lo tanto $a \in Q$. Ahora también tenemos que si $as \in Q$, entonces $a \in (Q : s)$. Por lo tanto $(Q : s) \subseteq Q$ para toda $s \in S$. Por lo tanto $\bigcup_s (Q : s) \subseteq Q$. Por la Proposición 1.9.5 tenemos que $Q^{ec} = \bigcup_s (Q : s)$. De aquí tenemos que $Q^{ec} \subseteq Q$. Por otra parte por la Proposición 1.4.3 tenemos que $Q \subseteq Q^{ec}$. Por lo tanto $Q = Q^{ec}$. Ahora por la Proposición 1.9.2 sabemos que la extensión Q^e en el anillo $S^{-1}A$ es el ideal $Q^e = S^{-1}Q$. Por lo tanto $(S^{-1}Q)^c = Q^{ec} = Q$. Solo falta demostrar que $S^{-1}Q$ es $S^{-1}P - primario$. Por la Proposición 1.9.5 tenemos que el operador S^{-1} conmuta con el radical. Así tenemos que $r(S^{-1}Q) = S^{-1}r(Q) = S^{-1}P$. Ahora por [1, Proposición 3.11] $S^{-1}P$ es ideal primo de $S^{-1}A$. Ahora veamos que $S^{-1}Q$ es primario. Para ello sean (x/s), $(y/t) \in S^{-1}A$ tales que $(x/s)(y/t) \in S^{-1}Q$ y $(x/s) \notin S^{-1}Q$, $xy \in Q$ y $x \notin Q$. Como Q es $P - primario$, entonces $y \in r(Q)$. Por lo tanto $(y/t) \in r(S^{-1}Q)$. ■

Para cualquier ideal I en un anillo A y cualquier subconjunto S de A multiplicativamente cerrado, a la contracción del ideal $S^{-1}I$ en A la denotamos como $S(I)$, es decir $(S^{-1}I)^c = S(I)$.

Proposición 2.1.21. *Sea S un subconjunto multiplicativamente cerrado en un anillo A y sea I un ideal descomponible. Sea $I = \bigcap_{i=1}^{n} Q_i$ una mínima descomposición primaria de I y $P_i = r(Q_i)$. Supongamos que los Q_i están ordenados de tal forma que para algún entero $m > 0$, $S \cap P_i = \emptyset$ para $1 \leq i \leq m$ y $S \cap P_j \neq \emptyset$ para $m < j \leq n$. Entonces: $S^{-1}I = \bigcap_{i=1}^{m} S^{-1}Q_i$ y $S(I) = \bigcap_{i=1}^{m} Q_i$. Son mínimas descomposiciones primarias.*

Demostración. Por la Proposición 1.9.5 tenemos que S^{-1} conmuta con la intersección, entonces $S^{-1}I = \bigcap_{i=1}^{n} S^{-1}Q_i$. Por la Proposición 2.1.20 tenemos que $S^{-1}Q_j = S^{-1}A$ para $j > m$, entonces $S^{-1}I = \bigcap_{i=1}^{n} S^{-1}Q_i = \bigcap_{i=1}^{m} S^{-1}Q_i$.
Por otra parte sabemos por la Proposición 2.1.20 tenemos que $S^{-1}Q_i$ es $S^{-1}P_i$-primario. Además $S^{-1}P_1, ..., S^{-1}P_m$, son distintos entre si ya que $P_1, P_2, ..., P_m$ son distintos por hipótesis. Por lo tanto $S^{-1}I = \bigcap_{i=1}^{m} Q_i$ es mínima descomposición primaria.
Ahora sabemos que $S(I) = (S^{-1}I)^c = (\bigcap_{i=1}^{m} (S^{-1}Q_i)^c)$. Por Proposición 1.4.3, tenemos que $(\bigcap_{i=1}^{m} (S^{-1}Q_i)^c) = \bigcap_{i=1}^{m} (S^{-1}Q_i)^c$. Ahora por Proposición 2.1.20 tenemos que $(S^{-1}Q_i)^c = Q_i$. Por lo tanto $S(I) = \bigcap_{i=1}^{m} Q_i$. Además esta descomposición es mínima ya que si para alguna $1 \leq i \leq m$ se cumpliera que $\bigcap_{j=1, j\neq i}^{m} S^{-1}Q_j \subseteq S^{-1}Q_i$ entonces $Q_i = (S^{-1}Q_i)^c \supseteq \bigcap_{j=1, j\neq i}^{m} (S^{-1}Q_j)^c = \bigcap_{j=1, j\neq i}^{m} Q_j$ y esto es una contradicción. ■

Definición 2.1.22. *Sea I un ideal descomponible y Γ un conjunto de ideales primos pertenecientes a I. Diremos que Γ es aislado si cumple lo siguiente:*

Si P' es un ideal perteneciente a I tal que existe $P \in \Gamma$ con $P' \subseteq P$ entonces $P' \in \Gamma$.

Sea Γ un conjunto aislado de ideales primos asociados a I y $S = A - \bigcup_{P\in\Gamma} P$, entonces S es un conjunto multiplicativamente cerrado. En efecto sean $x, y \in S$, entonces $x \notin P$ y $y \notin P$ para todo $P \in \Gamma$. Como cada P es primo, entonces $xy \notin P$ para todo $P \in \Gamma$. Por lo tanto $xy \in S$. Si $P' \in \Gamma$, entonces $P' \cap S = \emptyset$.
Si $P' \notin \Gamma$, entonces $P' \nsubseteq P$ para todo $P \in \Gamma$. Por [1, Proposición 1.11] tenemos que $P' \nsubseteq \bigcup_{P\in\Gamma} P$. Por lo tanto $P' \in \Gamma \Leftrightarrow P \cap S = \emptyset$.

Sea I un ideal descomponible en un anillo A y $P_1, P_2, ..., P_n$ los ideales primos que pertenecen a I (Por el primer teorema de unicidad son independientes de la descomposición).

Teorema 2.1.23. *(Segundo teorema de unicidad) Sea I un ideal descomponible. Sea $I = \bigcap_{i=1}^{n} Q_i$ una descomposición primaria mínima de I con $r(Q_i) = P_i$. Sea $\Gamma = \{P_{j_1}, P_{j_2}, ..., P_{j_m}\}$ un conjunto aislado de ideales primos pertenecientes a I. Entonces $\bigcap_{k=1}^{m} Q_{j_k}$ es independiente de la descomposición.*

Demostración. Consideremos el conjunto multiplicativamente cerrado $S = A \setminus (\bigcup_{I\in\Gamma} I)$. Sabemos que $P_{i_k} \in \Gamma$ para $1 \leq k \leq m$. Por lo tanto $P_{j_k} \cap S = \emptyset$ para todo $1 \leq k \leq m$. Ahora por la Proposición 2.1.21 tenemos que $S(I) = \bigcap_{k=1}^{m} Q_{j_k}$. Por otra parte sabemos que por el primer teorema de unicidad que los ideales primos P_i con $1 \leq i \leq n$ son únicos. Sea $I = \bigcap_{i=1}^{n} Q'_i$ otra descomposición primaria mínima de I. Por la unicidad sabemos que $r(Q'_i) = P_i$. Por lo tanto $\bigcap_{k=1}^{m} Q_{j_k} = S(I) = \bigcap_{i=1}^{n} Q'_{j_i}$. Así esta intersección es única. Llamamos a una componente primaria Q_i de una descomposición primaria aislada si $r(Q_i)$ es aislado, (en cuyo caso $\{r(Q_i)\}$ es aislado), e inmersa en otros casos. ■

Corolario 2.1.24. *Sea I un ideal descomponible. Sea $I = \bigcap_{i=1}^{n} Q_i$ una descomposición primaria mínima y $\Gamma = \{P_{j_1}, P_{j_2}, ..., P_{j_m}\}$ el conjunto aislado de los ideales primos mínimos pertenecientes a I. Entonces $\bigcap_{k=1}^{m} Q_{j_k}$ es únicamente determinada por I.*

Demostración. Sea $S = A \setminus (\bigcup_{I\in\Gamma} I)$, sabemos que S es un conjunto

multiplicativamente cerrado. Por el segundo teorema de unicidad tenemos que $S(I) = \bigcap_{k=1}^{m} Q_{j_k}$ y esta intersección es única. ■

Capítulo 3

Anillos Neterianos

3.1. Descomposición Primaria de Anillos Neterianos

En esta sección probaremos que cada ideal en un anillo neteriano conmutativo tiene descomposición primaria.

Proposición 3.1.1. *Para un anillo conmutativo A las siguientes condiciones son equivalentes:*

i) Todo conjunto de ideales Γ no vacío en A tiene un elemento máximo.

ii) Toda cadena ascendente $I_1 \subseteq I_2 \subseteq ...$ de ideales en A se estaciona, es decir $\exists n$ tal que $I_n = I_{n+1}$.

iii) Todo ideal en A está finitamente generado.

Demotración. $(i) \Rightarrow (ii)$ Sea $\{I_m\}_{m\geq 1}$ una cadena de ideales ascendente con la relación contención, entonces por inciso (i) el conjunto de ideales $\{I_m\}_{m\geq 1}$ tiene un elemento máximo, sea I_n tal elemento, entonces la cadena ascendente $I_1 \subseteq I_2 \subseteq ... \subseteq I_n$, se estaciona en I_n por ser este el elemento máximo.

$(ii) \Rightarrow (i)$ Si (i) es falso entonces hay un conjunto de ideales φ de A que no tiene elemento máximo por lo que podemos construir una cadena $\{I_m\}_{m\geq 1}$ en φ que no se estaciona lo cual es una contradicción al inciso (ii).

$(i) \Rightarrow (iii)$ Sea J un ideal de A y sea F el conjunto de todos los ideales finitamente generados contenidos en J, entonces F es un conjunto no vacío ya que $0 \in F$ por lo tanto por inciso (i) tiene elemento máximo. Sea N_0 tal

elemento. Si $N_0 \subsetneq J$ entonces existe $x \in J$ y $x \notin N_0$. Por lo tanto $N_0 + Ax$ es un ideal tal que $N_0 \subsetneq N_0 + Ax \subseteq J$ y $N_0 + Ax$ es finitamente generado, lo cual es una contradicción ya que N_0 es máximo. Por lo tanto $J = N_0$.

$(iii) \Rightarrow (ii)$ Sea $I_1 \subseteq I_2 \subseteq ...$ una cadena ascendente de ideales en A, y sea $I = \bigcup_{k=1}^{\infty} I_k$ que es un ideal. Por (iii) I es finitamente generado. Sean $x_1, ..., x_r$ los generadores de I. Como cada $x_l \in I_{k_l}$, entonces sea $n = max\{k_1, k_2, ..., k_r\}$. Por lo tanto $x_l \in I_n$ para todo $1 \leq l \leq r$, entonces $I_n = I$ y por lo tanto la cadena se estaciona en I_n. ■

Definición 3.1.2. *Un anillo A es Noetheriano si cumple alguna de las condiciones de la Proposición 3.1.1.*

Los anillos Neterianos son parte importante de las clases de anillos en el álgebra conmutativa. Haremos importantes deducciones alrededor de los anillos Neterianos incluyendo la existencia de descomposiciones primarias.

Proposición 3.1.3. *Sea A un anillo neteriano, I un ideal de A entonces A/I es neteriano.*

Demostración. Dada una cadena ascendente de ideales en A/I da lugar a una cadena ascendente de ideales en A, y como A es neteriano, entonces se estaciona. Por lo tanto A/I es neteriano. ■

Proposición 3.1.4. *Sea A es un anillo neteriano y Φ un morfismo de A a un anillo B, tal que Φ es suprayectivo, entonces B es neteriano.*

Demostración. Dado A un anillo neteriano, entonces por Proposición 3.1.3 si $I = ker(\Phi)$, entonces tenemos que $A/I = A/ker(\Phi)$ es también neteriano, entonces por primer teorema de isomorfismos $A/ker(\Phi) \cong Im(\Phi) = B$. Por lo tanto B es neteriano. ■

Proposición 3.1.5. *Sea A un subanillo de B. Supongamos que A es neteriano y que B es $A-$módulo finitamente generado. Entonces B es un anillo neteriano.*

Demostración. Como B es una $A-$*módulo* finitamente generado, entonces por [1, Proposición 6.5] B es neteriano como $A-$*módulo*. Como A es subanillo de B entonces B es neteriano como $B-$*módulo*. Por lo tanto B es neteriano como anillo. ■

Teorema 3.1.6. *(Teorema de la base de Hilbert) Si A es un anillo ne-*

teriano, entonces el anillo de polinomios $A[x]$ es neteriano.

Demostración. Sea J un ideal en $A[x]$. Los coeficientes principales de los polinomios en J forman un ideal I en A. Como A es neteriano, entonces I es finitamente generado. Sean $a_1, a_2, ..., a_n$ los elementos que generan a I. Para cada $i = 1, ..., n$ existe un polinomio $f_i \in A[x]$ y $f_i \in J$, de la forma $f_i = a_i x^{r_i} +$ (términos de grado menor). Sea $r = max\{r_1, r_2, ..., r_n\}$. Sea J' el ideal generado por $f_1, f_2, ..., f_n$, entonces $J' \subseteq J \subseteq A[x]$.

Sea $f = cx^m +$ (términos de grado menores) cualquier elemento de J, entonces $c \in I$. Si $m \geq r$, entonces escribimos $c = \sum_{i=1}^{n} u_i a_i$, donde $u_i \in A$; luego $f - \sum u_i f_i x^{m-r_i}$ pertenece a J y tiene grado menor que m. Procediendo de esta manera, podemos seguir restando elementos de J' a f hasta que tengamos un polinomio g de grado menor a r tal que $f = g + h$, donde $h \in J'$.

Sea M un $A - módulo$ generado por $1, x, ..., x^{r-1}$. Afirmación $J = (J \cap M) + J'$. En efecto como M es un $A - módulo$ finitamente generado, entonces por [1] Proposición 6.5 tenemos que M es neteriano. Nuevamente por [1, Proposición 6.2] tenemos que $J \cap M$ es $A - módulo$ finitamente generado. Si $g_1, ..., g_t$ generan a $J \cap M$ es claro que $\{f_1, ..., f_n, g_1, ..., g_t\}$ generan a J. Por lo tanto J es finitamente generado y por lo tanto $A[x]$ es neteriano. ■

Proposición 3.1.7. *Si A es neteriano entonces $A[x_1, ..., x_n]$ también es neteriano.*

Demostración. Por inducción sobre n a partir del Teorema 3.1.6. ■

Las siguientes dos proposiciones muestran que todo ideal distinto de (1) en un anillo neteriano tiene una descomposición primaria.

Definición 3.1.8. *Un ideal I en un anillo A se llama irreducible si $I = J \cap K$ entonces $I = J$ o $I = K$.*

Note que si P es un ideal primo de A (un anillo conmutativo con 1); entonces P también resulta ser irreducible. En efecto, sean J,K ideales de A tales que P $= J \cap K$, se tiene que $JK \subseteq J \cap K$, entonces $JK \subseteq P$. Por hipótesis P es un ideal primo, entonces $J \subseteq P$ ó $K \subseteq P$. Pero $P = J \cap K \subseteq J, k$. Por lo tanto $P = J$ ó $P = K$.

Proposición 3.1.9. *En un anillo neteriano A todo ideal es una intersección finita de ideales irreducibles.*

Demostración. Suponemos que existe un ideal I que no es intersección

finita de ideales irreducibles, entonces el conjunto Γ de ideales en A para los cuales la proposición es falsa es no vacío, como A es neteriano, Γ tiene un ideal máximo M. Entonces M no es ideal reducible. Por lo tanto $M = J \cap K$ donde $M \subsetneq K$ y $M \subsetneq J$ con J, K ideales de A y como M es máximo de Γ, entonces $J, K \notin \Gamma$. Por lo tanto J, K son una intersección finita de ideales irreducibles. Así M también lo es, lo cual es una contradicción. ■

Proposición 3.1.10. *En un anillo neteriano A todo ideal irreducible es primario.*

Demostración. Tomando el anillo de cocientes, es suficiente mostrar que si el ideal cero es irreducible, entonces es primario. Supongamos que (0) es irreducible. Sea $xy = 0$ con $y \neq 0$, y considere la cadena de ideales $Ann(x) \subseteq Ann(x^2) \subseteq ....$ Como A es neteriano, entonces la cadena se estaciona, es decir tenemos que $Ann(x^n) = Ann(x^{n+1}) = ...$ para algún n. Afirmación $Ax^n \cap Ay = 0$. En efecto, sea $bx^n = ay$, entonces $(bx^n)x = (ay)x$. Como $xy = 0$, entonces $yx = 0$. así $(ay)x = a(yx) = 0$. Por lo tanto $0 = (bx^n)x = bx^{n+1}$, entonces $b \in Ann(x^{n+1}) = Ann(x^n)$. De donde tenemos que $b \in Ann(x^n)$. Por lo tanto $0 = bx^n = ay$. Así $Ax^n \cap Ay = 0$. Puesto que (0) es irreducible y $Ay \neq 0$, entonces $x^n = 0$. Así tenemos que el ideal cero es primario. ■

Teorema 3.1.11. *En un anillo neteriano cada ideal tiene una descomposición primaria.*

Demostración. El resultado se obtiene de las Proposiciones 3.1.9 y 3.1.10. ■

Proposición 3.1.12. *En un anillo neteriano A, cada ideal contiene una potencia de su radical.*

Demostración. Como A es neteriano entonces $r(I)$ es finitamente generado. Sea $r(I)$ generado por $x_1, ..., x_k$: es decir $x_i^{n_i} \in I$ $(1 \leq i \leq k)$. Sea $m = \sum_{i=1}^{k}(n_i - 1) + 1$, entonces $r(I)^m$ está generado por los productos $x_1^{r_1} \cdots x_k^{r_k}$ con $\sum_{i=1}^{n} r_i = m$; por definición de m se tiene que $r_i \geq n_i$ para al menos un indice i. Por lo tanto cada uno de estos monomios esta en I y así $r(I)^m \subseteq I$. ■

Proposición 3.1.13. *En un anillo neteriano el nilradical es nilpotente.*

Demostración. Tómese $I = (0)$ en el Teorema 3.1.11. ■

Proposición 3.1.14. *Sea A un anillo neteriano, M un ideal máximo e I un ideal cualquiera en A. Entonces las siguientes condiciones son equivalentes:*

i) I es $M-primario$;

ii) $r(I) = M$;

iii) $M^n \subseteq I \subseteq M$ para algún $n > 0$.

Demostración. *i)* $\Rightarrow$ *ii)* Es claro de la definición; *ii)* $\Rightarrow$ *i)* Por el Teorema 2.1.16; *ii)* $\Rightarrow$ *iii)* Aplicando la Proposición 3.1.12; *iii)* $\Rightarrow$ *ii)* Tomando los radicales y por propiedades del radical $r(M^n) \subseteq r(I) \subseteq r(M)$ pero como M es máximo entonces $r(M^n) = M$ y $r(M) = M$, por lo tanto $r(I) = M$. ■

Proposición 3.1.15. *Sea $I \neq A$ un ideal en un anillo neteriano A. Entonces los ideales primos pertenecientes a I son precisamente los ideales primos que aparecen en el conjunto de ideales $(I : x)$ con $x \in A$.*

Demostración. Si tomamos el anillo cociente A/I podemos suponer que $I = 0$. Sea $\bigcap_{i=1}^{n} Q_i = 0$ una descomposición primaria mínima del ideal cero. Sea $P_i = r(Q_i)$ e $I_k = \bigcap_{j \neq k} Q_j \neq 0$. Entonces de la demostración del primer teorema de unicidad Teorema 2.1.16, se tiene que $r(Ann(x)) = P_i$ para cada $x \neq 0$ en I_k, de manera que $Ann(x) \subseteq P_i$. Puesto que cada Q_i es P_i-primario entonces por Proposición 3.1.12 existe un entero m tal que $P_i^m \subseteq Q_i$. Por lo tanto $I_i P_i^m \subseteq I_i \cap P_i^m \subseteq I_i \cap Q_i = 0$. Sea $m \geq 1$ el menor entero tal que $I_i P_i^m = 0$ y sea x un elemento no nulo en $I_i P_i^{m-1}$, entonces $P_i x = 0$. Por lo tanto para cada una de estas x se tiene que $P_i \subseteq Ann(x)$ y por lo tanto $P_i = Ann(x)$.

Recíprocamente, si $Ann(x)$ es un ideal primo P, entonces $r(Ann(x)) = P$ y por lo tanto por el primer teorema de unicidad Teorema 2.1.16, P es un ideal primo perteneciente a cero. ■

Capítulo 4

Descomposición primaria de Módulos

En este capítulo extenderemos el concepto de descomposición primaria de ideales a descomposición primaria de submódulos de un $R-$*módulo* M. A lo largo del mismo, consideraremos R-módulos izquierdos por conveniencia de notación, donde R denotará a un anillo conmutativo con 1.

4.1. Radical

Definición 4.1.1. *Sea R un anillo conmutativo y N un submódulo de un $R-$módulo izquierdo M. El radical de N en M se define como $r_M(N) = \{x \in R : x^q M \subseteq N$ para algún entero $q > 0\}$.*

Definición 4.1.2. *Sean N y L son submódulos de un $R-$módulo M, definimos $(N : L) = \{x \in R | xL \subseteq N\}$.*

Note que $(N : L)$ es un ideal del anillo R. En efecto sea $x \in (N : L)$ es claro que $rx \in (N : L)$ para todo $r \in R$. Sean $x, y \in (N : L)$ tal que $xA \subseteq N$ y $yL \subseteq N$, entonces $xL + yL = (x + y)L \subseteq N$. Por lo tanto $(N : L)$ es un ideal de R. En particular, $(0 : M)$ es llamado el *anulador* de M y se denota por $Ann(M)$.

Si $(x) = Rx$ es el submódulo generado por $x \in M$, escribiremos $(N : x)$ y $Ann(x)$ en lugar de $(N : Rx)$ y $Ann(Rx)$ respectivamente. Como R es conmutativo, entonces $(N : x) = \{r \in R | rx \in N\}$. En efecto si $rx \in N$, entonces $Rrx \subseteq N$ de donde $r(Rx) \subseteq N$. Por lo tanto $r \in (N : Rx) = (N : (x))$. Ahora si $r \in (N : (x))$ tenemos que $r(Rx) \subseteq N$ así $rx \in N$.

Observe también que si N es un submódulo de M y $x \in M$, entonces

$(N : x) = Ann(\bar{x})$ donde $\bar{x} = x + N \in M/N$.

Proposición 4.1.3. *Sea N un submódulo de un $R-$módulo M. Entonces $r_M(N) = r((N : M)) = r(Ann(M/N))$. En particular $r_M(N)$ es un ideal.*

Demostración. Sea $x \in r_M(N)$, entonces existe un entero $q > 0$ tal que $x^q M \subseteq N$, entonces $x^q \in (N : M)$. Por lo tanto $r_M(N) \subseteq r(N : M)$.
Ahora sea $x \in r((N : M))$, entonces existe un entero $q > 0$ tal que $x^q \in (N : M)$. Entonces $x^q M \subseteq N$. Por lo tanto $x^q m \in N$ para todo $m \in M$. Así $x^q m + N = \bar{0} = N/N$. De aquí obtenemos que $x^q m + N \subseteq N$ $\forall$m $\in M$. Por lo que $x^q(m + N) \subseteq N$ para todo $m \in M$, así $x^q(M/N) = \bar{0}$. Por lo tanto $x^q \in Ann(M/N)$. Finalmente $x \in r(Ann(M/N))$ y tenemos que $r((M : N)) \subseteq r(Ann(M/N))$.
Por último si $x \in r(Ann(M/N))$, entonces existe un entero $q > 0$ tal que $x^q(M/N) = \bar{0}$; de aquí se tiene que $x^q(M+N) \subseteq N$. Por lo tanto $x^q M \subseteq N$, es decir $x \in r_M(N)$.
Como $r_M(N) \subseteq r((M : N)) \subseteq r(Ann(M/N)) \subseteq r_M(N)$ obtenemos el resultado deseado. ■

Note que como $(N : M)$ es un ideal entonces $r_M(N) = r(N : M)$ también es un ideal.

Proposición 4.1.4. *Sean $N, N_1, N_2, ..., N_m$ submódulos de un $R-$módulo M, entonces:*

i) Si $L \subseteq N$, entonces $r_M(L) \subseteq r_M(N)$

ii) $r_M(N) = r(r_M(N))$

iii) $r_M(\bigcap_{j=1}^m N_j) = \bigcap_{j=1}^m r_M(N_j)$

iv) $r_M(N) = R \Leftrightarrow N = M$

v) $r(r_M(N_1) + r(r_M(N_2)) \subseteq r_M(N_1 + N_2)$.

Demostración. i) Sea $x \in r_M(L)$, entonces existe un entero $q > 0$ tal que $x^q M \subseteq L$. Como $L \subseteq N$, entonces $x^q M \subseteq N$. Así $x \in r_M(N)$. Por lo tanto $r_M(L) \subseteq r_M(N)$.

(ii) Si $x \in r(r_M(N))$, entonces $x^q \in r_M(N)$. Por lo tanto existe un entero $p > 0$ tal que $(x^q)^p M \subseteq N$. Por lo tanto $x \in r_M(N)$. Así $r(r_M(N)) \subseteq r_M(N)$.

La otra inclusión se deduce del inciso (i) de la Proposición 1.2.4.

(iii) Si $x \in \bigcap_{j=1}^{m} r_M(N_j)$, entonces existe enteros $q_1, q_2, ..., q_m > 0$ tal que $x^{q_j} M \subseteq N_j$ para cada $j = 1, ..., m$. Si $q = q_1 + q_2 + ... + q_m$, entonces $x^q = x^{q_1} x^{q_2} ... x^{q_m} M \subseteq \bigcap_{j=1}^{m} N_j$. Así $\bigcap_{j=1}^{m} r_M(N_j) \subseteq r_M(\bigcap_{j=1}^{m} N_j)$. Recíprocamente si $x \in r_M(\bigcap_{j=1}^{m} N_j)$, entonces existe un entero $q > 0$ tal que $x^q M \subseteq \bigcap_{j=1}^{m} N_j$. Por lo tanto para cada $j = 1, ..., m$, se tiene que $x^q M \subseteq N_j$, es decir $x \in r_M(N_j)$. Por lo tanto $x \in \bigcap_{j=1}^{m} r_M(N_j)$ y $r_M(\bigcap_{j=1}^{m} N_j) \subseteq \bigcap_{j=1}^{m} r_M(N_j)$.

(iv) Sea $r_M(N) = R$ entonces para todo $r \in R$, existe un entero $q > 0$ tal que $r^q M \subseteq N$, en particular $M = 1^q M \subseteq N$. Por lo tanto $M = N$. La otra implicación es trivial.

(v) Por inciso (ii), tenemos que $r_M(N_1) = r(r_M(N_1))$ y $r_M(N_2) = r(r_M(N_2))$. Ahora por el inciso (i) tenemos que $r_M(N_1) \subseteq r_M(N_1 + N_2)$ y $r_M(N_2) \subseteq r_M(N_1 + N_2)$. Por lo tanto $r_M(N_1) + r_M(N_2) \subseteq r_M(N_1 + N_2)$. Como $r_M(N_1) + r_M(N_2)$ y $r_M(N_1 + N_2)$ son ideales del anillo, entonces $r(r_M(N_1) + r_M(N_2)) \subseteq r(r_M(N_1 + N_2))$. Ahora por inciso (ii) $r(r_M(N_1 + N_2)) = r_M(N_1 + N_2)$. Así obtenemos que $r(r_M(N_1) + r_M(N_2)) \subseteq r_M(N_1 + N_2)$. ■

4.2. Módulos Primarios

Definición 4.2.1. *Sea $x \in R$ y $\phi_x : M \longrightarrow M$ el endomorfismo, tal que $\phi_x(m) = xm$. El elemento x se dice que es un divisor de cero en M si ϕ_x no es inyectivo, se dice que x es nilpotente en M si ϕ_x es nilpotente.*

Note que el morfismo ϕ_x es un morfismo de $R - módulos$ porque R es anillo conmutativo. Notese también que x es divisor de cero en M si existe $0 \neq m \in M$ tal que $xm = 0$.

También se puede observar que si x es nilpotente entonces existe un entero $q > 0$ tal que $(\phi_x)^q$ es el morfismo cero; esto es, $(\phi_x)^q(m) = 0$, $\forall m \in M$. Por lo tanto, $(\phi_x)^q(m) = (\phi_x)...(\phi_x)(m) = x^q m = 0$, $\forall m \in M$. Así x es nilpotente en M si existe un entero $q > 0$ tal que $x^q m = 0, \forall m \in M$.

Definición 4.2.2. *Un submódulo Q de un $R - módulo$ M es primario en M si $Q \neq M$ y cada divisor de cero en M/Q es nilpotente.*

Note que Q es primario en M si para cada $\alpha \in R$ y para cada $x \notin Q$ tal

que $\alpha x \in Q$, entonces $\alpha^n M \subseteq Q$ para algún entero positivo n.

Proposición 4.2.3. *Sea Q un submódulo primario de M, entonces $(Q : M)$ es un ideal primario. Por lo tanto $r_M(Q)$ es un ideal primo P.*

Demostración. Sean $x, y \in R$ tales que $yx \in (Q : M)$ y $x \notin (Q : M)$, entonces $yxM \subseteq Q$ y $xM \nsubseteq Q$. Afirmemos que $\phi_y : M/Q \longrightarrow M/Q$ no es inyectiva. En efecto, como $xM \nsubseteq Q$, entonces existe $m' \in M$ tal que $xm' \notin Q$. Por otra parte sabemos que $yxM \subseteq Q$; Por lo tanto $y(xm') \in Q$. Así $\phi_y(xm') = \bar{0}$ pero $xm' \neq \bar{0}$. Por lo tanto ϕ_y no es inyectiva. de donde se sigue que y es un divisor de cero en M/Q. Como Q es submódulo primario de M existe un entero $q > 0$ tal que $\phi_y^q = \bar{0}$. Así, para todo $m \in M$, se sigue que $\bar{0} = \phi_y^q(m+Q) = y^q(m+Q) = y^q m + Q$. Por lo tanto $y^q M \subseteq Q$ y en consecuencia $y^q \in (Q : M)$. Con lo cual hemos probado que $(Q : M)$ es primario. Ahora por la Proposición 4.1.3 tenemos que $r_M(Q) = r((Q : M))$. Ahora por la Proposición 2.1.5 tenemos que $r((Q : M))$ es un ideal primo P. ■

Definición 4.2.4. *Si Q es un submódulo primario en M y $r_M(Q) = P$, diremos que Q es $P-$primario en M.*

Proposición 4.2.5. *Sean $Q_1, Q_2, ..., Q_n$ submódulos $P-$primarios en M, entonces $Q = \bigcap_{i=1}^n Q_i$ es $P-$primario en M.*

Demostración. Note primero que $(Q : M) = \bigcap_{i=1}^n (Q_i : M)$. En efecto $x \in (Q : M) \Leftrightarrow x \in (\bigcap_{i=1}^n Q_i : M) \Leftrightarrow xM \subseteq \bigcap_{i=1}^n Q_i \Leftrightarrow xM \subseteq Q_i$ para toda $1 \leq i \leq n$, $\Leftrightarrow x \in (Q_i : M)$ para toda $1 \leq i \leq n$, $\Leftrightarrow x \in \bigcap_{i=1}^n (Q_i : M)$. Ahora por la Proposición 4.1.3 tenemos que $r_M(Q) = r(Q : M) = r(\bigcap_{i=1}^n Q_i : M) = r(\bigcap_{i=1}^n (Q_i : M))$. También por la Proposición 1.2.4, inciso (ii); se tiene que $r(\bigcap_{i=1}^n (Q_i : M)) = \bigcap_{i=1}^n r((Q_i : M)) = \bigcap_{i=1}^n r_M(Q_i)$. Como cada Q_i es $P-primario$, entonces $\bigcap_{i=1}^n r_M(Q_i) = P$. De donde se sigue que $r_M(Q) = P$. Solo falta demostrar que Q es primario en M. Sea x un divisor de cero en M/Q, entonces $\phi_x : M/Q \longrightarrow M/Q$ no es inyectivo. Así existe $m + Q \neq \bar{0}$ tal que $\phi_x(m + Q) = \bar{0}$. Además se tiene que $xm + Q = \bar{0}$, entonces $xm \in Q$. En consecuencia tenemos que $m \notin Q$ pero $xm \in Q$. Como $m \notin Q = \bigcap_{i=1}^n Q_i$, entonces existe $1 \leq j \leq n$ tal que $m \notin Q_j$.
Por otra parte, ya que $xm \in Q = \bigcap_{i=1}^n Q_i$, entonces $xm \in Q_j$ para toda $j = 1, 2, ..., n$. Así, para $\phi_x : M/Q_j \longrightarrow M/Q_j$ tenemos que $\phi_x(m + Q_j) = xm + Q_j = \bar{0}$, es decir ϕ_x no es inyectiva. Por lo tanto, x es divisor de cero en M/Q_j. Como Q_j es primario en M, se sigue que ϕ_x es nilpotente, es decir existe un entero $n > 0$ tal que $(\phi_x)^n(M/Q_j) = \bar{0}$. De donde, $x^n(M/Q_j) = \bar{0}$. Así tenemos que $x^n M \subseteq Q_j$. En consecuencia $x \in r_M(Q_j) = P$. Además

sabemos que $r_M(Q) = P$, por lo que se tiene que $x \in r_M(Q)$. Entonces existe un entero $q > 0$ tal que $x^q M \subseteq Q$. Así tenemos que $x^q(M/Q) = \bar{0}$. Finalmente $\phi_x : M/Q \longrightarrow M/Q$ es nilpotente, de donde obtenemos que x es nilpotente en M/Q. De donde Q es primario en M. ■

Proposición 4.2.6. *Sea Q un submódulo $P-$primario de M y $x \in M$, entonces:*

i) Si $x \in Q$ entonces $(Q : x) = R$;

ii) Si $x \notin Q$ entonces $(Q : x)$ es $P -$ primario, $r(Q : x) = P$.

Demostración. i) Se deduce de la Definición 4.1.2.

(ii) Veamos que $(Q : x)$ es primario. Para ello sean $z, y \in R$ tales que, $zy \in (Q : x)$, $y \notin (Q : x) = (Q : Rx)$. Como $yz \in (Q : x) = (Q : Rx)$, entonces $(yz)Rx \in Q$. Ya que $y \notin (Q : Rx)$, se sigue que $y(Rx) \nsubseteq Q$ así existe $t \in R$ con $ytx \notin Q$. Pero $z(ytx) \in Q$, por lo cual z es un divisor de cero en M/Q ya que $\phi_z(yx + Q) = zyx + Q = \bar{0}$ e $yx \notin Q$. dado que Q es primario existe un entero $q > 0$ tal que $\phi_z^q(M) = z^q M + Q = \bar{0}$ en particular $z^q Rx \subseteq Q$. Por lo tanto $z^q \in (Q : x)$.
Solo falta probar que $r((Q : x)) = P$. Sea $y \in (Q : x)$ luego $yx \in Q$ entonces como $x \notin Q$ tenemos que y es un divisor de cero en M/Q. Teniendo que Q es primario, entonces y es nilpotente en M/Q. De donde se sigue que $\phi_y^q(M) = y^q M + Q = \bar{0}$ para cierto entero $q > 0$. Así $y \in r_M(Q)$. Ahora por la Proposición 3.1.1, tenemos que $r_M(Q) = r((Q : M)) = P$. Por lo cual $y \in P$. De donde $(Q : x) \subseteq P$. Tomando radicales obtenemos que $r((Q : x)) \subseteq r(P) = P$. Ahora sea $y \in P$. Como Q es $P - primario$, se sigue que $y \in P = r_M(Q)$, entonces $y^q M \subseteq Q$ para cierto entero $q > 0$, en particular $y^q Rx \subseteq Q$. Por lo tanto $y \in r((Q : x))$ y $P \subseteq r((Q : x))$. Con lo cual queda demostrada la igualdad. ■

Definición 4.2.7. *Una descomposición primaria de un submódulo N en M es una representación de N como una intersección finita de submódulos primarios en M, es decir $N = \bigcap_{i=1}^{n} Q_i$. Si además ninguna de las componentes Q_i puede omitirse la intersección, es decir $\bigcap_{j \neq i} Q_j \nsubseteq Q_i$ y los ideales primos $P_i = r_M(Q_i)$son distintos, entonces la descomposición primaria se dice mínima. Diremos que N tiene una descomposición en M si N tiene una descomposición primaria en M.*

Teorema 4.2.8. *Sea N un submódulo de M tal que $N = \bigcap_{j=1}^{n} Q_j$ es una descomposición primaria mínima de N. Sea $P_i = r_M(Q_i)$ $(1 \leq i \leq n)$,*

entonces los P_i son precisamente los ideales primos que aparecen en el conjunto de ideales $r(N : x)$, $x \in M$ y son independientes de la descomposición particular de N.

Demostración. Veamos primero que $(\bigcap_{i=1}^{n} Q_i : x) = \bigcap_{i=1}^{n}(Q_i : x)$. Sea $y \in (\bigcap_{i=1}^{n} Q_i : x)$, entonces $yRx \subseteq \bigcap_{i=1}^{n} Q_i$, de donde $yRx \subseteq Q_i$ para $i = 1, 2, ..., n$. Por lo tanto $y \in (Q_i : x)$ para cada $i = 1, 2, ..., n$. Así $(\bigcap_{i=1}^{n} Q_i : x) \subseteq \bigcap_{i=1}^{n}(R_i, x)$. Recíprocamente si $y \in \bigcap_{i=1}^{n}(Q_i : x)$, entonces para cada i, tenemos que $yRx \subseteq Q_i$. Se sigue que $yRx \subseteq \bigcap_{i=1}^{n} Q_i$. En consecuencia $y \in (\bigcap_{i=1}^{n} Q_i : x)$. Así $\bigcap_{i=1}^{n}(Q_i : x) \subseteq (\bigcap_{i=1}^{n} Q_i : x)$.
Entonces por lo demostrado antes, para cada $x \in M$ se tiene que $(N : x) = (\bigcap_{i=1}^{n} Q_i : x) = \bigcap_{i=1}^{n}(Q_i : x)$. Por lo tanto $r(N : x) = \bigcap_{i=1}^{n} r(Q_i : x)$. Ahora por la Proposición 4.2.6, se tiene que $\bigcap_{i=1}^{n} r((Q_i : x)) = \bigcap_{x \notin Q_j} P_j$. Supongamos que $r(N : x)$ es primo, por la Proposición 2.1.3, se sigue que $r(N : x) = P_j$ para alguna j. Por lo tanto cada ideal primo de la forma $r(N : x)$ es uno de los P_j. Recíprocamente como la descomposición es mínima, para cada i existe $x_i \notin Q_i$, pero $x_i \in \bigcap_{i \neq j} Q_j$, entonces se tiene que $r((N : x)) = \bigcap_{j \notin Q_j} P_j = P_i$. ■

Definición 4.2.9. *Los P_i del teorema anterior se dice que son ideales primos pertenecientes a N en M. Los elementos mínimos del conjunto $\{P_1, ..., P_n\}$ se denominan ideales primos mínimos o aislados pertenecientes a N. Los otros se denominan ideales primos inmersos.*

Proposición 4.2.10. *Sea N un submódulo de M tal que $N = \bigcap_{j=1}^{n} Q_j$ es una descomposición primaria mínima de N. Si $P_i = r_M(Q_i)$ $(1 \leq i \leq n)$, entonces los P_i son precisamente los ideales primos pertenecientes a 0 en M/N.*

Demostración. Por el Teorema 4.2.8 P es un ideal primo perteneciente a N en M si y sólo si existe un $x \in M$ tal que $P = r((N : x))$. Como $r((N : x)) = r((\bar{0} : \bar{x})) = r(Ann(\bar{x}))$, donde $x + N = \bar{x} \in M/N$, entonces $P = (\bar{0} : \bar{x})$ es un ideal primo. Lo que es equivalente a decir que P es un ideal primo perteneciente a M/N. ■

Proposición 4.2.11 *Sea N un submódulo descomponible de M, entonces cada ideal primo P tal que $r_M(N) \subseteq P$, contiene un ideal primo mínimo perteneciente a N. Así los ideales primos mínimos pertenecientes a N son precisamente los elementos mínimos en el conjunto de todos los ideales primos que contienen a $r_M(N)$.*

Demostración. Sea P un ideal primo tal que $r_M(N) \subseteq P$, entonces

tenemos que $r_M(N) = \bigcap_{i=1}^{n} r_M(Q_i) = \bigcap P_j$, donde P_j es primo mínimo perteneciente a N, entonces $\bigcap P_j \subseteq P$. Así tenemos que $P_j \subseteq P$ para algún entero j. Por lo tanto P contiene un ideal primo mínimo perteneciente a N. Ahora si P es un elemento mínimo del conjunto de ideales primos que contienen a $r_M(N)$, entonces $P_i = P$. Además como $r_M(N) = \bigcap P_j$ y cada P_j es un ideal primo mínimo perteneciente a N, tenemos claramente que $r_M(N) \subseteq P_j$. ■

Sea S un conjunto multiplicativamente cerrado del anillo R. La construcción de $S^{-1}R$ puede efectuarse con un $R-$*módulo* M en lugar del anillo R, definimos en $M \times R$ la relación $\equiv$ como sigue: $(m, s) \equiv (m', s')$ si y solo si existe $t \in S$ tal que $t(sm' - s'm) = 0$.
Es rutinario verificar que ésta relación es de equivalencia. Denotamos por m/s la clase de equivalencia de la pareja (m, s) y por $S^{-1}M$ al conjunto de estas clases de equivalencia. Ahora $S^{-1}M$ tiene la estructura de $S^{-1}R-$*módulo* con las siguientes operaciones: $(\frac{m}{s}) + (\frac{m'}{s'}) = \frac{s'm + sm'}{ss'}$. Si $\frac{a}{s} \in S^{-1}R$, entonces $(\frac{a}{s})(\frac{m}{s'}) = \frac{am}{ss'}$.

Proposición 4.2.12. *Sea S un subconjunto multiplicativamente cerrado de R, y sea Q un submódulo $P-$primario de un $R-$módulo M. Entonces las siguientes condiciones se cumplen.*

i) Si $S \cap P \neq \emptyset$, entonces $S^{-1}Q = S^{-1}M$.

ii) Si $S \cap P = \emptyset$, entonces $S^{-1}Q$ es $S^{-1}P-$primario.

Demostración. i) Sea $s \in S \cap P$. Como $P = r_M(Q)$, entonces $s^n M \subseteq Q$ para algún entero $n > 0$. Sea $m/t \in S^{-1}M$, entonces $m/t = (s^n m)/(s^n t) \in S^{-1}Q$. Por lo tanto $S^{-1}M \subseteq S^{-1}Q$. La otra inclusión es clara.

ii) Si $S \cap P = \emptyset$, entonces $S^{-1}Q \neq S^{-1}M$. Veamos que $r_{S^{-1}M}(S^{-1}Q) = S^{-1}P$, para ello sea $x/s \in S^{-1}P$, se sigue que $x \in P$ y existe un entero $q > 0$ tal que $x^q M \subseteq Q$, por lo que $(x^q/s^q)(S^{-1}M) \subseteq S^{-1}Q$. Por lo tanto $S^{-1}P \subseteq r_{S^{-1}M}(S^{-1}Q)$. Para la otra inclusión sea $(x/s) \in r_{S^{-1}M}(S^{-1}Q)$, de donde se tiene que $(x/s)^q(S^{-1}M) \subseteq S^{-1}Q$, entonces $x^q M \subseteq Q$. Como $P = r_M(Q)$, se sigue que $x \in P$. Por lo tanto $(x/s) \in S^{-1}P$.
Ahora veamos que $S^{-1}Q$ es primario, para ello sean $(r/s) \in S^{-1}R$ y $(x/t) \in S^{-1}Q$ tales que $(r/s)(x/t) \notin S^{-1}Q$. Por lo cual $rx \in Q$, con $r \in R$ y $x \notin Q$. Como Q es primario, entonces $r^n M \subseteq Q$ para algún entero $n > 0$. De donde se tiene que $(r^n/s^n)S^{-1}M \subseteq S^{-1}Q$. ■

Capítulo 5

Descomposición Terciaria

5.1. Ideales Primos Asociados

En este capítulo se estudiará la descomposición terciaria para un $R-$ *módulo* izquierdo donde R es un anillo que no necesariamente es conmutativo.
Recordemos que un anillo R es neteriano izquierdo si para cualquier cadena ascendente de ideales izquierdos $I_1 \subseteq I_2 \subseteq ... \subseteq I_n \subseteq ...$, existe un entero positivo m tal que $I_m = I_{m+1}$.

En este capítulo, daremos por hecho que R es un anillo neteriano izquierdo y los $R-$ *módulos* serán izquierdos.

Definición 5.1.1. *Si M es un $R-$ módulo izquierdo el anulador de M, es el conjunto $Ann(M) = \{r \in R | rm = 0$ para todo $m \in M\}$.*

Proposición 5.1.2. *Si R es un anillo y $M \in R-mod$, entonces $Ann(M)$ es un ideal bilateral.*

Demostración. Sea $r \in Ann(M)$, $\alpha \in R$ y $m \in M$, entonces $(\alpha r)(m) = \alpha(rm) = 0$. Por lo tanto $Ann(M)$ es un ideal izquierdo. Ahora $(r\alpha)(m) = r(\alpha m)$. Como M es $R-$ *módulo* izquierdo, entonces $\alpha m \in M$. Así $r(\alpha m) = 0$. Por lo tanto $Ann(M)$ es bilateral. ■

Definición 5.1.3. *Si R es un anillo diremos que un ideal bilateral $P \subsetneq R$ es ideal primo si para cuales quiera ideales bilaterales I, J tales que $IJ \subseteq P$, entonces $I \subseteq P$ o $J \subseteq P$.*

Notemos que en el caso de un anillo conmutativo con 1, las definiciones 5.1.3 y 1.1.1 son equivalentes.

Un anillo R se dice que es anillo primo si 0 es ideal primo de R.

Note que P es ideal primo de R si y solo sí R/P es un anillo primo.

Definición 5.1.4. *Sea M un $R-$módulo y $P \subseteq R$ un ideal bilateral. Diremos que P es asociado a M si existe $0 \neq L \subseteq M$ tal que $P = Ann(L') = Ann(L)$ para todo $0 \neq L' \subseteq L$.*

Proposición 5.1.5. *Si P es asociado a un $R-$módulo M, entonces P es un ideal primo.*

Demostración. Sea P el ideal asociado a M, entonces existe $0 \neq L \subseteq M$, tal que $P = Ann(L) = Ann(L'), \forall 0 \neq L' \subseteq L$. Consideremos I, J ideales bilaterales de R, tales que $IJ \subseteq P$. Supongamos que $J \nsubseteq P$, de donde existe $x \in J$ tal que $x \notin P$. Como $P = Ann(L)$ se tiene que $xL \neq 0$. Sea $L' = xL$, entonces $L' \subseteq L$. Así $P = Ann(L')$. Por otra parte $IJ \subseteq P$, entonces $IJL = 0$, de donde $I(JL) = 0$. Como $x \in J$, se sigue que $0 = I(xL) = IL'$. En conclusión $I \subseteq Ann(L') = P$. ■

Definición 5.1.6 *Si M es un $R-$módulo denotamos por $Ass(M)$ al conjunto de los ideales primos asociados a M.*

Note que si $I = Ann(L)$ es elemento máximo de la familia $F = \{Ann(K) \mid 0 \neq K$ es submódulo de $M\}$, entonces I es asociado a M. En efecto sea $I = Ann(L)$ con I máximo de F. Sea $0 \neq L' \subseteq L$ un submódulo, entonces $Ann(L) \subseteq Ann(L')$. Como $I = Ann(L)$ es máximo de F, entonces $Ann(L) = Ann(L')$. Para asegurar la existencia de estos máximos se asume que R es anillo neteriano izquierdo. De esta forma tenemos que la siguiente:

Proposición 5.1.7 *Si M es un $A-$módulo no cero, entonces $Ass(M) \neq \emptyset$.*

Proposicón 5.1.8 *Si $0 \to L \to M \to N \to 0$ es una sucesión exacta de módulos, entonces $Ass(L) \subseteq Ass(M) \subseteq Ass(L) \cup Ass(N)$.*

Demostración. Sea $I \in Ass(L)$ entonces para todo L' no cero submódulo de L se tiene que $Ann(L') = I$. Como todo submódulo de L es submódulo de M, entonces $I \in Ass(M)$. Por lo tanto $Ass(L) \subseteq Ass(M)$. Sea $P = Ann(K) \in Ass(M)$, entonces $P = Ann(K')$ para todo $0 \neq K'$ submódulo de $K \subseteq M$. Ya que $K \cap L = 0$ y la sucesión es exacta, entonces K es isomorfo a un submódulo de N y por lo tanto $P \in Ass(N)$.

Por otra parte, si $K \cap L \neq 0$ se sigue que $P = Ann(K')$ para todo $K' \neq 0$ submódulo de $K \cap L$, por lo que $P \in Ann(L)$. De donde tenemos que $Ass(M) \subseteq Ass(L) \cup Ass(N)$. ■

Proposición 5.1.9. $Ass(\bigoplus_{i\in H} M_i) = \bigcup_{i\in H} Ass(M_i)$.

Demostración. Sea $M = \bigoplus_{i\in H} M_i$ y $P \in Ass(M)$, entonces existe $L \subseteq M$, tal que $Ann(L') = Ann(L)$ para todo $0 \neq L' \subseteq L$. Por lo tanto si $x \in L$, entonces el cíclico $Rx \in L$ tiene la propiedad $Ass(Rx) = P$. Podemos suponer que L es cíclico. Como $L \subseteq M = \bigoplus_{i\in H} M_i$, entonces $L \subseteq M_1 \bigoplus M_2 \bigoplus ... \bigoplus M_n$. Así la demostración la podemos hacer por inducción y podemos reducir para el caso de una suma directa $M_1 \oplus M_2$. Consideremos la sucesión $0 \to M_1 \to M_1 \oplus M_2 \to M_2 \to 0$ entonces esta sucesión se escinde. Ahora aplicamos la Proposición 5.1.8 y tenemos que $Ass(M_1 \oplus M_2) \subset Ass(M_1) \cup Ass(M_2)$. La otra contención es clara. ■

Definición 5.1.10. *Sea M un $R-$módulo y N un submódulo de M. Diremos que N es esencial en M y lo denotamos por $N \subseteq_{es} M$ si para todo $0 \neq L \subset M$ se tiene que $L \cap N \neq 0$.*

Proiposición 5.1.11. *Sea $M \neq 0$ un $R-$módulo y $N \subseteq_{es} M$, entonces $Ass(M) = Ass(N)$.*

Demostración. Claramente tenemos que $Ass(N) \subseteq Ass(M)$. Ahora sea $P \in Ass(M)$, se sigue que existe $L \subset M$ tal que $Ann(L') = Ann(L)$ para todo $0 \neq L' \subseteq L$. Teniendo en cuenta que $N \subseteq_{es} M$, entonces $0 \neq L \cap N \subseteq N$. Ahora sea $L'' \subset L \cap N$. Como $L'' \subset L \cap N \subset L$, entonces $Ann(L'') = Ann(L \cap N) = Ann(L) = P$. Como $L \cap N \subset N$, se tiene que $P \in Ass(N)$. Así $Ass(M) \subseteq Ass(N)$. ■

Corolario 5.1.12 *Sea M un $R-$módulo y $E(M)$ la capsula inyectiva de M, entonces $Ass(M) = Ass(E(M))$.*

Demostración. Se sabe que $M \subseteq_{es} E(M)$. Ahora por la Proposición 5.1.7 tenemos el resultado. ■

Definición 5.1.13. *Un $R-$módulo M se dice que es uniforme o coirreducible si para cualesquiera L, N submódulos no cero de M se tiene que $L \cap N \neq 0$.*

Corolario 5.1.14. *Sea $M \neq 0$ un $R-$módulo, si M es uniforme, entonces $Ass(M)$ tiene un solo elemento.*

Demostración. Sea $0 \neq N \subseteq M$ un submódulo. Como M es uniforme, se sigue que $N \subseteq_{es} M$. Así por lo Proposición 5.1.8, tenemos que $Ass(N) = Ass(M)$. De donde $Ass(N) = Ass(M)$ para todo N submódulo de M. Ahora sea $P \in Ass(M)$, entonces existe $N \subseteq M$ tal que $Ann(N') = Ann(N) = P$ para todo $0 \neq N' \subseteq N$. Por lo tanto $Ass(N) = \{P\}$. En conclusión $Ass(M) = \{P\}$. ■

Definición 5.1.15. *Un $R-$módulo M tiene rango finito si existe un entero no negativo n tal que $E(M)$, es suma directa de n submódulos uniformes.*

Note que por [3, Lema 5.16] se tiene que si M es de rango finito, entonces cualquier otra descomposición de $E(M)$ en suma directa de submódulos uniformes tiene exactamente n sumandos.

Corolario 5.1.16. *Sea M un $R-$módulo si R tiene rango finito, entonces $Ass(M)$ es finito.*

Demostración. Por la Definición 5.1.15, tenemos que $E(M) = E_1 \bigoplus ... \bigoplus E_n$, donde cada E_i es módulo uniforme. Ahora por la Proposición 5.1.9 tenemos que $Ass(E(M)) = Ass(M_1) \cup ... \cup Ass(M_n)$. Así por los Corolarios 5.1.12 y 5.1.14 tenemos que $Ass(M) = Ass(E(M))$ es finito. ■

Definición 5.1.17. *Un $R-$módulo M es llamado coterciario si $Ass(M)$ consiste de un elemento, el cual denotaremos por $ass(M)$. Un submódulo L de M es terciario en M si M/L es un módulo coterciario.*

El Corolario 5.1.14 muestra que todo módulo uniforme es coterciario. Dado P un ideal primo, diremos que un submódulo L de M es $P-terciario$ en M si $Ass(M/L) = \{P\}$.

Proposición 5.1.18 *Si P es un ideal primo del anillo R, entonces P es un ideal izquierdo $P-terciario$.*

Demostración. Sea $B \in Ass(R/P)$, entonces existe $(I/P) \subseteq R/P$ tal que $B = Ann(J/P) = Ann(I/P)$ para toda $0 \neq J/P \subseteq I/P$. Afirmamos que $B = P$. En efecto, $P(I/P) = PI/P$. Como P es ideal bilateral, entonces $PI \subseteq P$. De donde tenemos que $(PI/P) = 0$. Por lo tanto $P \subseteq Ann(I/P) = B$. Ahora como $B(I/P) = \bar{0}$, se sigue que $BI \subseteq P$. Además P es ideal primo, con lo cual se tiene que $B \subseteq P$ o $I \subseteq P$. Como

$0 \neq (I/P)$, entonces $B \subseteq P$. En conclusión $B = P$. ■

Proposición 5.1.19 *Toda intersección de submódulos $P-$ terciarios de M es $P-$ terciaria en M.*

Demostración. Sean $\{L_i\}_{i\in I}$ submódulos $P-terciarios$ de M, entonces el monomorfismo $(M/\bigcap_{i\in I} L_i) \to \bigoplus_{i\in I}(M/L_i)$ muestra que $Ass(M/\bigcap_{i\in I} L_i) \subset \bigcup_{i\in I} Ass(M/L_i) = \{P\}$. Por lo tanto $Ass(M/\bigcap_i L_i) = \{P\}$. ■

Definición 5.1.20. Sea M un $R-módulo$ y $N \subseteq M$ un submódulo. Diremos que N es irreducible en M si para cualesquiera L y K submódulos de M tales que $N = L \cap K$ se tiene que $L \subseteq N$ o $K \subseteq N$.

Note que si N es irreducible en M, entonces M/N es uniforme. en efecto, sea N irreducible en M y sean $L/N \cap K/N = \bar{0}$ Así obtenemos que $L \cap K/N = \bar{0}$. Por lo tanto $L \cap K = N$. Como N es irreducible $L = N$ o $K = N$. Así $L/N = \bar{0}$ o $K/N = \bar{0}$, entonces M/N es uniforme. Por lo tanto M/N es coterciario, es decir $Ass(M/N)$ tiene un solo elemento.

Consideremos el módulo $E(R/P)$ para un ideal primo P. Este es un módulo coterciario, pero en general no inescindible, por que P no es necesariamente irreducible. Sin embargo, ya que R es anillo neteriano izquierdo, entonces hay una descomposición $E(R/P) = \bigoplus_{i\in I} E_i$ de módulos inyectivos inescindibles E_i.

Proposición 5.1.21. *Si P es un ideal primo y $E(R/P) = \bigoplus_{i\in I} E_i$, donde los E_i son módulos inyectivos inescindibles, entonces todos los E_i son isomorfos entre sí.*

Demostración. Por [6] Capitulo II sabemos que el anillo (izquierdo) clásico de cocientes Q de un anillo neteriano izquierdo R/P es una anillo simple. Así R/P tiene un anillo simple de cociente Q. Como R/P es esencial en Q como un R/P módulo y también es esencial como un $R-módulo$ izquierdo. Se sigue que la inclusión $(R/P) \to E(R/P)$ puede ser extendido a un monomorfismo $R-lineal$, $Q \to E(R/P)$, el cual es esencial. El anillo simple Q puede descomponerse en una suma directa mínima de ideales izquierdos B_j, los cuales son isomorfos entre si. Así se obtiene $(\bigoplus_{i\in I} E_i) = E(R/P) = (\bigoplus_j E(B_j))$. De el Teorema de Azumaya [6] Corolario V 5.5, tenemos que $E_i \cong E(B_j)$ para todo i, y por lo tanto todos los E_i son isomorfos. ■

Ahora daremos el siguiente resultado.

Proposición 5.1.22. *Sea M un $R-$módulo finitamente generado, entonces existe una cadena $(0) = M_0 \subset ... \subset M_n = M$ tal que*

1) *M_i es un submódulo terciario de M_{i+1};*

2) *M_{i+1}/M_i es anulado por su ideal primo asociado.*

Demostración. Haremos la desmotración pot inducción. Supongamos que M_0,..., M_{i-1} cumplen la proposición. Si $M_i \neq M$, entonces $Ass(M/M_i) \neq \emptyset$ y se tiene que existe $M_i \subset M$ tal que todo submódulo no cero de M_{i+1}/M_i es anulado por un ideal primo P_{i+1}. Como M es finitamente generado, entonces m es finito. Por lo tanto las condiciones (1) y (2) se satisfacen. ■

Definición 5.1.23. *(Descomposición Terciaria) Sea M un módulo finitamente generado. Una descomposición terciaria de un submódulo L de M se obtiene al escribir a L como una intersección finita $L = M_1 \cap ... \cap M_n$ donde cada M_i es terciario en M y*

i) La descomposición es irredundante,

ii) $ass(M/M_i) \neq ass(M/M_j)$ para $i \neq j$.

Proposición 5.1.24. *Sea M un $R-$módulo izquierdo y $L \subseteq M$ un submódulo finitamente generado, entonces tenemos lo siguiente:*

1) *L tiene descomposición terciaria.*

2) *Si $L = M_1 \cap ... \cap M_m = N_1 \cap ... \cap N_n$ son descomposiciones de L, entonces $m = n$ y $\{ass(M/M_i) \mid i = 1, ..., m\} = \{ass(M/N_j) \mid j = 1, ..., n\}$.*

Demostración. 1) Como R es anillo neteriano izquierdo y M un $R-$*módulo* izquierdo es finitamente generado, entonces por [6] Proposición 3.1 capitulo I tenemos que M es neteriano. Así L puede escribirse como una intersección irredundante $L = M_1 \cap ... \cap M_k$ de submódulos irreducibles M_i de M. Por lo tanto cada M_i es terciario en M. Para cada ideal primo $P \in \{ass(M/M_i)\}$, sea $M(P)$ la intersección de todos los M_i tales que son $P-terciarios$. Por la Proposición 5.1.19 tenemos que $M(P)$ es $P-terciario$ en M. Así tenemos que $L = \bigcap_P M(P)$ es la descomposición terciaria deseada.

2) Ahora veamos la unicidad. Sea $L = M_1 \cap ... \cap M_m$ cualquier descomposición terciaria de L en M. Consideremos el monomorfismo $(M/L) \to (M/M_1) \oplus ... \oplus (M/M_m)$. La irredundancia implica que M/L tiene una intersección no nula K_i con cada M/M_i. Por lo tanto hay monomorfismos $(K_1 \oplus ... \oplus K_m) \to (M/L) \to (M/M_1) \oplus ... \oplus (M/M_m)$. Ahora por las Proposiciones 5.1.8 y 5.1.9 obtenemos que $\bigcup_i Ass(K_i) \subset Ass(M/L) \subset \bigcup_i Ass(M/M_i)$. Pero cada M/M_i es coterciario y $Ass(K_i) \neq \emptyset$. Por lo tanto $Ass(K_i) = Ass(M/M_i)$. Se sigue que $\{ass(M/M_i) \mid i = 1, ..., m\} = Ass(M/L)$, y de esto se sigue la unicidad. ■

Note que si R es un anillo neteriano conmutativo, entonces cualquier ideal irreducible I es terciario en R, ya que R/I es uniforme. Además por la Proposición 3.1.10 sabemos que I es ideal primario. Por otra parte cada ideal es intersección finita de ideales irreducibles. Por lo tanto cada ideal en un anillo neteriano conmutativo tiene descomposición terciaria y es la misma que su descomposición primaria. Riley demuestra en [5] que la descomposición terciaria tiene una razonable generalización de la descomposición primaria de anillos Noetherianos no conmutativos.

Se puede mencionar otra forma de generalizar la descomposición primaria para anillos no conmutativos aunque no es tan buena como la descomposición terciaria. Sea M un R-módulo finitamente generado, un submódulo L de M es primario en M, si L es terciario en M y $P^n M \subseteq L$, donde $P = ass(M/L)$ para algún entero n. Así se pueden definir descomposiciones primarias análogamente a la descomposición terciaria. Una condición suficiente para la descomposición primaria de M es que cada submódulo irreducible sea primario.
En particular, todo ideal es primario si y solo si es terciario y contiene una potencia del ideal primo asociado. Esta condición puede ser reformulada en un anillo conmutativo de forma que rearmemos la definición tradicional de ideales primarios en un anillo conmutativo. Para cada ideal izquierdo I sea $\tilde{I}$ el ideal bilateral mas grande contenido en I, es decir $\tilde{I} = \{b \in R | Rb \subset I\}$. Se denota a $\sqrt{I}$ a la intersección de todos los ideales primos que contienen a $\tilde{I}$. Se puede demostrar que $\sqrt{I}$ es el mayor ideal bilateral de R tal que alguna potencia de $\sqrt{I}$ está contenida en I.

Bibliografía

[1] Atiyah M. F., Macdonald I. G. Introduction to commutative algebra. Addison Wesley, 1969.

[2] Castro P. J. C-Primary Descomposition for modules, JP Journal of Algebra, Number Theory and Applications, Volume 10, Number 1, 2008 Pushpa Publishing House.

[3] Goodearl K. R. and Warfield R. B., Jr. An Introduction to Noncommutative Noetherian Rings. London Mathematical Society, Student Texts 61. C, Cambridge University Press 2004.

[4] Lesieur. L. Croisot. R. I. Sur la décomposition en idéaux primaries dans un anneau non necessairement commutatif. C. R. Acad. Sci. París 243. 1988-1991 (1956).

[5] Riley J.A. Axiomatic primary and tertiary decomposition Theory. Trans. Amer. Math. Soc. 105, 177-201 (1962).

[6] Stenström Bo. Rings and Modules of Quotients. Springer-Verlag, 1975.