UNIVERSIDAD DE EL SALVADOR
FACULTAD DE CIENCIAS NATURALES
Y MATEMÁTICA
ESCUELA DE MATEMATICA

“TEORÍA DE MULTIPLICIDAD APLICADO A LA FÓRMULA LÍMITE DE SAMUEL”

TRABAJO DE GRADUACIÓN PRESENTADO POR:

MAIRA RAQUEL PÉREZ BENÍTEZ

PARA OPTAR AL TÍTULO DE:

LICENCIADA EN MATEMÁTICA

CIUDAD UNIVERSITARIA, Agosto de 2011

UNIVERSIDAD DE EL SALVADOR

Msc. RUFINO ANTONIO QUEZADA SÁNCHEZ

RECTOR

Lic. DOUEGLAS VLADIMIR ALFARO CHÁVEZ

SECRETARIO GENERAL

FACULTAD DE CIENCIAS NATURALES Y MATEMÁTICA

Dr. RAFAEL ANTONIO GÓMEZ ESCOTO

DECANO

Licda. MARIA TRINIDAD TRIGUEROS DE CASTRO

SECRETARIA

ESCUELA DE MATEMÁTICA

Ing. CARLOS MAURICIO CANJURA

DIRECTOR

UNIVERSIDAD DE EL SALVADOR FACULTAD DE CIENCIAS NATURALES Y MATEMÁTICA ESCUELA DE MATEMATICA

"TEORÍA DE MULTIPLICIDAD APLICADO A LA FÓRMULA LÍMITE DE SAMUEL"

TRABAJO DE GRADUACIÓN PRESENTADO POR:

MAIRA RAQUEL PÉREZ BENÍTEZ

PARA OPTAR AL TÍTULO DE:

LICENCIADA EN MATEMÁTICA

Licda. INGRID CAROLINA MARTÍNEZ BARAHONA

ASESOR DIRECTOR

Licda. CLAUDIA PATRICIA CORCIO BELTRÁN

ASESOR DIRECTOR

CIUDAD UNIVERSITARIA, Agosto de 2011

Agradecimientos

Esta tesis se la dedico a mi hija Karen Vanessa Sánchez Pérez que es lo más imporatnte en mi vida y mi hermano Luis Ernesto Benítez que me motivo en mi preparación acádemica.

Gracias a Dios

Mi gratitud, principalmente está dirigida al Dios Todopoderoso por haberme dado la existencia y permitido llegar al final de mi carrera. Gracias a él pudo ser posible.

Gracias a mi hermano Luis Ernesto Benítez

Gracias por tu cariño incondicional y por siempre confiar en mí. Además por ser parte de mi inspiración desde el primer año de mi carrera.

Gracias a mis padres Carlos Pérez y Luz Benítez

Quienes permanentemente me apoyaron con espíritu alentador, contribuyendo incondicionalmente a lograr las metas y objetivos propuestos.(Ambos están ante la presencia del Altísimo)

Gracias a mi esposo Jorge Alberto Sánchez Linares

Por tu apoyo, compresión y amor que me motiva a lograr lo que me propongo. Gracias por escucharme y por tus consejos. Gracias por ser parte de mi vida.

Gracias a mi asesora Licda. Ingird Carolina Martínez Barahona

Por su paciencia y opiniones que me sirvieron mucho para terminar mi proyecto de investigación . Además quien me ha orientado en todo momento con su asesoría técnica.

Gracias a mi asesora Licda. Claudia Patricia Corcio de Beltrán

Por su tiempo y dedicación al brindarme su apoyo para la terminación de la presente tesis.

Gracias a cada uno de los maestros

Que participaron en mi desarrollo profesional durante mi carrera, sin su ayuda y conocimientos no estaría en donde me encuentro ahora.

Gracias a todos mis amigos

A todas y todos quienes de una u otra forma han colocado un granito de arena para el logro de este Trabajo de investigación, agradezco de forma sinceramente su confianza en mí para que siguiera adelante.

Cantor:
"La esencia de la matemática reside en su libertad".

F. Maira Raquel Pérez Benítez

Índice general

Parte I

Introducción

Introducción

La matemática actual se caracteriza por el predominio del álgebra, y se habla a menudo de la algebrización de todas las ramas de la tradicional matemática. Esta tendencia se origina en los trabajos geniales de Galois para dar solución definitiva al problema de hallar las raices de las ecuaciones algebraicas, de donde surgió la noción de grupo. Más tarde apareció la teoría abstracta de grupos y otras teorías, como las de cuaternios y de matrices.
Además tanto los cuaternios como las matrices contradicen la ley conmutativa de la multiplicación de números, según la cual el orden de los factores no altera el producto, como en el caso de las geometrías no euclidianas, se llegó por esta vía a un grado de abstracción mayor de las operaciones aritméticas y algebraicas, que se definen hoy únicamente por los axiomas que se desee que cumplan.

Sin duda que la noción de grupo, en especial de grupo de Galois de la ecuación que constituye el tema central de Galois, estaba ya esbozada en los trabajos de Lagrange y de Alexandre-Theophile Vandermonde (1735-1796) del siglo XVIII, y en los de Gauss, Abel, Ruffini y Cauchy del XIX, implícita en problemas de teoría de las ecuaciones, teoría de números y de transformaciones geométricas, pero es Galois quien muestra una idea clara de la teoría general con las nociones de subgrupo y de isomorfismo.

La teoría de grupos culmina hacia 1880 al aparecer la teoría de los grupos abstractos (ya esbozada por Cayley en 1854), que confiere a la teoría iniciada por Galois los caracteres de estructura algebraica. Como tal estructura, y en virtud del isomorfismo, un grupo puede entonces estudiarse bajo el aspecto particular de uno de sus modelos o interpretaciones, bajo su forma general puramente abstracta como resultado de un proceso de rasgos propios, específicos de la matemática de hoy, que evidencia que la misma abstracción, ha cambiado o evolucionado a través de los tiempos.

En la actualidad el Álgebra Abstracta juega un papel muy importante en el estudio de la Matemática ya que en ella se involucran diversidad de contenidos lo que se centra en el estudio de conjuntos, estructura de grupo, categorías, anillos, módulos en donde estos se dividen en las importantes ramas de Campos y Teoría de Galois, Álgebra lineal, Anillos conmutativos y módulos y estructura de anillos entre otros. Toda esta teoría contribuye al estudio de el álgebra homológica dentro de la cual se prende desarrollar la Teoría de multiplicidad y en base a esta poder demostrar la fórmula límite de Samuel.

Capítulo 1

Anillos e Ideales

1.1. Anillos

Definición 1. *Un conjunto A dotado de dos operaciones binarias cerradas que escribiremos $+$ (suma) y $\cdot$ (producto) se llama **anillo** si se cumplen las siguientes propiedades:*

1. *$(A, +)$ es un grupo abeliano.*

2. *El producto $\cdot$ es asociativo.*

3. *Se cumplen las propiedades distributivas, es decir:*
   $a \cdot (b + c) = a \cdot b + a \cdot c$ ***ley distributiva a izquierda.***
   $(b + c) \cdot a = b \cdot a + c \cdot a$ ***ley distributiva a derecha.***

Definición 2. ***Grupo abeliano o conmutativo:*** *Para todo $x, y \epsilon M$*
$x * y = y * x$,***conmutatividad***.
*Todo **anillo** es un grupo abeliano con respecto a su adición. En un **anillo conmutativo**, los elementos invertibles forman un grupo abeliano bajo la multiplicación.*

Nótese que al producto $\cdot$ no se le impone ser conmutativo; de aquí que sea necesario especificar que se han de cumplir las propiedades distributivas por la derecha y por la izquierda.
Si el producto es conmutativo. A se dice que es un anillo conmutativo;
si existe un elemento, que simbolizaremos mediante 1, tal que para todo $a \in A$, $a1 = 1a = a$, A se dice que es un anillo con unidad; en este caso, el elemento 1, que recibe el nombre de elemento unidad,y es único.

Definición 3. *Un subconjunto S de un anillo $(A, +, \cdot)$ se dice que es un subanillo de A si $(S, +)$ es un subgrupo de $(A, +)$ y el producto $\cdot$ restringido* *a S es cerrado; de forma equivalente, la suma y el producto son operaciones cerradas sobre S y $(S, +, \cdot)$ es un anillo.*

Definición 4. *Un subanillo I de un anillo A se dice que es un ideal de A si para todo $i \in I$ y para todo $a \in A$, ai e ia pertenecen a I.*

El papel de los ideales de un anillo es similar al de los subgrupos normales dentro de la teoría de grupos. Si I es un ideal de un anillo la relación $x \equiv y(I)$ si y sólo si $x - y \in I$, es una realación de equivalencia.
En particular, el cociente A/I es un subgrupo respecto a la suma de clases $(r + I) + (s + I) = (r + s) + I$ y en analogía con esto se tiene la definición de un producto de clases: $(r + I)(s + I) = rs + I$

Definición 5. *Sea I un ideal de un anillo A; la suma y el producto de clases en el cociente A/I están bien definidas y, con estas, A/I posee una estructura de anillo.*

Definición 6. *Un subgrupo $(a, +)$ de un anillo A se dice:*

- ***ideal a izquierda*** *si $a \cdot a \subseteq A$ para todo $a \epsilon A$.*

- ***ideal a derecha*** *si $a \cdot a \subseteq A$ para todo $a \epsilon A$.*

- ***ideal o ideal bilario*** *si es a la vez ideal a derecha y a izquierda.*

- *Si A es conmutatitvo todo ideal es ideal a ambos lados.*

Definición 7.

Ideal maximal: *Un ideal M es maximal $\Longleftrightarrow$ existe exactamente dos ideales que contiene a M.*

Definición 8. *El nilradical de A es la intersección de todos los ideales primos de A.*

Definición 9. *El radical de Jacobson R de A se define como la intersección de todos los ideales maximales de A.*

Sin embargo, la intersección de todos los ideales maximales izquierdos siempre coincide con la intersección de todos los ideales maximales derechos.

1.2. Módulos

Definición 10. *Un **módulo izquierdo** sobre el anillo R consiste en un **grupo abeliano** $(M, +)$ y una operación $R \times M \to M$ (multiplicación escalar, es decir como rx para r en R y x en M) tal que:*
Para todo r, s en R, x, y en M, tenemos

1. $(rs)x = r(sx)$
2. $(r + s)x = rx + sx$
3. $r(x + y)x = rx + ry$
4. $1x = x$

generalmente, escribimos simplemente R-módulo izquierdo M o ${}_RM$

Definición 11. *Un **R-módulo derecho** o M_R se define de forma semejante, sólo que el anillo actúa por la derecha, es decir tenemos una multiplicación escalar de la forma $M \times R \to M$ y los tres axiomas se escriben con los escalares r y s a la derecha de x e y.*
*Si R es **Conmutativo**, entonces los R-módulo izquierdo son lo mismo que R-módulo a la derecha y se llaman simplemente R-módulos.*

Definición 12. *Suponga que M es un R-módulo izquierdo y N es un **subgrupo** de M. Entonces N es un **submódulo** (R-submódulo) si para cualquier n en N y cualquier r en R el producto rn está en N (o el nr para un módulo derecho).*

TIPOS DE MÓDULOS:

1. **Finitamente generado**. un módulo M es **finitamente generado** si existe un número finito de elementos $x_1, x_2, ..., x_n$ en M tales que cada elemento de M es una **combinación lineal** de esos elementos con coeficientes del anillo escalar R.

2. **Noetheriano**. un **módulo noetheriano** es un módulo tal que cada submódulo es finitamente generado. Equivalente, cada cadena creciente de submódulos llega a ser estacionaria en finitos pasos.

3. **Artiniano**. un **módulo artiniano** es un módulo en el cual cada cadena decreciente de submódulos llega a ser estacionaria en finitos pasos.

Definición 13. *Sea $(\Sigma, \leq)$ un conjunto parcialmente ordenado por una relación $\leq$ (es decir, $\leq$ es reflexiva y transitiva y es tal que $x \leq y$ e $y \leq x$ simultáneamente implica $x = y$).*
Las siguientes condiciones en Σ son equivalentes:

i) Cada sucesión creciente $x_1 \leq x_2 \leq ... \leq x_n \leq x_{n+1} \leq ...$ en Σ es estacionaria (es decir, existe un n tal que $x_n = x_{n+1} = ...$).

ii) Cada subconjunto $T \subset \Sigma$ no vacío de Σ tiene un elemento maximal. (con respecto a $\leq$)

Definición 14. *Diremos que M es **Artiniano** si satisface alguna de las siguientes condiciones:*

i) Todo cociente M/N, siendo N un submódulo de M, es finitamente cogenerado(si posee alguna colección de submódulos de M tal que su intersección es $\{0\}$)

ii) Toda sucesión decreciente de submódulo de M
*$M_1 \supset M_2 \supset ... \supset M_n \supset ...$ es **estacionaria o finita**.*

*iii) Todo conjunto S de submódulo de M tiene un elemento **minimal**, esto es, un submódulo M_0 tal que para todo elemento N de S que esté contenido por M_0 se tiene $N = M_0$.*

Definición 15. *Sea R un anillo conmutativo con unidad $1 \neq 0$ Un módulo sobre R es un grupo aditivo X juntamente con la función*

$$\mu : R \times X \to X$$

$$(\alpha, x) \to \mu(\alpha, x) = \alpha x$$

Satisface las condiciones siguientes:

i) $(\alpha + \beta)x = \alpha x + \beta x$
ii) $\alpha(x + y) = \alpha x + \alpha y$
iii) $\alpha(\beta x) = (\alpha\beta)x$
iv) $1x = x$

para cualquier $\alpha, \beta \in R$ y $x, y \in X$

Ejemplo 1. *Sea R el anillo Z de los enteros. Para cualquier grupo abeliano X, la función*

$$\mu : Z \times X \to X$$

$$(n, x) \to \mu(n, x) = nx$$

para todo $n \in Z,\ x \in X$

satisface que si $n_1, n_2 \in Z,\ x_1, x_2 \in X$
i.

$$\begin{aligned}\mu(n_1+n_2,x) &= (n_1+n_2)x \ \in X \\ &= n_1x+n_2x \\ &= \mu(n_1,x)+\mu(n_2,x)\end{aligned}$$

ii.

$$\begin{aligned}\mu(n,x_1+x_2) &= n(x_1+x_2) \ \in X \\ &= nx_1+nx_2 \\ &= \mu(n,x_1)+\mu(n,x_2)\end{aligned}$$

iii.

$$\mu(1,x) = 1x = x$$

Ejemplo 2. *Sea X un anillo con unidad 1 y R un subanillo conmutativo de X que contenga 1. Entonces la función $\mu : R \times X \to X$, definida por $\mu(\alpha, x) = \alpha x$ para todo ($\alpha \in R$ y $x \in X$), satisface las siguientes condiciones*

i)

$$\mu(\alpha+\beta,x) = (\alpha+\beta)(x) = \alpha x+\beta x = \mu(\alpha,x)+\mu(\beta,x)$$

se cumple la distributiva ya que $\alpha, \beta, x \in X$
ii)

$$\mu(\alpha,x_1+x_2) = \alpha(x_1+x_2) = \alpha x_1+\alpha x_2 = \mu(\alpha,x_1)+\mu(\alpha,x_2)$$

iii)

$$\mu[\alpha,\mu(\beta,x)] = \mu[\alpha,\beta x] = \alpha(\beta x) = \mu(\alpha\beta,x)$$

ya que estamos en el anillo X lo cumple
iv)

$$\mu(1x) = 1x = x$$

luego todo anillo X con unidad 1 es un módulo sobre cualquiera de sus subanillos conmutativos que contienen 1. En particular, todo anillo conmutativo con unidad puede ser considerado como módulo sobre sí mismo.

Ejemplo 3. *El conjunto $X = R^S$ de todas las funciones $f : S \to R$ de un conjunto S en R es un grupo abeliano respecto a la adición funcional definida por $(f+g)(s) = f(s)+g(s)$ para cualesquiera $f, g \in X$ y $s \in S$. La función $\mu : R \times X \to X$, definida asignando a cada elemento α, f de $R \times X$ la*

función $\alpha f : S \to R$*, dada por* $(\alpha f)(s) = \alpha[f(s)]$ *para todo* $s \in S$*, satisface las siguientes condiciones*
i)

$$\begin{aligned}
[\mu(\alpha+\beta, f)](s) \quad &= [(\alpha+\beta)f](s)\\
&= (\alpha+\beta)f(s)\\
&= \alpha f(s) + \beta f(s)\\
&= [\alpha f]s + [\beta f]s\\
&= [\alpha f + \beta f](s)\\
&= \mu(\alpha, f)(s) + \mu(\beta, f)(s)
\end{aligned}$$

ii)

$$\begin{aligned}
[\mu(\alpha, g+f)](s) \quad &= \alpha(g+f)(s)\\
&= \alpha(g(s) + f(s))\\
&= \alpha[g(s)] + \alpha[f(s)]\\
&= \mu[\alpha, g](s) + \mu[\alpha, f)](s)
\end{aligned}$$

iii)

$$\begin{aligned}
[\mu(\alpha\beta, f)](s) \quad &= [(\alpha\beta)f](s)\\
&= (\alpha\beta)f(s)\\
&= \alpha(\beta f(s))\\
&= \alpha[(\beta f)(s)]\\
&= [\alpha(\beta f)](s)\\
&= \mu[\alpha, \mu(\beta, f)](s)
\end{aligned}$$

Lema 1. *Para cualquier elemento* u *de* R*-módulo* X *se cumple*

$$0u = 0 \qquad (-1)u = -u$$

Prueba: En virtud de i) y iv), tenemos $u + 0u = (1+0)u = 1u = u$ por tanto $0u = 0$. Por otra parte, tenemos también

$$u + (-1u) = (1-1)u = 0u = 0$$

por tanto $(-1)u = -u$.||

1.2.1. Submódulos

Definición 16. *Sea X un R-módulo arbitrario, A un subconjunto no vacío de X entonces A es submódulo de X sí y solo sí*

i) A es subgrupo del grupo abeliano aditivo X
ii) $\forall \alpha \in X$ y $\forall x \in A$ entonces $\alpha x \in A$

Ejemplo 4. *Todo subgrupo A de un grupo abeliano aditivo X es un submódulo de X considerado como módulo sobre el anillo Z de los enteros.*

i. Sea $x, y \in A$, como A es submódulo sobre Z

$$\Rightarrow y^{-1} \in A \Rightarrow xy^{-1} \in A$$

por tanto A es subgrupo de X

ii. Sea $\alpha \in R$ $\; x \in A$. Como A es módulo sobre el anillo Z de los enteros entonces $\alpha x \in A$ $\; ; \alpha \in Z$

Lema 2. *Un subconjunto no vacío A de un R-módulo X es un submódulo de X sí y solo sí para cualesquiera que sean $\alpha \in R$ y $u, v \in X$, se tiene que $u + v \in A$ y $\alpha u \in A$.*

Prueba: $\Rightarrow$ Por definición de submódulo, como $A \neq \oslash$ y es un submódulo de X respecto a la adición y multiplicación escalar del módulo X se cumple que $u + v \in A$ $\; \alpha u \in A \Rightarrow$ Basta probar que el opuesto $-u$ de $u \in A$ esta en A (Por lema 1) $-u = (-1)$ $\; u \in A$. Entonces existe $\alpha = (-1)$ que satisface $\alpha u \in A$, además $u + v \in A$ ya que X es aditivo.||

Lema 3. *Sea A un submódulo de un R-módulo de X, entonces, para todo $\alpha \in R$ y $u \in X$, tenemos $\{\alpha(u + a) \; a \in A\} \subset \alpha u + A$*

Prueba: Sea A un submódulo de X entonces $\alpha a \in A$ $\; \forall a \in A$ por tanto

$$\alpha(u + a) = \alpha u + \alpha a \in \alpha u + A$$

ya que se cumple la ley distributiva.||

Lema 4. *La intersección de cualquier familia de submódulos de un R-módulo X, es un submódulo de X.*

Prueba: Consideremos una familia $\Phi = \{A_i / i \in M\}$ de submódulos de un R-módulo X y sea A su intersección $A = \bigcap_{i \in M} A_i$. A probar que A es un submódulo de X, sean $\alpha \in R$ $\; u, v \in A$ (por lema 2) hay que establecer $u + v \in A$ $\; \alpha u \in A$. Para eso consideremos un $i \in M$ arbitrario. Ya que $A \subset A_i$, A_i es un submódulo de X (por lema 2) $u + v \in A_i$ $\; \alpha u \in A_i$

y como esto es cierto para todo $i \in M$ entonces $u + v \in A$ $\alpha u \in A$. Por tanto A es submódulo de X.
Sea ahora S un subconjunto arbitrario de un R-módulo X. Entonces S esta contenido en al menos un submódulo de X, a saber, en el propio X. Por (lema 4), la intersección A de todos los submódulos de X que contienen S es un submódulo de X. Precisamente, A es el mínimo submódulo de X que contiene el subconjunto dado S, y recibe el nombre de submódulo engendrado por S. En el caso $A = X$, se dice que S es un sistema de generadores de X y que X esta engendrado por S.||

Definición 17. *Un elemento X de un R-módulo X se dice que es combinación lineal de elementos de un subconjunto S de X sí y solo si existe un numero finito de elementos $x_1, x_2, ...x_n$ de S tales que*

$$x = \sum_{i=1}^{n} \alpha_i x_i$$

donde $\alpha_1, \alpha_2, ...\alpha_n \in R$

Proposición 1. *El submódulo de un R-módulo X engendrado por un subconjunto S de X es el conjunto de todas las combinaciones lineales de elementos de S.*

Prueba: Sea A el conjunto de todas las combinaciones lineales de elementos de S. Por (Lema 2) A es un submódulo de X. Para cada $x \in S$, tenemos $x = 1x \in A$. Luego A contiene S. Sea B un submódulo de X que contenga S.Toda combinación lineal de elementos de S esta contenida en B. Luego $A \subset B$. Por tanto A es el mínimo submódulo de X que contiene S.

Concluimos la presente sección, definiendo algunas nociones que serán usadas en lo sucesivo. Siendo S y T subconjuntos cualesquiera de un R-módulo arbitrario X, su suma $S + T$ es el subconjunto X definido por

$$S + T = \{u + v/u \in S,\ v \in T\}$$

si S y T son submódulos de X, es evidente que también lo es $S + T$. Por otra parte, para todo subconjunto C de R, CS denota el subconjunto de X definido por

$$CS = \{\alpha u/\alpha \in C,\ u \in S\}$$

Definición 18. *Sea R un anillo con unidad 1, conmutativo o no.*
Un R-módulo por la izquierda es un grupo abeliano aditivo X juntamente con la función

$$\mu : R \times X \to X$$

que satisface las condiciones de módulo. Análogamente, definimos R-módulos por la derecha.

Proposición 2. *Probar que, si R es conmutativo, ambas nociones coinciden esencialmente.*

Prueba: Sea

$$\begin{aligned} \mu: \quad & R \times X \to X \\ & (r,x) \to \mu(r,x) = rx \end{aligned}$$

un R-módulo por la izquierda. Por hipotesis del ejercicio se satisface que para $r_1, r_2 \in R, \quad x_1 + x_2 \in X$

$$\begin{aligned} i) \quad & r(x_1+x_2) = rx_1 + rx_2 \\ ii) \quad & (r_1+r_2)x = r_1x + r_2x \\ iii) \quad & r(\alpha x) = (r\alpha)x \\ iv) \quad & 1x = x \end{aligned}$$

definamos R-módulos por la derecha

$$\begin{aligned} \mu: \quad & X \times R \to X \\ & (x,r) \to \mu(x,r) = xr \end{aligned}$$

entonces tenemos que

$$\begin{aligned} i) \quad & x(r_1+r_2) = xr_1 + xr_2 \\ ii) \quad & (x_1+x_2)r = x_1r + x_2r \\ iii) \quad & x(\alpha r) = (x\alpha)r \\ iv) \quad & 1r = r \end{aligned}$$

y obtenemos que las propiedades de un R-módulo por la izquierda y derecha son iguales. ||

Proposición 3. *Sea K un ideal de un anillo conmutativo con unidad R y x un elemento dado de un R-módulo X. Entonces el subconjunto de X*

$$A = Kx = \{\alpha x / \alpha \in K\}$$

es un submódulo.

Prueba. Dado que A es subconjunto de X. Sea u y $v \in A$ debemos probar que $v + v \in A$ y que $\alpha u \in A$ para todo $\alpha \in K, u = \alpha_1 x \quad \alpha_1 \in K \qquad v = \alpha_2 \in K$

$$\begin{aligned} u + v \quad & = \alpha_1 x + \alpha_2 x & \alpha u \quad & = \alpha(\alpha_1 x) \\ & = (\alpha_1 + \alpha_2) & & = (\alpha\alpha_1)x \\ & = \alpha_3 x \in A & & = \alpha_3 x \quad \text{para } \alpha\alpha_1 \in k \qquad || \end{aligned}$$

1.3. Sumas Directas

Consideremos una familia arbitraria dada

$$\Im = \{X_i / i \in M\}$$

de R-módulos X_i y designamos con $P = \prod_{i \in M} X_i$

el producto

$$\psi' = \sigma \circ \psi : \sum_{i \in M} X_i \rightarrow Y$$

se llamará suma directa *realizada* de la familia

$$\wp = \{h_i : X_i \rightarrow Y / i \in M\}$$

Si ψ' es isomorfismo, entonces

$$\sum_{i \in M} X_i \approx Y$$

y la familia $\wp$ se dice que es una representación inyectiva del módulo Y como suma directa. En particular, si X_i es un submódulo de un R-módulo X y si la familia

$$\wp = \{h_i : X_i \rightarrow X / i \in M\}$$

de homomorfismo inclusión es una representación inyectiva del módulo X como suma directa, entonces

$$\sum_{i \in M} X_i \approx X$$

en este caso decimos que el módulo es descomponible en la suma directa de los submódulos

$$\Im = \{X_i / i \in M\}$$

también diremos que el módulo X es la suma directa (interna) de sus submódulos $\Im$. Si $\Im$ es una familia finita de R-módulos,

$$\Im = \{X_1, X_2, ..., X_n\}$$

entonces la suma directa de $\Im$ se denota por

$$X_1 \oplus X_2 \oplus ... \oplus X_n$$

además, si cada X_i es un módulo de un R-módulo X, entonces

$$X = X_1 \oplus X_2 \oplus ... \oplus X_n$$

expresa que X es la suma directa de los submódulos $X_1, X_2, ..., X_n$.
El siguiente teorema es de gran utilidad.

Teorema 1. *Un R-módulo X es la suma directa de los submódulos A y B sí y sólo sí*

$$A + B = X, \quad A \bigcap B = 0$$

Prueba: $\Rightarrow$ Supongamos que X es la suma directa de A y B. Entonces, por definición, el homomorfismo definido

$$\begin{aligned} \psi' : \qquad & A \oplus B \rightarrow X \\ & (a,b) \rightarrow \psi'(a,b) = a + b \end{aligned}$$

es un isomorfismo.

Para probar que, $A + B = X$, sea $x \in X$. Como ψ' es un epimorfismo, existe un elemento $(a, b) \in A \oplus B$ tal que

$$x = \psi'(a,b) = a + b \in A + B$$

luego $x \in A + B$, y siendo x arbitrario, resulta $A + B = X$

Para probar $A \bigcap B = 0$ por contradicción suponemos que $A \bigcap B$ contiene un elemento no nulo $x \in X$. Como $A \bigcap B$ es un submódulo de X, tenemos $-x \in A \bigcap B$. Entonces $-x, x$ es un elemento no nulo de $A \oplus B$. Puesto que

$$\begin{gathered} \psi'(-x, x) = x - x = 0, \\ \Rightarrow (x, -x) \in Ker(\psi') \end{gathered}$$

y como $(-x, x)$ es un elemento no nulo ψ'. No es un monomorfismo $\rightarrow\leftarrow$, entonces $A \bigcap B = 0$

$\Leftarrow$ Supongamos que $A + B = X,\ A \bigcap B = 0$. Debemos probar que ψ' es un isomorfismo. Sea $x \in X$. Como $A + B = X$, existen $a \in A$ y $b \in B$ tales que $a + b = x$. Esto implica

$$\psi'(a,b) = a + b = x$$

por lo que ψ' es un epimorfismo. Sea $x \in X$. Entonces

$$a + b = \psi'(a + b) = 0$$

se deduce que $a \in A$ y $a = -b \in B$. Luego $a \in A \bigcap B$. Como $A \bigcap B = 0$, es $a = 0$ y $b = -a = 0$. Por tanto (a, b), es el elemento cero $\{(0, 0)\} \in A \oplus B$. Así $Ker(\psi') = 0$, ψ' es un monomorfismo. Por tanto

$$\psi' \text{ es un isomorfismo } \quad ||$$

Teorema 2. *Si el producto $h = g \circ f$ de los homomorfismos $f : X \rightarrow Y$ y $g : Y \rightarrow Z$ de R-módulos X, Y, Z es un isomorfismo, entonces se cumple:*

i) *f es monomorfismo.*

ii) *g es epimorfismo.*

iii) *El módulo Y es descomponible en la suma directa de $Im(f)$ y $Ker(g)$; en símbolos,*

$$Y = Im(f) \oplus Ker(g)$$

Prueba: i) Si h es monomorfismo entonces f es monomorfismo. Sabemos que como $ker(h) = 0$ entonces $x \in Ker(h) \Leftrightarrow h(x) = 0$. Sea $x \in Kerf$, como

$$\begin{aligned} h(x) \quad &= (g \circ f)(x) \\ &= g(f(x)) \\ &= 0 \\ &\Rightarrow x = 0 \quad \text{Porque } h \text{ es monomorfismo} \\ &\Rightarrow Ker(f) = 0 \end{aligned}$$

por tanto f es monomofismo.
ii. Si h es epimorfismo entonces g es epimorfismo

Sabemos que $h(x) = z \in Z$ por ser h sobreyectiva. Sea $z \in Z$ necesito definir un elemento $y \in Y$ tal que $g(y) = z \in Z$, como
$h(x) = (g \circ f)(x) = g(f(x)) = z \in Z$

Si $\qquad y = f(x) \in Y \qquad g(y) = z \in Z$. Por tanto g es epimorfismo.
iii. Sea $A = Im(f)$ y $B = Ker(g)$

$$X \xrightarrow{f} Y \xrightarrow{g} Z$$

sea y un elemento arbitrario de Y, y sea $z = g(y) \in Z$. Como $h : X \to Z$ es un isomorfismo, existe un elemento $x \in X$ tal que $h(x) = z$

$$\begin{array}{c} \overset{h=g\circ f}{\longrightarrow} \\ X \xrightarrow{f} \ Y \xrightarrow{g} \ Z \\ \quad y \to g(y) = z \\ x \to h(x) = z \end{array}$$

sean $a = f(x) \in A$ y $b = y - a$. Entonces

$$g(b) = g(y - a) = g(y) - g(a) = z - g(f(x)) = z - h(x) = z - z = 0$$

$$g(b) = 0 \Rightarrow B \in Ker(g) = B$$

y de lo anterior

$$\begin{array}{ccccc} & & a \in A = Im(f) & & \\ X & \xrightarrow{f} & Y & \xrightarrow{g} & Z \\ & & b \in B = Ker(g) & & \end{array}$$

luego $b \in B$, por lo que $y = a + b \in A + B$. Como y es arbitrario, deducimos que $A + B = Y$.

Para probar que $A \bigcap B = 0$, consideremos $y \in A \bigcap B$. Como $y \in A$, existe un elemento $x \in X$ tal que $f(y) = y$. Como $y \in B = Ker(g)$, tenemos $g(y) = 0$. Entonces

$$h(x) = g(f(x)) = g(y) = 0$$

puesto que g es un isomorfismo, deducimos que $x = 0$, y de aquí

$$y = f(x) = f(0) = 0$$

por tanto $A \bigcap B = 0$. Por (teor. 2), Y es la suma directa de los submódulos A y B. Por tanto

$$Y = Im(f) \oplus Ker(g) \quad ||$$

Proposición 4. *Un proyector de un R-módulo es un endomomorfismo ρ del módulo X que satisface $\rho \circ \rho = \rho$. Sea X un R-módulo que es la suma directa de una familia*

$$\Im = \{X_i / i \in M\}$$

de submódulos de X. Probar que existe una unica familia

$$\{\rho_i : X \to X / i \in M\}$$

de proyectores de X tales que $\rho_i(X) = X_i$ y $\rho_i(X_j) = 0$ si $i \neq j$.
Además, para todo elemento $x \in X$, es $\rho_i(x) = 0$ para todo índice $i \in M$ salvo a lo sumo en un número finito de ellos.

Prueba: Sea la sucesión de funciones

$$X \xrightarrow{\pi_i} X_i \xrightarrow{i_i} X$$

en donde

i_i: es la función inclución
π_i: función proyección
$\rho_i = i_i \circ \pi_i$

y se satisface que

$$\begin{aligned}\rho\circ\rho &= (i_i\circ\pi_i)(i_i\circ\pi_i)\\ &= i_i\circ(\pi_i\circ i_i)\circ\pi_i\\ &= i_i\circ\pi_i\\ &= \rho\end{aligned}$$

entonces tenemos que

$$\begin{aligned}\rho_i(X) &= (i_i\circ\pi_i)(X) & \rho_i(X-j) &= (i_i\circ\pi_i)(X_j)\\ &= i_i(\pi_i(X)) & &= i_i(\pi_i(X_j))\\ &= i_i(X_i) & &= i-i(0)\\ &= X_i & &= 0\end{aligned}$$

Proposición 5. *Sea $\wp=\{h_i : X_i\to X/i\in M\}$ una representación inyectiva del R-módulo X como suma directa. Entonces existe un única familia*

$$\Im=\{g_i; X\to X_i/i\in M\}$$

de homomorfismos de módulos tal que el producto

$$g_k\circ h_j : X_j\to X_k$$

es el homomorfismo trivial si $j\neq k$ y es el homomorfismo identidad si $j=k$. Por tanto, para cada $i\in M$, h_i es un monomorfismo y g_i es un epimorfismo. Ademas, tenemos también

$$X=Im(h_i)\oplus Ker(g_i)$$

para todo $i\in M$. Las dos familias $\wp$ y $\Im$ se dice que constituyen una representación completa del módulo X como suma directa

$$\begin{array}{ccccc} X_j & \xrightarrow{h_j} & X & \xrightarrow{g_k} & X_k\\ x_j & \to & (x_i)_i\in M=\begin{cases}x_j, & i=j\\ 0, & i\neq j\end{cases} & \to x_k = & \begin{cases}x_k=x_j, & k=j\\ x_h=0, & k\neq j\end{cases}\end{array}$$

por tanto $(g_k\circ h_k)(x_j)=x_j$ si $k=j$ me induce el homomorfismo identidad y $(g_k\circ h_k)(x_j)=0$ si $k\neq j$ me induce el homomorfismo trivial.
Como $(g_k\circ h_k)(x_j)$ es el homomorfismo identidad si $k=j$. Entonces

$$(g_k\circ h_j)(x_j)=(g_j\circ h_j)(x_j)=g_j(h_j(x_j))=g_j(x_j)=x_j$$

Por tanto

$$(g_k \circ h_j)(x_j) = x_j$$

por tanto h_i es monomorfismo y g_k es epimorfismo
Además obtenemos también que

$$X = Im(h_i) \oplus ker(g_i) \qquad ||$$

1.4. Sucesiones Exactas

Una sucesión exacta de módulos es una sucesión finita o infinita

$$.... \longrightarrow X \xrightarrow{f} Y \xrightarrow{g} Z \longrightarrow ...$$

de homomorfismos de R-módulos tal que la imagen del homomorfismo entrante coincide con el núcleo del homomorfismo saliente de todo módulo distinto de los extremos (*si existen*) de la sucesión.
Por ejemplo, en el módulo Y, deberá ser $Im\,(f) = Ker\,(g)$ Una sucesión exacta de la forma

$$0 \longrightarrow X \xrightarrow{f} Y \xrightarrow{g} Z \longrightarrow 0$$

se llama sucesión exacta corta.

Como ejemplo de sucesión exacta consideremos un submódulo arbitrario E de un R-módulo X y el módulo cociente $Q = X/E$. Como el homomorfismo inclusión $i : E \to X$ es un monomorfismo ya que para todo $x \in E$ al aplicarle la función $i\,(e) = e$.

$$i : E_x \longrightarrow X_{i(x)=x}$$

la proyección natural $p : X \to Q$ es un epimorfismo, y

$$Im\,(i) = E = Ker\,(p)$$

obteniéndose una sucesión exacta corta

$$0 \longrightarrow E \xrightarrow{i} X \xrightarrow{p} Q \longrightarrow 0$$

recíprocamente, consideremos una sucesión exacta corta arbitraria

$$0_o \longrightarrow A_{f'(0)=0} \xrightarrow{f} X \xrightarrow{g} B \longrightarrow 0$$

para todo elemento que tomemos en 0, tenemos que:

$$Im\,(f') = 0,\ Ker\,(f) = 0$$

por tanto f es monomorfismo.
Para ver que g es sobreyectiva tenemos que:

$$B_{para\ todo\ b} \longrightarrow \left\{0_{g'(b)=0}\right\}$$

entonces

$$Ker\left(g'\right) = \{b \in B | g\left(b\right) = 0\}$$
$$\Rightarrow Im\left(g\right) = Ker\left(g'\right)$$

por tanto g es epimorfismo. De la exactitud, se deduce que $Im\left(f\right) = Ker\left(g\right)$.

Sea E este submódulo común $Im\left(f\right) = Ker\left(g\right)$ de X.

$$0 \longrightarrow A \longrightarrow Im\left(f\right) = Ker\left(g\right) \longrightarrow 0$$

Entonces f define un isomorfismo $j : A \to E$ y g induce un isomorfismo $k : Q \to B$ del módulo cociente $Q = X/E$. Si identificamos los módulos A y B con los módulos E y Q por medio de los isomorfismos j y k^{-1}, la sucesión exacta corta dada se convierte en

$$0 \longrightarrow E \longrightarrow X \longrightarrow Q \longrightarrow 0$$

por tanto, podemos decir que una sucesión exacta corta es simplemente otro nombre para un submódulo y su módulo cociente.

Como ejemplo de sucesión exacta más larga, considemos un homomorfismo arbitrario $h : X \to Y$ de un R-módulo X en un R-módulo. Y Consideremos el núcleo y el conúcleo de h:

$ker\left(h\right) \subset X$, $Coker\left(h\right) = Y/Im\left(h\right)$. Sea $i : Ker\left(h\right) \to X$ el homomorfismo inclusión y $p : Y \to Coker\left(h\right)$, la proyeción natural. Veamos que obtenemos una sucesión exacta

$$0 \longrightarrow Ker\left(h\right) \xrightarrow{i} X \xrightarrow{h} Y \xrightarrow{p} Coker\left(h\right) \longrightarrow 0$$

llamada sucesión exacta corta del homomorfismo h. Veamos que es exacta en X. Sea $a \in Ker\left(h\right)$ como i es el homomorfismo inclusión y $i\left(a\right) = a$

$$Im\left(i\right) = \{a \in Ker\left(h\right) | i\left(a\right) = a\} = Ker\left(h\right)$$

por tanto es exacta en X, por que $Im\left(i\right) = Ker\left(h\right)$

veamos que es exacta en Y. Sea $y \in Ker\left(\rho\right)$ tal que

$$\begin{aligned} \rho\left(y\right) &= y + Im\left(h\right) \\ &= 0 + Im\left(h\right) \\ \Rightarrow Ker\left(\rho\right) &= Im\left(h\right) \\ \Rightarrow y \in Im\left(h\right) & \end{aligned}$$

por tanto la sucesión del homomorfismo h es exacta.

Teorema 3. *En una sucesión exacta arbitraria*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$$

de homomorfismos de R- módulos, las siguientes tres proposiciones son equivalentes:

a) *f es un epimorfismo.*

b) *g es el homorfismo trivial.*

c) *h es un monomorfismo.*

Prueba: $(a) \Leftrightarrow (b)$. Por definición, f es un epimorfismo sí y solo sí $Im\,(f) = B$. Por otra parte, g es el homomorfismo trivial sí y sólo sí $Ker\,(g) = B$. Debido a la exactitud, tenemos $Im\,(f) = Ker\,(g)$. Luego $(a) \Leftrightarrow (b)$.

$(b) \Leftrightarrow (c)$. Por definición, g es el homomorfismo trivial sí y sólo sí $Im\,(h) = 0$. Además h es un monomorfismo sí y sólo sí $ker\,(h) = 0$. Por la exactitud tenemos, $Im\,(g) = Ker\,(h)$. Luego $(b) \Leftrightarrow (c)$.

Corolario 1. *En una sucesión exacta arbitraria*

$$A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D \xrightarrow{k} E$$

de homomorfirmos de R-módulos, $C = 0$ sí y sólo sí f es un epimorfismo y k es un monomorfismo.

Demostracion: Necesidad: Supongamos que $c = 0$.

$$Ker\,(h) = 0$$

$$Im\,(g) = 0$$

Entonces g y h son homomorfismos triviales. Luego, f es un epimorfismo y k es un monomorfismo.

Suficiencia: Supongamos que f un epimorfismo y k un monomorfismo.
Tal que g y h son homomorfismos triviales. Se deduce que la $Im\,(g) = 0$ y el $Ker\,(h) = C$. Por la exactitud , tenemos que:

$$Im\,(g) = Ker\,(h)$$

luego $C = 0$.

Corolario 2. *Si una sucesión $0 \to C \to 0$ de R-módulos es exacta, entonces $c = 0$.*

Prueba:

$$0 \xrightarrow{f} C \xrightarrow{g} 0$$

por la exactitud $Im\,(f) = Ker\,(g)$

$$Im\,(f) = 0 \; y \; Ker\,(g) = c$$

, $\Rightarrow C = 0.||$

Corolario 3. *En una sucesión exacta arbitraria*

$$A \xrightarrow{d} B \xrightarrow{f} C \xrightarrow{g} D \xrightarrow{h} E \xrightarrow{k} F$$

Las siguientes proposiciones son equivalentes:

a) *g es isomorfismo.*

b) *f y h son homomorfismos triviales.*

c) *d es epimorfismo y k es monomorfismo.*

Prueba: $(a) \Leftrightarrow (b)$ y $(b) \Leftrightarrow (c)$

Corolario 4. *Si la sucesión*

$$0 \rightarrow C \xrightarrow{g} D \rightarrow 0$$

de homomorfismos de R-módulos es exacta, entonces g es isomorfismo.

Prueba: Sea

$$0_0 \longrightarrow C_{f(0)=0} \longrightarrow D \longrightarrow 0$$

Entonces $Im\,(f) = 0$, por la exactitud, tenemos que:

$$Im\,(f) = ker\,(g)$$

$$\Rightarrow Ker\,(g) = 0$$

$$\Rightarrow \; g \, esmonomorfismo$$

veamos que es sobreyectiva: $Im\,(f) = 0$; por la exactitud.
Sea $c \in C \;\Rightarrow\; g\,(c) = d$

$$\Rightarrow \; Im\,(g) = \{d \in D |\; D \in Ker\,(h)\} = Ker\,(h)$$

Por tanto g es epimorfismo. Por tanto g es isomorfismo. Se dice que una sucesión exacta

$$... \longrightarrow X \xrightarrow{f} Y \xrightarrow{g} Z \longrightarrow ...$$

se descompone en el módulo Y; o es descomponible en Y, sí y sólo sí el submódulo $A = Im\,(f) = Ker\,(g)$ de Y en el sumando directo de Y. Es decir, sí y sólo sí Y se descompone en suma directa de A y otro submódulo. Si la sucesión exacta es descomponible en cada uno de sus módulos no extremos , decimos que se descompone o que es descomponible. Puesto que un sucesión exacta corta

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

por lo tanto se descompone en A y C, es descomponible sí y sólo sí lo es en B.||

Teorema 4. *Si una sucesión exacta*

$$... \longrightarrow X \xrightarrow{f} Y \xrightarrow{g} Z \longrightarrow ...$$

de homomorfismos de R-módulos se descompone en el módulo Y, entonces Y es isomorfo a la suma directa $Im\,(f) \oplus Im\,(g)$

Prueba: Por definición, Y se descompone en la suma directa del módulo $A = Im\,(f)$ y otro submódulo B. Basta probar que $B \approx Im\,(g)$. Para ello, consideremos la restricción $h = g|B : B \to Z$ entonces h es un homomorfismo del módulo B en el módulo Z. Como

$$Ker\,(g) = Im\,(f) = A,\ A \cap B$$

se sigue que $Ker\,(h) = \{0\}$, entonces h es un monomorfismo. Queda por establecer que $Im\,(h) = Im\,(g)$. Sea $z \in Im\,(g)$ arbitrariamente dado.
Entonces existe un elemento $y \in Y$ tal que $g\,(y) = z$.
Como $Y = A + B$, existen elementos $a \in A$ y $b \in B$ con $y = a + b$. Entonces tenemos:

$$\begin{aligned} z \quad &= g\,(y) \\ &= g\,(a+b) \\ &= g\,(a) + g\,(b) \\ &= g\,(b)\,,\ g\,(a) = 0\ \textit{por que}\ Ker\,(g) = A \\ &= h\,(b) \end{aligned}$$

y como $h\,(b) = g\,(b)$ por como esta definido, ya que $a \in A$ y $b \in B$. Por tanto

$$Im\,(h) = Im\,(g)$$

Corolario 5. *Si una sucesión exacta corta*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

de homomorfsmos de R-módulos se descompone, entonces B es isomorfo a la suma direta $A \oplus C$.

Prueba: Similar a la prueba anterior.||

Corolario 6. *Una sucesión exacta arbitraria*

$$... \longrightarrow X \xrightarrow{f} Y \xrightarrow{g} Z \longrightarrow ...$$

de homomorfismos de R-módulos se descompone en el módulo Y si existe un homomorfismo $h : Y \rightarrow X$ *tal que el producto* hof *es un automorfismo del módulo X. En este caso, tenemos*

$$Y \approx Im\,(f) \oplus Im\,(g) \approx X \oplus Im\,(g)$$

Prueba: Tenemos que si $h = gof$ de dos homomorfismos $f : X \longrightarrow Y$ y $g : Y \longrightarrow Z$ de R-módulos X,Y,Z es un isomorfismo entonces se cumple:

i) f es monomorfismo.

ii) g es epimorfismo.

iii) El módulo Y es descomponible en la suma directa de $Im\,(f)\;\; y\; Ker\,(g)$ en simbolos:

$$Y = Im\,(f) \oplus Im\,(g)$$

$$... \longrightarrow X \xrightarrow{f} Y \xrightarrow{g} Z \longrightarrow ...$$

$$f\,(x) = y$$

$$h\,(y) = x$$

$\Rightarrow Im\,(f) = y$, h es sobreyectiva, f es inyectivo.

$Im\,(f) \approx X$ Por que f es sobreyectiva e inyectiva por corolario 11
$X \longrightarrow Im\,(f)$, $X \cong Im\,(f)$

Corolario 7. *Una sucesión exacta arbitraria*

$$... \longrightarrow X \xrightarrow{f} Y \xrightarrow{g} Z \longrightarrow ...$$

de homomorfismos de R-módulos se descompone en el módulo Y si existen un homomorfismo $k : Z \rightarrow Y$ *tal que el producto* gok *es un automorfismo del módulo Z. En este caso, tenemos*

$$Y \approx Im\,(f) \oplus Im\,(g) \approx Im\,(f) \oplus Z$$

.

Prueba: Similar a la demostracion anterior.||

Sea $f : X \to Y$ un homomorfismo arbitrario de un R-módulo X e un R-módulo Y. Un inverso por la izquierda de f, es un homomorfismo

$$h : Y \to X$$

tal que el producto hof es el automorfismo identidad del módulo X. Analogamente, un inverso por la derecha de f es un homomorfismo

$$k : Y \to X$$

tal que el producto fok es el automorfismo identidad del módulo Y. Entonces se tiene el siguiente corolario.

Corolario 8. *Para cualquier sucesión exacta corta*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

de homomorfismos de R-módulos, las proposiciones siguientes son equivalentes:

a) *La sucesión exacta corta se descompone.*

b) *El homomorfismo f tiene un inverso por la izquierda.*

c) *El homomorfismo g tiene un inverso por la derecha.*

Prueba: $(a) \Rightarrow (b)$ y $(a) \Rightarrow (c)$. Para ello, supongamos que la sucesión exacta corta dada se descompone. Sea $D = Im\,(f) = Ker\,(g)$. Por definición,el módulo B se descompone en la suma directa de su submódulo D y otro submódulo E de B. Observemos que f es un monomorfismo y por tanto define un isomorfismo $i : A \to D = Im\,(f)$. Sea $x \in B$ arbitrariamente dado. Entonces existen elementos $u \in D$ y $v \in E$ unicamente determinados.
Se puede comprobar fácilmente que la correspondencia.

$$x \to h\,(x) = i^{-1}\,(u)$$

define un homomorfismo $h : B \to A$ que es el inverso por la izquierda de f. Para establecer (c), observemos que g es un epimorfismo con D como núcleo. Puesto que $D \cup E = 0$, se deduce que la restriccion $j = g|E : E \to C$ es un isomorfismo.
Por ello, la correspondencia, $x \to k\,(x) = j^{-1}\,(x)$ para todo $x \in C$ define un homomorfismo $k : C \to B$ que es inverso por la derecha de g.

Capítulo 2

Módulos y Anillos Noetherianos

2.1. Anillos Noetherianos y Artinianos

Muchos anillos de importancia, tanto en geometría algebraica como en teoría de números, satisfacen ciertas condiciones de finitud que se suelen expresar mejor, siguiendo a Noether y Artin, en términos de condiciones de cadena en sus ideales. Ejemplos de especial importancia son los anillos de polinomios con coeficientes en un campo $K[X_1, X_2, ..., X_n]$ y el anillo de enteros $\mathbb{Z}$.

Definición 19.

Anillos noetherianos. *Un anillo A es noetheriano si todos sus ideales son finitamente generados.*

Proposición 6. *Si A es anillo, son equivalentes:*

(1) *A es noetheriano.*

(2) *Toda cadena ascendente de ideales propios*

$$I_1 \subseteq I_2 \subseteq ... \subseteq I_n \subseteq ...$$

se estaciona,es decir, existe un entero m tal que $I_m = I_{m+1} = ...$

(3) *Todo conjunto no vacío de ideales propios de A tiene un elemento máximo,es decir, un ideal que no está contenido en ninguno de los ideales de la familia dada.*

Prueba . (1) $\Rightarrow$ (2) : Sea $I := \bigcup I_j$. Como los ideales I_j están encadenados, entonces I es un ideal de A y es propio porque los I_j lo son.
Por hipótesis I es finitamente generado, digamos $I = (a_1, ..., a_n)$, donde notamos que para m suficientemente grande se tiene que $a_i \in I_m$ y por lo tanto $I \subseteq I_m$, es decir, $I_k = I_m$ para todo $k \geq m$.
(2) $\Rightarrow$ (3) : Si F es una familia no vacía de ideales propios de A que no contiene un elemento máximo, entonces para cualquier $I_1 \in F$ existe un $I_2 \in F$ tal que $I_1 \nsubseteq I_2$.
De esta manera se construye una cadena que no se estaciona.
(3) $\Rightarrow$ (1) : Si $I \nsubseteq A$ es un ideal propio, sea F la familia de ideales contenidos en I de la forma $(a_1, ..., a_m)$. Por hipótesis esta familia tiene un elemento máximo, digamos $(a_1, ..., a_n)$.
Entonces, para todo $a \in I$ se tiene que $(a_1, ..., a_n, a) \subseteq (a_1, ..., a_n)$,
y como éste es máximo se sigue que $(a_1, ..., a_n, a) = (a_1, ..., a_n)$ y por lo tanto $a \in (a_1, ..., a_n)$ y así $I = (a_1, ..., a_n)$.

Ejemplo 5. *El anillo $\mathbb{Z}$ es un DIP y por lo tanto es noetheriano.*
Todo campo K es noetheriano y el anillo de polinomios $K[X_1, X_2, ..., X_n]$ también es noetheriano por el teorema siguiente:

Teorema 5.

Teorema de la base de Hilbert *Si A es un anillo noetheriano, entonces $A[x]$ también lo es. En particular, si K es un campo, entonces el anillo de polinomios $K[X_1, X_2, ..., X_n]$ es noetheriano.*

Prueba. La segunda afirmación se sigue de la primera por inducción.
Para demostrar la primera afirmación, mostraremos que si $A[x]$ no fuera noetheriano entonces A no lo es. Supongamos entonces que $A[x]$ no es noetheriano y sea $I \subseteq A[x]$ un ideal que no es finitamente generado. Sea $f_1 \in I$ de grado minimo. Escojamos $f_2 \in I - (f_1)$ de grado menor (el cual existe porque I no es finitamente generado).
Iterando este proceso, escojamos $f_{k+1} \in I - (f_1, ..., f_k)$ de grado menor.
Por la elección de los f_i, sus grados n_i satisfacen que $n_1 \leq n_2$... Más aún, si a_i es el coeficiente de grado de f_i, entonces

$$(a_1) \subseteq (a_1, a_2) \subseteq ... \subseteq A$$

es una cadena de ideales de A que no se estaciona, ya que si lo hiciera, digamos

$$(a_1, ..., a_k) = (a_1, ..., a_k, a_{k+1})$$

se tendría una igualdad de la forma

$$a_{k+1} = \sum_{i=1}^{k} r_i a_i \text{ con los } r_i \in A$$

y poniendo

$$g := f_{k+1} - \sum_{i=1}^{k} r_i x^{n_{k+1}-n_i} f_i \in I - (f_1, ..., f_k)$$

este es un polinomio de grado $gr(g) < gr(f_{k+1})$ porque el coeficiente a_{k+1} de f_{k+1} se cancela en

$$a_{k+1}x^{n_k+1} - \sum_{i=1}^{k} r_i x^{n_{k+1}-n_i} a_i x^{n_i} = a_{k+1}x^{n_{k+1}} - \sum_{i=1}^{k} r_i a_i x^{n_{k+1}} = 0$$

porque $\sum_{i=1}^{k} r_i a_i = a_{k+1}$, lo cual contradice la minimalidad del grado de f_{k+1}.

Lema 5. *En un anillo noetheriano todo conjunto de generadores de un ideal contiene un conjunto finito de generadores.*

Prueba. Si $I = A$, $1 \in I$ se puede escribir como $1 = r_1a_1 + ... + r_na_n$ con los a_i en cualquier conjunto de generadores de I. Se sigue que I está generado por $a_1, ..., a_n$. Supongamos ahora que $I \not\subseteq A$ es un ideal propio y sea A un conjunto de generadores de I.
Sea F el conjunto de ideales generados por subconjuntos finitos de A. Como A es noetheriano F tiene un elemento máximo m y este m debe contener a todos los elementos de A (si no fuera así añadiendo cualquier otro elemento de A a los generadores de m se obtendría otro ideal mayor que m) y por lo tanto $m = I$.

Definición 20.

Anillos artinianos. *Un anillo A es artiniano si toda cadena descendente de ideales de A:*

$$I_1 \supseteq I_2 \supseteq ...$$

se estaciona, es decir, existe un n tal que $I_n = I_{n+k}$ para toda $k \geq 0$.

Teorema 6. *Si M y M' son A-módulos artinianos, también lo es $M \oplus M'$.*

Prueba. Basta considerar la sucesión exacta

$$0 \to M \to M \oplus M' \to M' \to 0.$$

Teorema 7. *Si A es un anillo artiniano y M es un A-módulo finitamente generado, entonces M es artiniano.*

Prueba. Si M tiene un generador con n elementos, A^n será artiniano, y existe un epimorfismo $A^n \to M$, luego M también es artiniano.

2.2. Módulo de Anillos Noetherianos y Artinianos

Recordamos que si E es un R-módulo,entonces $AnnE$ o (más explícito) Ann_RE se utiliza para denotar el aniquilador de E. Por supuesto Ann_RE es un ideal y por lo tanto podemos formar el anillo de residuos R/Ann_RE.
Ahora se demuestra que, cuando E es finitamente generado, el comportamiento de E se rige en gran medida por la de R/Ann_RE.
Por lo que la multiplicación de R es conmutativa.

Teorema 8. *Sea E finitamente generado de un R-módulo y sea $A = Ann_RE$. Entonces E satisface condición maximal y minimal respectivamente para submódulos si y sólo si el anillo de residuos R/A satisface la condición maximal y minimal para ideales.*

Observación 1. *Vale la pena señalar que el teorema tiene la consecuencia siguiente. Si un R-módulo E cumple la condición maximal para submódulos, entonces el anillo R/Ann_RE satisface la condición maximal para ideales. Y E será finitamente generado y por lo tanto el teorema puede ser aplicado.*

Prueba. Sea $E = Re_1 + Re_2 + Re_3 + ... + Re_s$ y por $A_i = Ann(Re_i)$.
Entonces$A = A_1 \cap A_2 \cap ... \cap A_s$.
Luego el R-epimorfismo $R \to Re_i$ en que $r \to re_i$ tiene núcleo A_i porque R es conmutativo.Por ello se dice que R/A_i y Re_i son isomorfos como R-módulos.
Ahora supongamos que E satisface la condición maximal(minimal) para submódulos. Puesto que R/A_i es isomorfo al submódulo Re_i, y además R/A_i satisface condición maximal (minimal) para submódulos. En consecuencia,

$$R/(A_1 \cap A_2 \cap ... \cap A_s) = R/A$$

satisface condición maximal (minimal) para R-submódulos.Sin embargo, el R-submódulos de R/A son los ideales del anillo R/A.De esta manera, R/A satisface la condición maximal (minimal) para ideales.
Ahora se supone que R/A satisface la condición maximal (minimal) para ideales. Y E es un R-módulo y, como tal, es claramente generados por $e_1, e_2, ..., e_s$.
Por ello se deduce, que E satisface la condición maximal (minimal) de R/A-submódulos. Sin embargo, el R/A-submódulos de E son los mismos que su R-submódulos. Por lo tanto todo está demostrado.

Corolario 9. *Sea E finitamente generado de un R-módulos y sea $A = Ann_RE$.Luego la longitud $L_R(E)$ es finito sí y sólo sí el anillo R/A cumple las condiciones maximales y minimales para ideales.*

Tenemos $L_R(E) < \infty$ si y sólo si E cumple las condiciones condición maximales y minimales de submódulos. En este punto se presentan dos definiciones. Estos nos ayudarán a describir, de forma relativamente concisa, ciertas situaciones.

Definición 21. *Un E R-módulo que satisface la condición maximal para submódulo se denomina “R-módulo Noetheriano ”. Si el anillo R cumple la condición maximal para los ideales, entonces es llamado un “Anillo Noetheriano”.*

Definición 22. *Un anillo R que cumple las condiciones maximales y minimales para los ideales es llamado “Anillo Artiniano”.*

Estos nombres se han dado en el reconocimiento de E. Noetheriano y Artin E. Hacemos algunos comentarios sobre las definiciones. Sea un R-módulo E es noetheriano sí y sólo sí todos sus submódulos son finitamente generado; equivalente (y las mismas proposiciones) E es noetheriano sí y sólo sí satisface la condición de cadena ascendente para submódulos.
En particular, tenemos otras formas de describir un anillo noetheriano.
Podríamos, por ejemplo, definir un anillo noetheriano como aquel en el que todo ideal es finitamente generado. Igualmente bien podríamos decir que un anillo es noetheriano si satisface la condición de cadena ascendente para ideales.
Y R es un anillo Artiniano si y sólo si $L_R(R) < \infty$. Por ejemplo, un campo F es un anillo Artiniano, entonces (0) y F son los únicos ideales, $L_F(F) = 1$.En realidad un anillo de un anillo Artiniano satisface sólo la condición minimal de los ideales. Sin embargo, como demostraremos más adelante, cuando la condición minimal de ideales se cumpla sostendrá,también las condiciones de los maximales. Para ilustrar la terminología, sea R-módulo E finitamente generado.Mostrando que E es un R-módulo noetheriano si y solo si R/Ann_RE es un anillo noetheriano, y $L_R(E)$ es finito sí y sólo sí R/Ann_RE es un anillo Artiniano. Una vez más, por el teorema 1,si R es un anillo noetheriano, entonces también lo es el anillo de polinomios $R[X_1, X_2, ..., X_n]$.

Teorema 9. *Sea $\phi : R \to R'$ un epimorfismo de un anillo R a un anillo R'. Ahora bien, si R es un anillo noetheriano y Anillo Artiniano respectivamente, entonces R' es también un anillo noetheriano y Artiniano respectivamente Este resultado es obvio por la correspondencia biunívoca entre la R'-ideales y la R-ideales que contienen $Ker\phi$.Para mostrar como se puede combinar con nuestros resultados en los anillos polinomiales, se prueba.*

Teorema 10. *Sea el anillo noetheriano R un subanillo de un anillo R'. Si ahora $\alpha_1, \alpha_2, ..., \alpha_n$ son elementos de R' entonces $R[\alpha_1, \alpha_2, ..., \alpha_n]$ es un anillo noetheriano.*

Prueba. Obtenemos un anillo-homomorfismo de anillo de polinomios $R[X_1, X_2, ..., X_n]$ para $R[\alpha_1, \alpha_2, ..., \alpha_n]$ por medio de la asignación en el que (con una notación explica por sí mismo).

$$\sum r_{\mu_1,\mu_2...\mu_n} X_1^{\mu_1} X_2^{\mu_2} ... X_n^{\mu_n} \to \sum r_{\mu_1,\mu_2...\mu_n} \alpha_1^{\mu_1} \alpha_2^{\mu_2} ... \alpha_n^{\mu_n}$$

Desde entonces $R[X_1, X_2, ..., X_n]$ es noetheriano, este resultado que sigue del teorema 3.

Corolario 10. *Sea F un campo y $\alpha_1, \alpha_2, ..., \alpha_n$ elementos que pertenezcan a algún anillo de extensión de F.*
Entonces el anillo $F[\alpha_1, \alpha_2, ..., \alpha_n]$ es noetheriano.

En contraste con el caso noetheriano, anillos de extensión de los anillos Artinianos es poco probable que heredan la propiedad Artiniana.
Sin embargo, a este siguiente resultado a veces es útil.

Teorema 11. *Sea R' un anillo de extensión de un anillo R Artiniano y supongamos que R', considerado como un R-módulo, es finitamente generado. Entonces R' es también un anillo Artiniano.*

Prueba. R' satisface las condiciones de los maximales y minimales para R-submódulos. Ahora vamos a ser Ω un conjunto no vacío de R'-ideales.
Ω Entonces también es un conjunto no vacío de R-submódulos de R'.
Ω En consecuencia contiene un miembro maximal y minimal. Esto demuestra el teorema. El comportamiento de los anillos noetheriano y anillos Artiniano en relación a la formación de fracciones es fácil de establecer. Primero necesitamos.

Lema 6. *Sea E un R-módulo y S un conjunto no vacío multiplicativamente cerrado subconjunto de R. Si ahora E satisface la la condición maximal (minimal) para el R-módulos, entonces E_S satisface la condición maximal(minimal) para R_S-submódulos.*

Teorema 12. *Sea S un subconjunto no vacío multiplicativamente cerrado del anillo R. Si ahora R es un anillo noetheriano y anillo Artiniano respectivamente, entonces R_S es un anillo noetheriano y anillo Artiniano respectivamente.*

A partir del anillo noetheriano de un tipo simple, es posible construir una o más otras de carácter sofisticado. Los ejemplos más evidentes de primaria anillos noetheriano son campos y ciclos que tienen sólo un número finito de elementos. A estos podemos añadir los números enteros. El teorema, con la siguiente, se establece el carácter de este anillo noetheriano particular. Aunque tanto el resultado de su prueba y están muy familiarizados, se incluyen en áreas de la exhaustividad.

Teorema 13. *Sea Z el anillo formado por el positivo, negativo y cero números enteros. Luego, cada ideal de Z puede ser generado por un elemento dado.*

Prueba. Está claro que podemos limitar nuestra atención a los no-cero ideales. Sea A un ideal. Entonces podemos encontrar que $m \in A$ con $m \neq 0$. Dado que tanto m y $-m$ pertenecen a A y uno de ellos es un enteros positivos se deduce que A contiene números enteros positivos. Sea d la parte baja de estos. Vamos a demostrar que $A = (d)$. En efecto $(d) \subseteq A$ o lo que sea necesario para demostrar la inclusión en el sentido contrario. Sea $n \in A$. Entonces (por la división de operaciones números enteros) podemos encontrar enteros q y r para que $n = qd + r$,con $0 \leq r < d$.Ahora $r = n - qd$ pertenece a A porque n y d pertenecen a A. Sin embargo es de la pequeña estrictamente entero positivo contenido en A y $0 \leq r < d$. Sigue el $r = 0$ y por lo tanto $n = qd \in (d)$. Esto muestra que $A \subseteq (d)$ y completa la prueba.

Lema 7. *Sea E un espacio vectorial con respecto a un campo F y supongamos que E satisface la condición minimal de subespacios. Entonces la dimensión de E es finita.*

Prueba. Será suficiente para demostrar que E es finito. Supongamos lo contrario. Entonces es posible encontrar una secuencia de E infinito $e_1(e_1 \neq 0), e_2, e_3, ...$ de elementos de E tales que, para cada n,

$$e_{n+1} \notin Fe_1 + Fe_2 + ... + Fe_n$$

de ello se deduce que si un $a_1e_1 + a_2e_2 + a_3e_3 + ... + a_pe_p = 0$, donde a_i pertenecen a F, entonces $a_1 = a_2 = a_3 = ... = a_p = 0$ (Por lo contrario sea q sea a_q el último distinto de cero coeficiente. Entonces, multiplicando por a_q^{-1}, con e_q vemos que la ecuación es

$$Fe_1 + Fe_2 + ... + Fe_{q-1}.$$

Sin embargo, denotemos por V_n el subespacio de E generado por los elementos $e_n, e_{n+1}, ...$ Entonces $e_n \in V_n$ y $e_n \notin V_{n+1}$ (Por lo contrario, debe obtener un no-relación trivial entre diferentes e_i', y esto, como hemos visto, es imposible.) En consecuencia

$$V_1 \supset V_2 \supset ... \supset V_n \supset ...$$

es una sucesión infinita estrictamente decreciente de subespacios. Esto, sin embargo, viola la hipótesis de que E satisface la condición minimal para los subespacios. Así hemos llegado a una contradicción y la prueba es completa.

Proposición 7. *Sea R un dominio de integridad y supongamos que R satisface la condición minimal de los ideales. Entonces R es un campo.*

Prueba . Supongamos que un $\alpha \in R$, $\alpha \neq 0$. Queremos demostrar que α tiene un inverso en R. Puesto que R satisface la condición minimal, la sucesión decreciente

$$(\alpha) \supseteq (\alpha^2) \supseteq (\alpha^3) \supseteq ...$$

de los ideales debe terminar. por consiguiente existe un entero m tal que $(\alpha^m) = (\alpha^{m+1})$. Por lo tanto $\alpha^m \in (\alpha^{m+1})$ y por lo tanto $\alpha^m = (\beta\alpha^{m+1})$ para $\beta \in R$. Sin embargo, R es un dominio de integridad y $\alpha^m \neq 0$.
Por consiguiente para $\alpha^m(1-\beta\alpha) = 0$ se sigue $\beta\alpha = 1$. Esto establece la proposición.

Teorema 14. *Sea el anillo R satisface la condición minimal para los ideales.Entonces R tiene un número finito de ideales primos y cada uno de estos es un ideal maximal.*

Prueba. Podemos asumir que R no es un anillo nulo para distintos teoremas es vacio. Sea P un ideal primo. Entonces R/P es un dominio de integridad y (en la vista de la correspondencia entre los ideales de R/P y el R-ideales que contienen P) también satisface la condición minimal. De ello se deduce, que R/P es un campo. Por lo tanto, P es un ideal maximal.
Sea Ω el conjunto de todos los R-ideales que se puede obtener como la intersección de un número finito de ideales primos. Entonces. Ω es no vacío y por ello este contiene un miembro minimal. Sea $P_1 \cap P_2 \cap ... \cap P_s$, donde los P_i son ideales primos, son tales miembros minimales. Ahora supongamos que P es un ideal arbitrario principal de R. Entonces

$$P \cap P_1 \cap ... \cap P_s$$

pertenece a Ω y está contenido en $P_1 \cap P_2 \cap ... \cap P_s$.
Por consiguiente, por la propiedad minimal de este último,

$$P \cap P_1 \cap P_2 \cap ... \cap P_s = P_1 \cap P_2 \cap ... \cap P_s$$

y por lo tanto

$$P \supseteq P_1 \cap P_2 \cap ... \cap P_s$$

de ello se deduce, que existe
$i(1 \leq i \leq s)$ tal que $P \supseteq P_i$. Sin embargo P_i es un ideal maximal de R por lo que $P = P_i$.
Esto demuestra que $P_1, P_2, ..., P_s$, son solo ideales primos de R y se completa la prueba.
Recordamos que un elemento de un anillo se dice que es nilpotente si algunos positivo de la misma es cero.

Lema 8. *Sea R un anillo que satisface la condición minimal de los ideales y sea $P_1, P_2, ..., P_s$ son ideales primos. Entonces, cada elemento de*

$$P_1 \cap P_2 \cap ... \cap P_s$$

es nilpotente.

Prueba. Sea α que pertenecen $P_1 \cap P_2 \cap ... \cap P_s$. Puesto que R satisface la condición minimal, la sucesión decreciente

$$(\alpha) \supseteq (\alpha^2) \supseteq (\alpha^3) \supseteq ...$$

debe terminar. Por tanto, es posible encontrar un entero m tal que $(\alpha^m) = (\alpha^{m+1})$. Por lo tanto $\alpha^m \in (\alpha^{m+1})$ y por lo tanto $\alpha^m = (r\alpha^{m+1})$ para $r \in R$.Considere $1 - r\alpha$.
Está claro que esto no puede pertenecer a cualquiera de $P_1, P_2, ..., P_s$; por lo tanto, el ideal $R(1 - r\alpha)$ no contienen ningún ideal maximal.
Por consiguiente $R(1-r\alpha) = R$ y por lo tanto $\rho(1-r\alpha) = 1$ para un decuado elemento ρ de R.Finalmente, entonces $\alpha^m(1 - r\alpha) = 0$, la multiplicación por muestra que $\alpha^m = 0$. Esto completa la prueba.

Corolario 11. *Tome en cuenta las suposiciones que estan en el lema y ponga*

$$I = P_1 P_2 ... P_s$$

Entonces existe un entero m tal que $I^m = 0$.

Prueba. Puesto que R satisface la condición minimal de los ideales, la sucesión

$$I \supseteq I^2 \supseteq I^3 \supseteq ...$$

debe terminar. Por lo tanto existe un entero m tal que $I^n = I^m$. para todo $n \geq m$. Vamos a suponer que $I^m \neq (0)$ y obtener una contradicción. Sea Ω integrado por todos los ideales de A tal que $I^m A \neq (0)$. Desde

$$I^m I^m = I^{2m} = I^m \neq (0),$$

tenemos que $I^m \in \Omega$. Así Ω no está vacío. Entre los ideales en el conjunto de Ω. seleccionamos un B que es mínimo. Desde $I^m B \neq (0)$, existe $b \in B$ tal que $I^m b \neq (0)$. Entonces $I^m(b) \neq (0)$ y $(b) \subseteq B$, por lo que, la propiedad minimal de B, $B = (b)$. Nuevamente

$$I^m(IB) = I^{m+1}B = I^m B \neq (0),$$

en consecuencia $IB \in \Omega$, Desde $IB \subseteq B$, se puede concluir que $B = IB$. Ahora se tienen

$$(b) = B = IB = I(b),$$

de ello se deduce que existe un $c \in I$ tal que $b = bc$. Por consiguiente

$$b = bc = bc^2 = bc^3 = ...,$$

donde $b = 0$, ya que, por el lema, c es nilpotente. Esto, sin embargo, contradice el hecho de que $I^m b \neq (0)$. La prueba se ha completado.

2.3. El concepto de grado

Sea R una anillo (conmutativo y poseedor de un elemento identidad), E un R-módulo, y $\alpha_1, \alpha_2, ..., \alpha_s$ una sucesión de elementos de R.

Definición 23. *La sucesión $\alpha_1, \alpha_2, ..., \alpha_s$ será llamada una “R-sucesión sobre E” que satisface que:*

(a) $(\alpha_1, \alpha_2, ..., \alpha_s)\, E \neq E$ *y*

(b) $(\alpha_1, \alpha_2, ..., \alpha_s)\, E :_E \alpha_i = (\alpha_1, \alpha_2, ..., \alpha_s)\, E$ *para* $1 \leq i \leq s$.

Naturalmente cuando $i = 1$ es entendido que (b) afirma que $0 :_E \alpha_1 = 0$. Si $\alpha_1, \alpha_2, ..., \alpha_s$ es una R-sucesión sobre R, entonces decimos que es una R-sucesión. Es conveniente a introducir alguna terminología en el futuro en orden a facilitar la discusión de R-sucesiónes sobre módulos.

Definición 24. *Un elemento γ de el anillo R es llamado un “divisor de cero” sobre el módulo E si existe $e \in E$, $e \neq 0$, tal que $\gamma e = 0$.*

Es importante notar que, cuando E es un R-módulo Noeteriano, γ es un divisor de cero sobre E cuando y sólo cuando está contenido en uno de los ideales primos pertenecientes al submódulo de E. Otra vez regresemos al caso general, un elemento $\alpha \in R$ no es un divisor de cero sobre E sí y sólo sí $0 :_E \alpha = 0$. Ahora supongamos que $(\alpha_1, \alpha_2, ..., \alpha_s)\, E \neq E$. Entonces $\alpha_1, \alpha_2, ..., \alpha_s$ es una R-sucesión sobre E precisamente cuando, para cada $i\,(1 \leq i \leq s)\,, \alpha_i$ no es un divisor de cero sobre $E/\,(\alpha_1, ..., \alpha_{i-1})\, E$. Además, para $p+1 \leq i \leq s$, tenemos

$$(\alpha_{p+1}, ..., \alpha_i)\,(E/\,(\alpha_1, ..., \alpha_p)\, E) = (\alpha_1, ..., \alpha_p, ..., \alpha_i)\, E/\,(\alpha_1, ..., \alpha_p)\, E$$

se sigue que *si $\alpha_1, \alpha_2, ..., \alpha_s$ es una R-sucesión sobre E, entonces $\alpha_{p+1}, \alpha_{p+2}, ..., \alpha_s$ es una R-sucesión sobre $E/(\alpha_1, \alpha_2, ..., \alpha_p)E$*

Lema 9. *Sea $\alpha_1, \alpha_2, ..., \alpha_{s-1}, \alpha_s$ una R-sucesión sobre E y supongamos que $s \geq 2$. Entonces*

$$(\alpha_1, \alpha_2, ..., \alpha_{s-2}, \alpha_s)\, E :_E \alpha_{s-1} = (\alpha_1, ..., \alpha_{s-2}, \alpha_s)\, E.$$

Se sigue que $\alpha_1, \alpha_2, ..., \alpha_{s-2}, \alpha_s, \alpha_{s-1}$ es una R-sucesión sobre E sí y sólo sí $(\alpha_1, \alpha_2, ..., \alpha_{s-2})\, E :_E \alpha_s = (\alpha_1, ..., \alpha_{s-2})\, E$

Prueba. Sea $e \in (\alpha_1, \alpha_2, ..., \alpha_{s-2}, \alpha_s)\, E :_e \alpha_{s-1}$. Entonces

$$\alpha_{s-1} e = \alpha_1 e_1 + \alpha_2 e_2 + ... + \alpha_{s-2} e_{s-2} + \alpha_s e_s$$

elementos adecuados para $e_1, ..., e_{s-2}, e_s$ en E. En consecuencia

$$e_s \in ((\alpha_1, \alpha_2, ..., \alpha_{s-2}, \alpha_{s-1})\, E_E : \alpha_s) = (\alpha_1, \alpha_2, ..., \alpha_{s-2}, \alpha_{s-1})\, E$$

y por tanto podemos expresar e_s la forma

$$e_s = \alpha_1 e'_1 + \alpha_2 e'_2 + ... + \alpha_{s-2} e'_{s-2} + \alpha_{s-1} e'_{s-1}$$

se sigue que

$$\alpha_{s-1} e - \alpha_s \alpha_{s-1} e'_{s-1} \in (\alpha_1, ..., \alpha_{s-2})\, E.$$

Por tanto

$$e - \alpha_s e'_{s-1} \in (\alpha_1, ..., \alpha_{s-2})\, E :_E \alpha_{s-1} = (\alpha_1, ..., \alpha_{s-2})\, E$$

y por tanto

$$e \in (\alpha_1, ..., \alpha_{s-2})\, E.$$

Esto prueba que

$$(\alpha_1, \alpha_2, ..., \alpha_{s-2}, \alpha_s)\, E :_E \alpha_{s-1} \subseteq (\alpha_1, ..., \alpha_{s-2}, \alpha_s)\, E$$

y la otra inclusión es obvia. ||

Lema 10. *Sea E un R-módulo y A un ideal de R. Además, sea α y α' elementos de A que no son divisores de cero sobre E. Entonces*

$$(\alpha E :_E A)\,/\alpha E \qquad y \qquad (\alpha' E :_E A)\,/\alpha' E$$

son isomorfismos con R-módulos.

Prueba. Si S permite designar el conjunto de todos los elementos de R que no son divisores de cero sobre E. Entonces S, como es fácil de verificar, es multiplicativamente cerrado y, por hipótesis, tanto α y α' pertenecen a él. Ahora formemos el módulo E_s de fracciones y, en lo que sigue, lo consideran como un R-módulo. El mapeo $\phi : (\alpha E :_E A) \rightarrow E_s$ definido por $\phi(x) = [x/\alpha]$, donde x es un elemento arbitrario de $\alpha E :_E A$, es un homomorfismo de R-módulos. Si $\phi(x) = 0$, entonces $sx = 0$ para algunos $s \in S$ y por tanto, $x = 0$. De esta manera ϕ es un monomorfismo. Sea $\chi : E \rightarrow E_S$ la función canónica. Sostenemos que

$$Im\,(\phi) = \chi\,(E) :_{E_S} A. \tag{2.3.1}$$

Sea x pertenece a $\alpha E :_E A$ y $a \in A$. Entonces $a\phi(x) = [ax/\alpha]$. Pero $ax = \alpha e'$ para algún $e' \in E$ y por tanto, $[ax/\alpha] = [\alpha e'/\alpha]$, que pertenecen a $\chi(E)$. Por

lo tanto $a\phi(x) \in \chi(E)$, donde $\phi(x)$ pertenece a $\chi(E) :_{E_S} A$.
Ahora supongamos que ξ es un elemento de $\chi(E) :_{E_S} A$.
Entonces $\alpha\xi \in \chi(E)$, expresa $\alpha\xi = \chi(e)$. Sea $a \in A$.
Entonces $\chi(ae) = a\chi(e) = a\alpha\xi \in \alpha\chi(E)$ y así $\chi(ae) = \chi(\alpha e^*)$ para algún $e^* \in E$.
Pero, el núcleo de χ es la S-componente del submódulo cero de E. Por lo tanto $s(ae - \alpha e^*) = 0$ para algún $s \in S$ y, por tanto, $ae = \alpha e^* \in \alpha E$ porque s no es divisor de cero sobre E. Se deduce que e pertence a $\alpha E :_E A$.
Además

$$\alpha\xi = \chi(e) = \left[\tfrac{\alpha e}{\alpha}\right] = \alpha\left[\tfrac{e}{\alpha}\right] = \alpha\phi(e)$$

pero E_S es un R_S-módulo, así como un R-módulo. Podemos, por tanto multiplicar $[\alpha/1]\,\xi = [\alpha/1]\,\phi(e)$ por $[1/\alpha]$ para obtener $\xi = \phi(e) \in Im(\phi)$.
Por lo tanto (2.3.1) es establecido.
Este resultado, combinado con el hecho de que ϕ es un monomorfismo, muestra que ϕ induce un isomorfismo de el R-módulo $\alpha E :_E A$ sobre el R-módulo de $\chi(E) :_{E_S} A$.
Además αE es llevado a $\chi(E)$. Por consiguiente, se induce un isomorfismo

$$(\alpha E :_E A)/\alpha E \approx (\chi(E) :_{E_S} A)/\chi(E)$$

ya que tenemos un isomorfismo similares en los que α' sustituye α. el lema resulta. ||

Corolario 12. *Sea E un R-módulo, K un submódulo de E y A un ideal de R. Si ahora $\alpha, \alpha' \in A$ y $K :_E \alpha = K = K :_E \alpha'$, entonces*

$$\{(\alpha E + K) :_E A\}/(\alpha E + K) \;\; y \;\; \{(\alpha' E + K) :_E A\}/(\alpha' E + K)$$

son isomorfismos de R-módulos.

Prueba. La hipótesis demuestra que ni α ni α' son divisores de cero sobre E/K. También

$$\alpha(E/K) = (\alpha E + K)/K \qquad \text{y} \qquad \alpha(E/K) :_{E/K} A = \{(\alpha E + K) :_E A\}/K$$

relaciones similares con la participación de α'. Por lo tanto, el corolario resulta del lema. ||

Teorema 15. *Sea E un R-módulo Noetheriano y A un ideal de R.
Supongamos que $\alpha_1, \alpha_2, ..., \alpha_k$ y $\beta_1, \beta_2 ..., \beta_K$ son dos R-sucesiónes sobre E que consisten de cada K elementos pertenecientes a el ideal A.
En estas circunstancias existe un isomorfismo*

$$\{(\alpha_1, \alpha_2, ..., \alpha_k)E :_E A\}/(\alpha_1, \alpha_2, ..., \alpha_k)E \approx \{(\beta_1, \beta_2, ..., \beta_k)E :_E A\}/(\beta_1, \beta_2, ..., \beta_k)E$$

entre las dos partes se consideran como R-módulos.

Prueba. Los módulos

$$(\alpha_1, \alpha_2, ..., \alpha_i)E \quad (0 \leq i \leq k-1) \text{ y } (\beta_1, \beta_2, ..., \beta_j)E \quad (0 \leq j \leq k-1)$$

son todos ellos de la propiedad submódulos de los R-módulos Noetherianos E y por lo tanto, a cada uno de ellos pertenece a un número finito de ideales primos. Denotados por $P_1, P_2, ..., P_s$ el primer conjunto de ideales primos que surgen de esta manera.
Consideremos P_1 pertenece a uno de los conjuntos de los submódulos $2k$. Supongamos que pertenecen a $(\alpha_1, \alpha_2, ..., \alpha_i)\, E$, donde $0 \leq i \leq k-1$. Ya que

$$(\alpha_1, \alpha_2, ..., \alpha_i)\, E :_E \alpha_{i+1} = (\alpha_1, \alpha_2, ..., \alpha_i)\, E$$

vemos que un $\alpha_{i+1} \notin P_1$, por tanto $A \not\subseteq P_1$, se deduce, por razones similares, que A no figura por algunos $P_1, P_2, ..., P_s$. Además existen $\gamma_K \in A$ tal que $\gamma_K \notin P_1, \gamma_K \notin P_2, ..., \gamma_K \notin P_S$. En consecuencia

$$(\alpha_1, \alpha_2, ..., \alpha_i)\, E :_E \gamma_k = (\alpha_1, \alpha_2, ..., \alpha_i)\, E \;\; (0 \leq i \leq k-1) \qquad (2.3.2)$$

$$\text{y} \quad (\beta_1, \beta_2, ..., \beta_i)\, E :_E \gamma_k = (\beta_1, \beta_2, ..., \beta_i)\, E \;\; (0 \leq i \leq k-1) \qquad (2.3.3)$$

en particular

$$(\alpha_1, \alpha_2, ..., \alpha_{k-1})\, E :_E \alpha_k = (\alpha_1, \alpha_2, ..., \alpha_{k-1})\, E = (\alpha_1, \alpha_2, ..., \alpha_{k-1})\, E :_E \gamma_k$$

y por tanto, tenemos un isomorfismo
$\{(\alpha_1, \alpha_2, ..., \alpha_k)\, E :_E A\} \,/\, (\alpha_1, , ..., \alpha_{k-1}\alpha_k)\, E$

$$\approx \{(\alpha_1, \alpha_2, ..., \alpha_{k-1}, \gamma_k)\, E :_E A\} \,/\, (\alpha_1, \alpha_2, ..., \alpha_{k-1}, \gamma_k)\, E \qquad (2.3.4)$$

es claro que $\alpha_1, \alpha_2, ..., \alpha_{k-1}, \gamma_k$ es una R-sucesión sobre E. Por (2.3.2) y lema 9, podemos concluir que $\alpha_1, \alpha_2, ..., \alpha_{k-2}, \gamma_k, \alpha_{k-1}$ es una R-sucesión sobre E. De hecho otra aplicación sobre estos resultados prueba que
$\alpha_1, \alpha_2, ..., \alpha_{k-3}, \gamma_k, \alpha_{k-2}, \alpha_{k-1}$ es una R-sucesión sobre E y, procediendo en este camino establecemos que $\gamma_k, \alpha_1, \alpha_2, ..., \alpha_{k-1}$ es una R-sucesión sobre E. Notese que (2.3.4) puede escribirse como
$\{(\alpha_1, \alpha_2, ..., \alpha_k)\, E :_E A\} \,/\, (\alpha_1, \alpha_2, ..., \alpha_k)\, E$

$$\approx \{(\gamma_k, \alpha_1, \alpha_2, ..., \alpha_{k-1},)\, E :_E A\} \,/\, (\gamma_k, \alpha_1, \alpha_2, ..., \alpha_{k-1})\, E \qquad (2.3.5)$$

de la exactitud deducimos que $\gamma_k, \beta_1, \beta_2, ..., \beta_{k-1}$ es una R-sucesión sobre E y, como una compañía para (2.3.5) tenemos un isomorfismo
$\{(\beta_1, \beta_2, ..., \beta_k)\, E :_E A\} \,/\, (\beta_1, \beta_2, ..., \beta_k)\, E$

$$\approx \{(\gamma_k, \beta_1, \beta_2, ..., \beta_{k-1})\, E :_E A\} \,/\, (\gamma_k, \beta_1, \beta_2, ..., \beta_{k-1})\, E \qquad (2.3.6)$$

este argumento condujo a (2.3.5) y (2.3.6) podemos ahora reiteradas veces con

$$\gamma_k, \alpha_1, \alpha_2, ..., \alpha_{k-1} \text{ y } \gamma_k, \beta_1, \beta_2, ..., \beta_{k-1}$$

la sustitución

$$\alpha_1, \alpha_2, ..., \alpha_k \text{ y } \beta_1, \beta_2, ..., \beta_k$$

se encuentra que existen elementos $\gamma_{k-1} \in A$ tal que (i) $\gamma_{k-1}, \gamma_k, \alpha_1, \alpha_2, ..., \alpha_{k-2}$ y $\gamma_{k-1}, \gamma_k, \beta_1, \beta_2, ..., \beta_{k-2}$ son R-sucesiónes sobre E y (ii) hay unos isomorfismos
$\{(\gamma_k, \alpha_1, \alpha_2, ..., \alpha_{k-1})\, E :_E A\} \,/\, (\gamma_k, \alpha_1, \alpha_2, ..., \alpha_{k-1},)\, E$

$$\approx \{(\gamma_{k-1}, \gamma_k, \alpha_1, \alpha_2, ..., \alpha_{k-2})\, E :_E A\} \,/\, (\gamma_{k-1}, \gamma_k, \alpha_1, \alpha_2, ..., \alpha_{k-2})\, E \quad (2.3.7)$$

con un isomorfismo similar la partición de $\beta_1, \beta_2, ..., \beta_{k-1}$. Observemos que, por combinar el nuevo isomorfismo con (2.3.5) y (2.3.6) obtenemos
$\{(\alpha_1, \alpha_2, ..., \alpha_k)\, E :_E A\} \,/\, (\alpha_1, \alpha_2, ..., \alpha_k)\, E$

$$\approx \{(\gamma_{k-1}, \gamma_k, \alpha_1, \alpha_2, ..., \alpha_{k-2})\, E :_E A\} \,/\, (\gamma_{k-1}, \gamma_k, \alpha_1, \alpha_2, ..., \alpha_{k-2},)\, E$$

y $\{(\beta_1, \beta_2, ..., \beta_k)\, E :_E A\} \,/\, (\beta_1, \beta_2, ..., \beta_k)\, E$

$$\approx \{(\gamma_{k-1}, \gamma_k, \beta_1, \beta_2, ..., \beta_{k-2})\, E :_E A\} \,/\, (\gamma_{k-1}, \gamma_k, \beta_1, \beta_2, ..., \beta_{k-2})\, E$$

es evidente como continua el argumento. Eventualmente obtenemos una R-sucesión $\gamma_1, \gamma_2, ..., \gamma_k$ sobre E tal que

$$\{(\gamma_1, \gamma_2, ..., \gamma_k)\, E :_E A\} \,/\, (\gamma_1, \gamma_2, ..., \gamma_k)\, E$$

es isomorfo a ambos

$$\{(\alpha_1, \alpha_2, ..., \alpha_k)\, E :_E A\} \,/\, (\alpha_1, \alpha_2, ..., \alpha_k)\, E \text{ y } \{(\beta_1, \beta_2, ..., \beta_k)\, E :_E A\} \,/\, (\beta_1, \beta_2, ..., \beta_K)\, E$$

esto completa la prueba. ||

Definición 25. *Si $\alpha_1, \alpha_2, ..., \alpha_n$ es una R-sucesión sobre un R-módulo E y si los α_i pertencen a un ideal A, entonces $\alpha_1, \alpha_2, ..., \alpha_n$ serán llamados “R-sucesiónes sobre E en A”.*

Como una aplicación del último teorema.

Teorema 16. *Sea E un R-módulo Noetheriano y A un ideal de R tal que $AE \neq E$. Además sean $\alpha_1, \alpha_2, ..., \alpha_m$ y $\beta_1, \beta_2, ..., \beta_n$ R-sucesiónes sobre E en A. Si ahora $m < n$, entonces es posible encontrar $\alpha_{m+1}, \alpha_{m+2}, ..., \alpha_n$ tal que $\alpha_1, \alpha_2, ..., \alpha_m, \alpha_{m+1}, \alpha_{m+2}, ..., \alpha_n$ es una R-sucesión sobre E en A.*

Prueba. Ya que $\alpha_1, \alpha_2, ..., \alpha_m$ y $\beta_1, \beta_2, ..., \beta_n$ son ambos R-sucesiónes sobre E donde ellos tienen el mismo número m de términos, en el último teorema se probó que es un isomorfismo
$\{(\alpha_1, \alpha_2, ..., \alpha_m) E :_E A\} / (\alpha_1, \alpha_2, ..., \alpha_m) E$

$$\approx \{(\beta_1, \beta_2, ..., \beta_m) E :_E A\} / (\beta_1, \beta_2, ..., \beta_m) E$$

de R-módulos. Ahora $m < n$ y $(\beta_1, \beta_2, ..., \beta_m) E :_E \beta_{m+1} = (\beta_1, \beta_2, ..., \beta_m) E$; en consecuencia $(\beta_1, \beta_2, ..., \beta_m) E :_E A = (\beta_1, \beta_2, ..., \beta_m) E$. Del isomorfismo se deduce que, $\{(\alpha_1, \alpha_2, ..., \alpha_m) E :_E A\} / (\alpha_1, \alpha_2, ..., \alpha_m) E$ es un módulo nulo y a la vez implica que $(\alpha_1, \alpha_2, ..., \alpha_m) E :_E A = (\alpha_1, \alpha_2, ..., \alpha_m) E$ en consecuencia A no está contenido por los ideales primos que pertenecen a los submódulos $(\alpha_1, \alpha_2, ..., \alpha_m) E$ de E.
Por lo tanto, existen $\alpha_{m+1} \in A$ que no está en ningno de estos ideales primos y por tanto satisface $(\alpha_1, \alpha_2, ..., \alpha_m) E :_E \alpha_{m+1} = (\alpha_1, \alpha_2, ..., \alpha_m) E$.
Pero $AE \neq E$; en consecuencia $(\alpha_1, \alpha_2, ..., \alpha_m, \alpha_{m+1}) E \neq E$.
Así $\alpha_1, \alpha_2, ..., \alpha_m, \alpha_{m+1}$ es una R-sucesión sobre E en A.
Si $m + 1 < n$, entonces podemos repetir el argumento. ||

Teorema 17. *Sea E un R-módulo Noeteriano y A un ideal de R tal que $AE \neq E$. Entonces hay un mayor número entero $k\,(k \geq 0)$ tal que existen R-sucesión sobre E en A que tiene k términos. Además, si $\alpha_1, \alpha_2, ..., \alpha_m$ es una R-sucesión arbitraria sobre E en A, entonces es posible encontrar elementos $\alpha_{m+1}, \alpha_{m+2}, ..., \alpha_k$ de modo que $\alpha_1, \alpha_2, ..., \alpha_m, \alpha_{m+1}, \alpha_{m+2}, ..., \alpha_k$ es una R-sucesión sobre E en A teniendo el máximo número de k términos.*

Prueba.Por el Teorema 16 sólo es necesario probar la primera afirmación. Para ello asumiremos que para todo $n > 0$ existen al menos una R-sucesión sobre E en A teniendo n términos. De ello se deriva una contradicción.
Sea α_1 una R-sucesión sobre E en A. Ya que existe una R-sucesión sobre E en A con dos términos, y podemos encontrar α_2 tal que α_1, α_2
son R-sucesiónes sobre E en A. Luego, porque existe una R-sucesión sobre E en A con tres términos, además podemos encontrar α_3 tal que $\alpha_1, \alpha_2, \alpha_3$ es una R-sucesión sobre E en A. Y así sucesivamente. En este camino obtenemos una sucesión infinita $\alpha_1, \alpha_2, \alpha_3, ...$ tal que, para cada n $\alpha_1, \alpha_2, ..., \alpha_n$ es una R-sucesión sobre E en A.
Ya que E es un R-módulo Noeteriano, la sucesión

$$(\alpha_1) E \subseteq (\alpha_1, \alpha_2) E \subseteq (\alpha_1, \alpha_2, \alpha_3) E \subseteq ...$$

de submódulos de E debe terminar. Podemos por tanto encontrar un entero m tal que $(\alpha_1, \alpha_2, ..., \alpha_m) E = (\alpha_1, \alpha_2, ..., \alpha_m, \alpha_{m+1}) E$. Entonces

$$(\alpha_1, \alpha_2, ..., \alpha_m) E = (\alpha_1, \alpha_2, ..., \alpha_m) E :_E \alpha_{m+1} = (\alpha_1, \alpha_2, ..., \alpha_m, \alpha_{m+1}) E :_E \alpha_{m+1} = E$$

Sin embargo, todos los $\alpha_i \in A$ y $AE \neq E$. Estos produce una contradicción y completa la prueba.||

Definición 26. *Sea E un R-módulo Noeteriano y A un ideal de R tal que $AE \neq E$. El número de términos de una R-sucesión maximal sobre E en A, será llamada el “grado de A sobre E” y denotado por $gr\,(A; E)$.*

Usaremos la expresión *maximal* R-sucesión sobre E en A, en el sentido de una R-sucesión sobre E en A que tengan el mayor número posible de términos. Por Teorema 17 el $gr\,(A; E)$ es definido y finito.

Definición 27. *Sea A un ideal propio de un Anillo R. Entonces por el “grado de A” significa el grado de A sobre R cuando R es considerado un módulo con respecto a sí mismo. El grado de A es denotado por $gr\,(A)$.*
Así $gr\,(A) = gr\,(A; R)$.

Asumiendo que E es un R-módulo Noetheriano y $AE \neq E$, observemos que $gr\,(A; E) = 0$ en el sentido que cada elemento de A es un divisor de cero sobre E y por lo tanto está contenido en algúnos ideales primos pertenecientes al submódulo cero de E. En consecuencia, A debe ser totalmente contenido por algunos de esos ideales primos. Por tanto

$$gr\,(A; E) = 0 \text{ sí y sólo sí } 0 :_E A \neq 0.$$

Otro punto a notar es que si $\alpha_1, \alpha_2, ..., \alpha_s$ es un R-sucesión sobre E en A, entonces $(\alpha_1, \alpha_2, ..., \alpha_s)\,E :_E A = (\alpha_1, \alpha_2, ..., \alpha_s)\,E$ Si $s < gr\,(A; E)$ mientras que $(\alpha_1, \alpha_2, ..., \alpha_s)\,E :_E A \neq (\alpha_1, \alpha_2, ..., \alpha_s)\,E$ si $s = gr\,(A; E)$. Esto es claro por que en el caso formal la sucesión puede extenderse y este último no puede.

Proposición 8. *Sea E un R-módulo Noeteriano y A un ideal de R satisfaciendo $AE \neq E$. Si ahora B es un ideal de R y $B \subseteq Rad\ A$, entonces $BE \neq E$ y $gr\,(B; E) \leq gr\,(A; E)$. Por tanto si $Rad\ A = Rad\ B$, entonces $gr\,(B, E) = gr\,(A; E)$.*

Prueba. Primero asumamos que $BE = E$ y conduce a una contradicción. Donde E es un R-módulo Noeteriano, es finitamente generado. Sea

$$E = Re_1 + Re_2 + Re_3 + ... + Re_p.$$

Entonces para cada $i\,(1 \leq i \leq p)$ tenemos una relación de la forma

$$e_i = b_{i1}e_1 + b_{i2}e_2 + ... + b_{ip}e_p$$

donde $b_{ij} \in B$. Sea B_0 el ideal generado por los b_{ij} así que $B_0 \subseteq B$ y $E = B_0E$. Puesto que $B_0 \subseteq Rad\ A$ y B_0 es finitamente generado, de ello resulta que m es un entero tal que $B_0^m \subseteq A$. Sin embargo de $E = B_0E$ sigue $E = B_0^mE$. Consecuentemente $E = AE$ que es la contradicción requerida.
Se debe probar que $BE \neq E$. Así $gr(B; E)$ es definido.
Sea $b_1, b_2, ..., b_s$ una R-sucesión maximal sobre E en B. Entonces $s = gr(B; E)$.
Escojamos n así que $b_1^n \in A$ y sea $\beta_1 = b_1^n$.
Puesto que $0 :_E b_1 = 0$, de ello resulta que $0 :_E \beta_1 = 0$.
De aquí β_1 es una R-sucesión sobre E en $A \cap B$ y, por el Teorema 17 puede ser prolongada a una R-sucesión maximal $\beta_1,\ b_2^{'}, ..., b_s^{'}$ sobre E en B.
Escojamos k así que $b_2^{'k} \in A$ y sea $\beta_2 = b_2^{'k}$. Entonces, porque

$$(\beta_1)E_E b_2^{'} = (\beta_1)E,$$

$$(\beta_1)E_E \beta_2 = (\beta_1)E.$$

Así $\beta_1,\ \beta_2$ es una R-sucesión sobre E en $A \cap B$ y podemos prolongarla a una R-sucesión maximal

$$\beta_1,\ \beta_2,\ b_3^{''}, ..., b_s^{''}$$

sobre E en B. Procediendo en este camino finalizamos obteniendo una R-sucesión $\beta_1, \beta_2, ..., \beta_s$ sobre E en $A \cap B$. De ello resulta que

$$gr(A; E) \geq s = gr(B; E).$$

La afirmación final de la proposición no necesita comentario. ||

Proposición 9. *Sea E un R-módulo Noetheriano y A, B ideales de R tal que $AE \neq E$ y $BE \neq E$. Entonces*

$$gr(AB; E) = gr(A \cap B; E) = min\,\{gr(A; E), gr(B; E)\}$$

Prueba. Es claro que $gr(AB; E) \leq gr(A \cap B; E) \leq min\,\{gr(A; E), gr(B; E)\}$
Sea $s = gr(A; E)$ y $t = gr(B; E)$. Sea $\alpha_1, \alpha_2, ..., \alpha_s$ una R-sucesión sobre E en A y $\beta_1, \beta_2, ..., \beta_t$ una R-sucesión sobre E en B.
Sin pérdida de generalidad podemos asumir que $s \leq t$. Sea $\gamma_1 = \alpha_1\beta_1$.
Entonces $\gamma_1 \in AB$ y, puesto que $0 :_E \alpha_1 = 0$ y $0 :_E \beta_1 = 0$, tenemos $0 :_E \gamma_1 = 0$. De esta manera γ_1 es una R-sucesión sobre E en AB.
Esto puede ser extendido a una R-sucesión $\gamma_1, \alpha_2^{'}, ..., \alpha_s^{'}$ sobre E en A.
Similarmente existe una R-sucesión $\gamma_1, \beta_2^{'}, ..., \beta_t^{'}$ sobre E en B. Ahora fijamos $\gamma_2 = \alpha_2^{'}\beta_2^{'}$.
Entonces $\gamma_2 \in AB$ y tenemos

$$(\gamma_1)E :_E \gamma_2 = (\gamma_1)E$$

porque

$$(\gamma_1)E :_E \gamma_2^{'} = (\gamma_1)E$$

y

$$(\gamma_1)E :_E \beta'_2 = (\gamma_1)E.$$

De esta manera γ_1, γ_2 es una R-sucesión sobre E en AB.
Además existen sucesiones

$$\gamma_1\gamma_2, \alpha_3^{''}, ..., \alpha_s^{''} \text{ y } \gamma_1\gamma_2, \beta_3^{''}, ..., \beta_t^{''}$$

que son R-sucesiónes sobre E en A y B respectivamente.
Después se pasa a s, esto produce una R-sucesión $\gamma_1, \gamma_2, ..., \gamma_s$ sobre E en AB.
Por consiguiente

$$gr(AB; E) \geq s = min\,\{gr(A; B), gr(B; E)\}$$

y la prueba se completa. ||

Son ciertas situaciones en que la propiedad será una R-sucesión sobre un módulo no es afectado si el orden de los elementos en la sucesión es cambiado. En esta conexión recordaremos que el radical de Jacobson de un anillo es definido como la intersección de todos sus ideales maximales.
Demostraremos presentando que, para módulos Noetherianos, el oden de los elementos en una R-sucesión no es importante siempre que todos los elementos pertenecen a el radical de Jacobson. En preparación para esto establecemos lo siguiente.

Lema 11. *Sea E un R-módulo Noetheriano y α, β una R-sucesión sobre E. Si ahora α pertenece a el radical de Jacobson de R, entonces β, es también una R-sucesión sobre E.*

Prueba. Es suficiente probar que $0 :_E \beta = 0$. Asumamos que $\beta e = 0$ donde $e \in E$. Afirmamos que $e \in (\alpha^m)E$ para $m \geq 0$. En efecto esto es trivial para $m = 0$. También, si $e \in (\alpha^s)E$, donde $s \geq 0$, entonces $e = \alpha^s e'$ para algunos $e' \in E$ y $\beta\alpha^s e' = 0$. Pero α no es un divisor de cero sobre E.
Por consiguiente $\beta e' = 0$ donde a *fortiori* $\beta e' \in \alpha E$. Sin embargo
$\alpha :_E \beta = \alpha E$ podemos por ello concluir que $e' \in \alpha E$, digamos $e' = \alpha e''$.
De esta manera

$$e = \alpha^s e' = \alpha^{s+1} e''$$

donde $e \in (\alpha^{s+1})E$. La afirmación que $e \in (\alpha^m)E$ para todo m se sigue por inducción. Tenemos ahora probado que

$$e \in \bigcap_{m=1}^{\infty} (\alpha^m)E = \bigcap_{m=1}^{\infty} (\alpha)^m E$$

De aquí que $e = 0$. Por consiguiente
$0 :_E \beta = 0$ y la prueba es completa. ||

Teorema 18. *Sea E un R-módulo Noetheriano y $\alpha_1, \alpha_2, ..., \alpha_s$ una R-sucesión sobre E de cada elemento que estan contenidos en el radical de Jacobson de R. Si ahora $\{i_1, i_2, ..., i_s\}$ es un nuevo arreglo arbitrario de $\{1, 2, ..., s\}$, entonces $\alpha_{i_1}, \alpha_{i_2}, ..., \alpha_{i_s}$ es también una R-sucesión sobre E.*

Prueba. Es suficiente probar que algunos dos términos adyacentes en la sucesión $\alpha_1, \alpha_2, ..., \alpha_s$ pueden ser cambiados sin perturbar la propiedad de ser una R-sucesión sobre E.
Claramente todo nos permite probar que $\alpha_1, ..., \alpha_{i-1}, \alpha_{i+1}, \alpha_i$ es una R-sucesión sobre E.
Y se sigue probando que

$$(\alpha_1, ..., \alpha_{i-1})E :_E \alpha_{i+1} = (\alpha_1, ..., \alpha_{i-1})E$$

por consiguiente para establecer el teorema es suficiente probar que α_{i+1} no es un divisor de cero sobre $E' = E/(\alpha_1, ..., \alpha_{i-1})E$. Ahora E' es un R-módulo Noetheriano y α_i, α_{i+1} es una R-sucesión sobre E'. Puesto que α_i pertenece a el radical de Jacobson de R. El Lema 11 prueba que α_{i+1}, α_i es una R-sucesión sobre E'. En particular, α_{i+1} no es un divisor de cero sobre E'. Esto completa la prueba. ||

Teorema 19. *Sea $E \neq 0$ un R-módulo Noetheriano. Sea B un ideal y γ un elemento de R y supongamos que ambos son contenidos en el radical de Jacobson de R. Entonces $gr((B, \gamma); E) \leq gr(B; E) + 1$*

La hipótesis asegura que $(B, \gamma)E \neq E$. Para distintos podemos concluir, que

$$E = \bigcap_{n=1}^{\infty} (B, \gamma)^n E = 0$$

y este no es el caso. Por ello se sigue que los dos grados (que ocurren en las condiciones de el teorema) son apropiados mediante definición. Como un paso para probar este resultado primero establecemos el siguiente lema:

Lema 12. *Sea E, B y γ como en las condiciones de el Teorema 19. Asumamos también que $gr((B, \gamma); E) \geq 1$. Entonces existe $b \in B$ tal que $\gamma + b$ no es un divisor cero sobre E.*

Prueba. Puesto que $gr((B, \gamma); E) \geq 1$, el ideal (B, γ) contiene un elemento x que no es divisor de cero sobre E. Sea $x = r\gamma + b_0$, donde $r \in R$ y $b_0 \in B$. Probaremos que uno el menor de los elementos

$$\gamma + b_0^v \qquad (v = 1, 2, ...)$$

no es un divisor de cero sobre E y esto establece el lema.
Asumamos lo contrario y sea $P_1, P_2, ..., P_s$ ideales primos que pertenecen a el submódulo cero de E. Entonces un elemento de R es un divisor de cero sobre E sí y sólo sí está contenido por uno de $P_1, P_2, ..., P_s$.
Puesto que $\gamma + b_0^v$ es un divisor de cero para todo valor de v, es posible encontrar enteros m, n tal que $m < n$ y ambos $\gamma + b_0^m$ y $\gamma + b_0^n$ que pertenecen al mismo ideal primo P, donde P tiene lugar entre $P_1, P_2, ..., P_s$. Entonces $b_0^m(1 - b_0^{n-m}) \in P$. Ahora $b_0 \in B$ y B es contenido en el radical de Jacobson. De ello resulta que $1 - b_0^{n-m}$ no está contenido en alguno de los ideales maximales y por ello es una unidad. Multiplicando $b_0^m(1 - b_0^{n-m})$ por el inverso de $1 - b_0^{n-m}$, vemos que $b_0^m \in P$ y por ello $b_0 \in P$. De ello resulta que γ también pertenece a P.
Por consiguiente $x = r\gamma + b_0$ pertenece a P esto es lo que requiere la contradicción porque x no es un divisor de cero sobre E. $||$

Corolario 13. *E, B y γ satisfacen las hipótesis del Teorema 19 y supongamos, en adicción, que todo elemento de B es un divisor cero sobre E. Entonces $gr((B, \gamma); E) \leq 1$*

Prueba. Asumamos que $gr((B, \gamma); E) \geq 1$. Entonces, por el lema, existe $b \in B$ tal que $\gamma + b$ no es un divisor de cero sobre E.
Sea β un elemento arbitrario de B Entonces $\gamma + b, \beta$ no es una R-sucesión sobre E. (Para asumir lo contrario. $\gamma + b, \beta$ son contenidos en el radical de Jacobson, por ello resulta que $\beta, \gamma + b$ es también una R-sucesión sobre E. Sin embargo es imposible puesto que, por hipótesis, β es un divisor de cero sobre E.)
Por consiguiente:

$$(\gamma + b)E :_E \beta \neq (\gamma + b)E$$

y por ello β está contenido en uno de los ideales primos $P_1^{'}, P_2^{'}, ..., P_m^{'}$ que pertenecen a el submódulo $(\gamma + b)E$ de E. Pero β es un elemento arbitrario de B. Por ello resulta, que B mismo es contenido por uno de $P_1^{'}, P_2^{'}, ..., P_m^{'}$. Supongamos por definición que $B \subseteq P'$.
Entonces, puesto que $P_1^{'}$ contiene el ideal $(\gamma + b)E : E$, vemos que $P_1^{'}$ también contiene $\gamma + b$. De esta manera $(B, \gamma) = (B, \gamma + b) \subseteq P_1^{'}$.
Sin embargo

$$(\gamma + b)E :_E P_1^{'} \neq (\gamma + b)E$$

y por ello $(\gamma + b)$ es una R-sucesión maximal sobre E contenida en $P_1^{'}$. Por consiguiente $gr(P_1^{'}; E) = 1$.
Finalmente

$$gr((B, \gamma); E) \leq gr({P'}_1; E) = 1$$

y ahora la prueba es completa. $||$

Prueba de Teorema 19. Sea E, B y γ como en las condiciones de el teorema. Sea $gr(B;E) = s$ y $gr((B,\gamma);E) = t$. Entonces existe una R-sucesión $\alpha_1, \alpha_2, ..., \alpha_s$ sobre E y consideremos en B. También, por Teorema 17, esto puede ser extendido a una R-sucesión $\alpha_1, ..., \alpha_s, \alpha_{s+1}, ..., \alpha_t$ sobre E en (B,γ). Escribamos $\bar{E} = E/(\alpha_1, ..., \alpha_s)E$. Puesto que $\alpha_1, \alpha_2, ..., \alpha_s$ es una R-sucesión maximal sobre E en B, todo elemento de B es un divisor sobre $\bar{E}$.
El corolario Lema 12 por ello prueba que $gr((B,\gamma);\bar{B}) \leq 1$.
Sin embargo $\alpha_{s+1}, \alpha_{s+2}...., \alpha_t$ es una R-sucesión sobre $\bar{E}$ y todos estos elementos son contenidos en (B,γ). Por consiguiente $t - s \leq 1$ y la prueba es completa. $||$

Supogamos que E es un R-módulo Noetheriano y B un ideal de R tal que $BE \neq E$. Por Teorema 17, $gr(B;E)$ es finito. Consolidaremos este resultado probaremos que

$$gr(B;E) \leq rank[(Ann_R E, B)/Ann_R E]$$

donde $Ann_R E$ denota (como usual) el aniquilador ideal de E, y $(Ann_R E, B)$ es usado como una abreviacíon de $(Ann_R E) + B$. Observe que, el anillo $R/Ann_R E$ es Noetheriano y por ello cada uno de sus ideales propios tiene rango finito. Es conveniente a empezar por establecer

Proposición 10. *Sea E un R-módulo Noetheriano y $\alpha_1, \alpha_2, ..., \alpha_p$ elementos de R. Entonces*

$$Rad[(Ann_R E, \alpha_1, ..., \alpha_p)] = Rad[Ann_R(E/(\alpha_1, ..., \alpha_p)E)]$$

y los ideales primos que contienen $(Ann_R E, \alpha_1, ..., \alpha_p)$ son los mismos como los ideales que contienen $Ann_R(E/(\alpha_1, ..., \alpha_p)E)$. Si $(\alpha_1, ..., \alpha_p)E \neq E$ entonces

$$rank[Ann_R(E/(\alpha_1, ..., \alpha_p)E)/Ann_R E] \leq p$$

Prueba. Sea $A = Ann_R E$ y $B = Ann_R(E/(\alpha_1, ..., \alpha_p)E)$. Entonces

$$(A, \alpha_1, ..., \alpha_p) \subseteq B \text{ y } BE \subseteq (\alpha_1, ..., \alpha_p)E = (A, \alpha_1, ..., \alpha_p)E$$

puesto que E es finitamente generado, se sigue, que $B^n \subseteq (A, \alpha_1, ..., \alpha_p)$ para algunos enteros positivos n. La relación $B^n \subseteq (A, \alpha_1, ..., \alpha_p) \subseteq B$ ahora probamos que $Rad\ B = Rad(A, \alpha_1, ..., \alpha_p)$ y también que un ideal primo contiene B sí y sólo sí este contiene $(A, \alpha_1, ..., \alpha_p)$
Asumamos que $(\alpha_1, ..., \alpha_p)E \neq E$. Puesto que

$$(A, \alpha_1, ..., \alpha_p)E = (\alpha_1, ..., \alpha_p)E$$

de ello resulta que $(A, \alpha_1, ..., \alpha_p) \neq R$.
Consideremos B/A y $(A, \alpha_1, ..., \alpha_p)/A$. Algunos ideales primos de R/A que contienen la forma que contendrá el último y viceversa. De aquí que ambos son ideales propios y

$$rank(B/A) = rank((A, \alpha_1, ..., \alpha_p)/A)$$

finalmente $(A, \alpha_1, ..., \alpha_p)/A$ es un ideal que puede ser generado por p elementos a saber la imagen natural de $\alpha_1, \alpha_2, ..., \alpha_p$.
Puesto que R/A es un anillo Noetheriano, concluimos, que

$$rank((A, \alpha_1, ..., \alpha_p)/A) \leq p.$$

la proposición ahora resulta. ||

Proposición 11. *Sea E un R-módulo Noetheriano y $\alpha_1, \alpha_2, ..., \alpha_p$ una R-sucesión sobre E. Entonces*

$$rank[(Ann_R E, \alpha_1, ..., \alpha_p)/Ann_R E] = rank[Ann_R(E/(\alpha_1, ..., \alpha_p)E)/Ann_R E] = p$$

Además, si C es un ideal de R tal que $CE \neq E$, entonces $(Ann_R E, C) \neq R$ y $gr(C; E) \leq rank[(Ann_R E, C)/Ann_R E]$

Prueba. Como en la prueba de la proposición 10, sea

$$A = Ann_R E \ \text{ y } \ B = Ann_R(E/(\alpha_1, ..., \alpha_p)E)$$

puesto que

$$(A, \alpha_1, ..., \alpha_p)E = (\alpha_1, ..., \alpha_p)E \text{ y } (\alpha_1, ..., \alpha_p)E \neq E$$

de ello resulta que $(A, \alpha_1, ..., \alpha_p) \neq R$. Ahora supongamos que $0 \leq i \leq p$. Entonces α_{i+1} no es un divisor de cero sobre $E/(\alpha_1, ..., \alpha_p)E$ y por ello α_{i+1} no está contenido en algún ideal primo minimal de sus submódulos cero.
Por otra parte, estos ideales primos minimales son los mismos como los ideales primos contenidos de $Ann_R(E/(\alpha_1, ..., \alpha_i)E) = B_i$ digamos.
Ahora, por la proposición 10, el ideal primo que contiene B_i son los mismos como los ideales contenidos $(A, \alpha_1, ..., \alpha_i)$. Por consiguiente α_{i+1} no está contenido en algún ideal primo minimal de el último. Sea $\bar{\alpha}_j$ denota la imagen de α_j en el anillo Noetheriano $\bar{R} = R/A$. La observación de arriba prueba que $\bar{\alpha}_{i+1}$ no está contenido en algún ideal primo minimal de $\bar{\alpha}_1, \bar{\alpha}_2, ..., \bar{\alpha}_i$ y por ello

$$rank(\bar{\alpha}_1, \bar{\alpha}_2, ..., \bar{\alpha}_{i+1}) > rank(\bar{\alpha}_1, \bar{\alpha}_2, ..., \bar{\alpha}_i)$$

para $0 \leq i \leq p-1$. De esta manera $rank(\bar{\alpha}_1, \bar{\alpha}_2, ..., \bar{\alpha}_p) \geq p$ y, puesto que la desigualdad opuesta cumple, de ello resulta que

$$rank[(A, \alpha_1, ..., \alpha_p)/A] = rank[B/A].$$

Además, como cerramos en la prueba de Proposición 10,

$$rank[(A, \alpha_1, ..., \alpha_p)/A] = rank[B/A]$$

de esta manera la primera parte de la proposición queda establecida.
Ahora supongamos que $\alpha_1, \alpha_2, ..., \alpha_p$ es una R-sucesión maximal sobre E contenida en C así que $gr(C; E) = p$. Puesto que $(A, C)E = CE$ y $CE \neq E$, de ello resulta que $(A, C) \neq R$. Finalmente

$$gr(C; E) = p = rank[(A, \alpha_1, ..., \alpha_p)/A] \leq rank[(A, C)/A]$$

porque $(A, \alpha_1, ..., \alpha_p) \subseteq (A, C)$. Esto completa la prueba. ||

Corolario 14. *Sea R un anillo Noetheriano y $\alpha_1, \alpha_2, ..., \alpha_p$ una R-sucesión. Entonces*
$rank(\alpha_1, \alpha_2, ..., \alpha_p) = p$

Corolario 15. *Sea R un anillo Noetheriano y C un ideal propio de R. Entonces $gr(C) \leq rank\ C$*

ambos corolarios son obtenidos por tomar $E = R$ en la proposición justamente demostrada.

2.4. La teoría de grado por anillo semi-local

La teoría de grado puede ser considerablemente extendida si restringimos nuestra atención a anillos semilocales. Los resultados adicionales que puede ser obtenidos en este camino son el objeto de la presente sección.
Sea R un anillo semilocal y $M_1, M_2, ..., M_h$ sus ideales maximales. Escribamos

$$J = M_1 \cap M_2 \cap ... \cap M_h \tag{2.4.8}$$

tal que J es el radical de Jacobson. Por brevedad nos remitimos a J como el radical de R. Ahora hacemos un número de observaciones simples en orden para atraer la atención a hechos básicos que empleamos en lo que sigue. Todo R-módulo de generación finita es un R-módulo Noetheriano. Sea E uno de tales módulos y B un ideal contenido en el radical de J. Entonces,

$$\bigcap_{n=1}^{\infty} B^n E = 0 \tag{2.4.9}$$

De aquí si $E \neq 0$, entonces $BE \neq E$. Note que como caso especial de (2.4.9)

$$\bigcap_{n=1}^{\infty} J^n = (0) \tag{2.4.10}$$

Si los elementos $\alpha_1, \alpha_2, ..., \alpha_p$ pertenecen al radical de R forman una R-sucesión sobre E. Observamos, también que si K es un submódulo de el R-módulo Noetheriano E, entonces los ideales primos pertenecen al submódulo K son el mismo que pertenecen a el submódulo nulo de E/K.
Sea $\sigma : R \to \bar{R}$ un epimorfismo del anillo semilocal R a un anillo no-nulo $\bar{R}$. Entonces, $\bar{R}$ es también un anillo semilocal. Podemos suponer que los ideales maximales $M_1, M_2, ..., M_h$ de R son numerados $M_1, M_2, ..., M_i$ conteniendo el núcleo de σ mientras que $M_{i+1}, M_{i+2}, ..., M_h$ no. Por eso $\sigma(M_1), ..., \sigma(M_i)$ son los ideales maximales de $\bar{R}$ y $\sigma(M_j) = \bar{R}$ para $t + 1 \leq j \leq h$. Ahora $M_i + M_j = R$ si $i \neq j$. Donde,

$$J = M_1 \cap M_2 \cap ... \cap M_i \cap ... \cap M_h = M_1 M_2 ... M_i ... M_h.$$

Por consiguiente

$$\sigma(J) = \sigma(M_1)\sigma(M_2)...\sigma(M_i)...\sigma(M_h) = \sigma(M_1)\sigma(M_2)...\sigma(M_i)$$

y este es el radical de $\bar{R}$. De esta manera el epimorfismo σ mapea el radical de R en el radical de $\bar{R}$. En esta etapa es conveniente introducir dos nuevas definiciones. La primera de esta es de interés general porque nos permite aplicar el concepto de dimensión a módulos.
La segunda definición juega sólo un menor rol y desaparece de la discusión una vez haya servido a su propósito inmediato.

Definición 28. *Sea $E \neq 0$ un R-módulo. Entonces por la "dimensión" de E entenderemos la dimensión del anillo $R/Ann_R E$. La dimensión del módulo E será denotado por $DimE$.*

De esa manera $DimE = Dim(R/Ann_R E)$ o igualmente que, $DimE$ es igual a la dimensión $Dim(Ann_R E)$ del ideal de elementos que aniquilan a E. Note que la definición no requiere que R sea un anillo semilocal o aunque sea Noetheriano. Otro punto a notar es que si tomamos $R = E$. Encontraremos que no hay conflicto con la noción de dimensión anteriormente aplicada a anillos. Puede ser que E es un R-módulo Noetheriano y $P_1, P_2, ..., P_t$ los ideales primos pertenecen al submódulo nulo. Entonces

$$DimE = \max_{1 \leq i \leq t} dimP_i \tag{2.4.11}$$

esto es porque los ideales primos minimales que pertenecen al submódulo nulo de E son los mismos ideales primos minimales de $Ann_R E$.
Ahora supongamos que R es un anillo semilocal. Sea $E \neq 0$ un R-módulo de generación finita y denotaremos por $P_1, P_2, ..., P_t$ los ideales primos pertenecientes a el submódulo nulo. Escribamos

$$s(E) = \max_{1 \leq i \leq t} dimP_i - \min_{1 \leq j \leq t} dimP_j \tag{2.4.12}$$

y llamaremos $S(E)$ la *envergadura* de el R-módulo E. El hecho que R es un anillo semilocal asegura que la dimensión que ocurre en (2.4.12) es finita. Note que $s(E) \geq 0$ y

$$\min_{1 \leq i \leq t} \dim P_j = DimE - s(E) \tag{2.4.13}$$

También $s(E) = 0$ cuando y sólo cuando las dimensiones de los ideales primos pertencen al submódulo nulo de E son todas iguales, en tal caso el valor común de las dimesiones es $DimE$.

Teorema 20. *Sea R un anillo semilocal, $E \neq 0$ un R-módulo de generación finita y γ un elemento que pertenece al radical J de R y no es un divisor de cero en E. De aquí que $Dim(E/\gamma E) = DimE - 1$ y $s(E/\gamma E) \geq s(E)$.*

Prueba. Sea $DimE = r,\ s(E) = p,\ A = Ann_R E$ y $\bar{R} = R/A$.
Supongamos además que $\bar{\gamma}$ denota la imagen de γ bajo el mapeo natural $R \to \bar{R}$.
Por Proposición 10, los ideales primos que contiene $Ann_R(E/\gamma L)$ son los mismos que contienen (A, γ). De donde

$$Dim(E/\gamma E) = dim(A, \gamma) = DimR/(A, \gamma) = Dim\bar{R}/(\bar{\gamma})$$

porque $R/(A, \gamma)$ es anillo isomorfo a $\bar{R}/(\bar{\gamma})$.
Por hipótesis, γ no es un divisor-nulo sobre E.
Se sigue que γ no está contenido en algún ideal primo minimal perteneciente a un submódulo nulo de E y por tanto no está contenido en algún ideal primo minimal de A. Esto prueba que $dim(A, \alpha) < dimA = r$ y por lo tanto $Dim\bar{R}/(\bar{\gamma}) = dim(A, \gamma) < r = Dim\bar{R}$. Ahora $\bar{R}$ es un anillo semilocal y $\bar{\gamma}$ pertenece a cada uno de sus ideales maximales.
Consecuentemente,

$$Dim\bar{R}/(\bar{\gamma}) \geq Dim\bar{R} - 1.$$

Por consiguiente

$$Dim(E/\gamma E) = Dim\ \bar{R}/(\bar{\gamma}) = r - 1$$

y la primera afirmación está probada. Puesto que $s(E) = p$, se sigue, de (2.4.13), que existe un ideal primo P que pertenece al submódulo nulo de E y es tal que $dimP = r - p$. Ahora $0 :_E P \neq 0$. Consecuentemente existe $y \in E$ tal que $y \neq 0$ y $Py = 0$. Por (2.4.9) y el hecho que γ pertenece al radical de R, tenemos

$$\bigcap_{n=1}^{\infty} \gamma^n E = 0.$$

Por consiguiente existe un entero k tal que $y \in \gamma^k E$ y $y \notin \gamma^{k+1} E$. Sea $y = \gamma^k z$, donde $z \in E$. Entonces $z \notin \gamma E$ pero $\gamma^K Pz = Py = 0$. Sin embargo γ no es un divisor de cero en E así, esto implica que $Pz = 0$. Esto prueba que $\gamma E :_E P \neq \gamma E$. Porque el lado izquierdo contiene Z mientras el lado derecho no. Esto prueba que $P \subseteq P'$, donde P' es uno de los ideales primos pertenecientes al submódulo γE de E. Además P' tiene que contener estrictamente a P. (Ya que si $P = P'$, entonces

$$\gamma \in (\gamma E : E) \subseteq P' = P$$

que es imposible porque γ no es un divisor nulo en E.)
Por consiguiente

$$DimP' < dimP = r - p$$

y por tanto, ya que P' pertenece a el submódulo cero de $E/\gamma E$,

$$s(E/\gamma E) \geq Dim(E/\gamma E) - dimP' \geq (r-1) - (r-p-1) = p$$

Esto completa la prueba. ||

Corolario 16. *Sea R un anillo semilocal con radical J, $E \neq 0$ un R-módulo con generación finita, y $\alpha_1, \alpha_2, ..., \alpha_m$ una R-sucesión sobre E en J. Entonces*

$$Dim[E/(\alpha_1, ..., \alpha_m)E] = DimE - m \;\; y \;\; s[E/(\alpha_1, ..., \alpha_m)E] \leq DimE - gr(J; E)$$

Observación 2. *Es importante notar que para el caso $m = 0$ está incluido en el corolario. De esta manera la prueba mostrará que*

$$s(E) \leq DimE - gr(J; E). \tag{2.4.14}$$

Esto a su vez implica, por (2.4.13), que

$$gr(J; E) \leq \min_{1 \leq j \leq t} dimP_j \leq DimE \tag{2.4.15}$$

donde $P_1, P_2, ..., P_t$ denotan los ideales primos que pertenecen a el submódulo nulo de E.

Prueba: Comenzamos con la afirmación $Dim[E/(\alpha_1, ..., \alpha_m)E] = DimE - m$. Esto es trivial si $m = 0$. Ahora supongamos que $m > 0$ y sus
$E_i = E/(\alpha_1, ..., \alpha_i)E$. Entonces, para $0 \leq i \leq m-1, \alpha_{i+1}$ no es un divisor nulo en E_i y por tanto por Teorema 57 $Dim(E_i/\alpha_{i+1}E_i) = Dim\ E_i - 1$. Sin embargo

$$\alpha_{i+1}E_i = (\alpha_1, ..., \alpha_i, \alpha_{i+1})E/(\alpha_1, ..., \alpha_i)E$$

y por tanto $E_i/\alpha_{i+1}E_i$ es isomorfo a E_{i+1}.
Por consiguiente $DimE_{i+1} = DimE_i - 1$ y la primera afirmación del corolario resulta. Ahora cambiamos nuestra atención a la afirmación

$$s[E/(\alpha_1, ..., \alpha_m)E] \leq DimE - gr(J; E).$$

Si $\alpha_1, \alpha_2, ..., \alpha_m$ es una R-sucesión maximal sobre E en J, entonces

$$gr(J; E) = m$$

y todo elemento de J es un divisor nulo en $E/(\alpha_1, ..., \alpha_m)E$. Se sigue que J está contenido en uno de los ideales primos pertenecientes al submódulo nulo de $E/(\alpha_1, ..., \alpha_m)E$. Pero J es una intersección de ideales maximales. Esto prueba que uno de los ideales maximales de R pertenece al submódulo nulo de $E/(\alpha_1, ..., \alpha_m)E$. Por tanto, por la definición de la envergadura de un módulo

$$\begin{aligned} s[E/(\alpha_1, ..., \alpha_m)E] \quad &= Dim[E/(\alpha_1, ..., \alpha_m)E] \\ &= DimE - m \\ &= DimE - gr(J; E). \end{aligned}$$

Finalmente, supongamos que $\alpha_1, \alpha_2, ..., \alpha_m$ no es una R-sucesión maximal sobre E en J. Entonces el Teorema 17 prueba que podemos extenderlo de manera que llegue a ser una.
Sea $\alpha_1, ..., \alpha_m, \alpha_{m+1}, ..., \alpha_i$ una R-sucesión maximal.
sobre E en J y escribimos $E_i = E/(\alpha_1, ..., \alpha_i)E$ como antes. Por teorema 20 y el hecho que $E_i/\alpha_{i+1}E_i$ es isomorfo a E_{i+1}, vemos que $s(E_{i+1}) \geq s(E_i)$ y por tanto $s(E_t) \geq s(E_m)$. Sin embargo, lo observado del último párrafo prueba que $s(E_i) = DimE - gr(J; E)$. Así todo es probado. $||$.

El siguiente lema recoge algunos resultados simples que se requieren en la prueba de los teoremas principales.

Lema 13. *Sea R un anillo semilocal, $E \neq 0$ un R-módulo con generación finita y $\alpha_1, \alpha_2, ..., \alpha_m$ elementos contenidos en el radical J de R. Asumamos que*

$$Dim[E/(\alpha_1, ..., \alpha_m)E] = DimE - m$$

entonces $Dim[E/(\alpha_1, ..., \alpha_i)E] = DimE - i$ para $i = 0, 1, ..., m$. Además, cada valor de i satisface $0 \leq i < m$. El ideal primo pertenece al submódulo nulo de $E/(\alpha_1, ..., \alpha_i)E$ todo tiene dimensión igual a $DimE - i$, entonces $\alpha_1, \alpha_2, ..., \alpha_m$ es una R-sucesión en E

Prueba. Sea $A = Ann_R E$ y $\bar{R} = R/A$. Por proposición 10 los ideales primos que contienen a $Ann_R(E/(\alpha_1, ..., \alpha_m)E)$ son los mismos que contienen $(A, \alpha_1, ..., \alpha_m)$. De ello resulta que

$$dim(A, \alpha_1, ..., \alpha_m) = Dim[E/(\alpha_1, ..., \alpha_m)E] = DimE - m = Dim\bar{R} - m$$

supongamos que $\bar{\alpha}_j$ denota la imagen natural de α_j en $\bar{R}$. Entonces $\bar{R}$ es un anillo semilocal cuyo radical contiene elementos $\bar{\alpha}_1, \bar{\alpha}_2, \ldots, \bar{\alpha}_m$. Pasando al anillo $\bar{R}/(\bar{\alpha}_1, ..., \bar{\alpha}_m)$, vemos que

$$Dim\bar{R}/(\bar{\alpha_1}, ..., \bar{\alpha_i}) = dim(\bar{\alpha_1}, \bar{\alpha_2}, ..., \bar{\alpha_m}) = dim(A, \alpha_1, ..., \alpha_m) = Dim\bar{R} - m$$

de aquí, $\bar{\alpha_1}, \bar{\alpha_2}, ..., \bar{\alpha_m}$ es un subconjunto de un sistema de parámetros de $\bar{R}$. Supongamos ahora que $0 \leq i \leq m$. Entonces $\bar{\alpha_1}, \bar{\alpha_2}, ..., \bar{\alpha_i}$ es también un subconjunto de un sistema de parámetros de $\bar{R}$ y por tanto por la misma proposición, $Dim\bar{R}/(\bar{\alpha_1}, ..., \bar{\alpha_i}) = Dim\bar{R} - i$. Por consiguiente

$$\begin{aligned} dim(A, \alpha_1, ..., \alpha_i) \quad &= dim(\bar{\alpha_1}, \bar{\alpha_2}, ..., \bar{\alpha_i}) = Dim\bar{R}/(\bar{\alpha_1}, ..., \bar{\alpha_i}) \\ &= Dim\bar{R} - i = DimE - i \end{aligned}$$

sin embargo, por proposición 10, $(A, \alpha_1, ..., \alpha_i)$ y el ideal aniquilador de $E/(\alpha_1, ..., \alpha_i)E$ tiene la misma dimensión. Esto lleva a

$$Dim[E/(\alpha_1, ..., \alpha_i)E] = DimE - i$$

y se establece la primera parte del lema. Ahora asumamos que (para cada i $0 \leq i < m$) el ideal primo pertenece al submódulo nulo de

$$E/(\alpha_1, ..., \alpha_i)E = E_i$$

(digamos) todos tienen dimensión igual a $DimE - i$. Entonces α_{i+1} no puede estar contenido en algún ideal primo que pertenece a el submódulo nulo de E_i. Si asumimos que uno de estos ideales primos, digamos P, contiene a α_{i+1}. Entonces tendríamos $dimP = DimE - i$ y también

$$(A, \alpha_1, ..., \alpha_i, \alpha_{i+1}) \subseteq P$$

porque P contiene todo ideal, tal como $(A, \alpha_1, ..., \alpha_i)$ que aniquila E_i. Por consiguiente

$$dim(A, \alpha_1, ..., \alpha_i, \alpha_{i+1}) \geq dimP = DimE - i$$

y ahora tenemos una contradicción porque ya vimos que

$$dim(A, \alpha_1, ..., \alpha_i, \alpha_{i+1}) = DimE - i - 1.$$

Se sigue que α_{i+1} no es un divisor nulo en E_i. Como esto se tiene para $0 \leq i < m$ vemos que $\alpha_1, \alpha_2, ..., \alpha_m$ es una R-sucesión en E. La prueba es ahora completa. ||

Teorema 21. *Sea R un anillo semilocal con radical J y $E \neq 0$ un R-módulo finitamente generado.*
Entonces las siguientes dos afirmaciones son equivalentes:

(a) $gr(J; E) = DimE$

(b) $\alpha_1, \alpha_2, ..., \alpha_m$ $(m \geq 0)$ *pertenece a J y*

$$Dim[E/(\alpha_1, ..., \alpha_m)E] = DimE - m$$

entonces todos los ideales primos que pertenecen al submódulo nulo de $E/(\alpha_1, ..., \alpha_m)E$ tiene la misma dimensión.

Prueba. Primero asumimos que (a) es verdadero. Sea $\alpha_1, ..., \alpha_m$ pertenece a J y tal que $Dim[E/(\alpha_1, ..., \alpha_m)E]DimE - m$. Sea $E_i = E/(\alpha_1, ..., \alpha_i)E$. Tenemos que probar que $s(E_m) = 0$. Esto se realizará usando inducción en i, $s(E_i) = 0$ para $i = 0, 1, ..., m$. El caso $i = 0$ es trivial porque, por (2.4.14),

$$0 \leq s(E) \leq DimE - gr(J; E)$$

Por tanto supongamos que $0 < i \leq m$ y también que $s(E_j) = 0$ para $0 \leq j < i$. Por Lema 13, tenemos

$$Dim[E/(\alpha_1, ..., \alpha_j)E] = DimE - j$$

para $0 \leq j \leq m$. Esto resulta (usando hipótesis inductiva) que si $0 \leq j < i$ entonces todo ideal primo pertenece al submódulo nulo de $E/(\alpha_1, ..., \alpha_j)E$ debe tener igual dimensión a $DimE - j$. De aquí que otra vez usamos Lema 13, $\alpha_1, \alpha_2, ..., \alpha_i$ es una R-sucesión sobre E. Por consiguiente, por el Teorema 20,

$$0 \leq s(E_i) \leq DimE - gr(J; E).$$

De esa manera $s(E_i) = 0$ y concluimos que (a) implica (b). Ahora asumimos que (b) es verdadero. Sea

$$A = Ann_R E, \quad \bar{R} = R/A \text{ y } DimE = p$$

entonces $\bar{R}$ es un anillo semilocal p-dimensional. Consideremos el epimorfismo natural $R \to \bar{R}$. Este mapeo de el radical de R sobre el radical de $\bar{R}$ encontraremos elementos $\alpha_1, \alpha_2, ...\alpha_p$ en J así que sus imagenes $\bar{\alpha}_1, \bar{\alpha}_2, ..., \bar{\alpha}_p$ forma un sistema de paramentros de $\bar{R}$. Entonces

$$\begin{aligned} Dim[E/(\alpha_1, \alpha_2, ...\alpha_p)E] \quad &= dim(A, \alpha_1, ...\alpha_p) = dim(\bar{\alpha_1}, \bar{\alpha_2}, ..., \bar{\alpha_p}) \\ &= 0 = DimE - p. \end{aligned}$$

Por Lema 13, $Dim[E/(\alpha_1, \alpha_2, ..., \alpha_i)E] = Dim\ E - i$ para $0 \leq i \leq p$
Además, todo ideal primo que pertenece al submódulo nulo de $E/(\alpha_1, \alpha_2, ...\alpha_i)E$ tiene dimensión igual a $DimE - i$ porque asumimos (b) es verdadero. Por consiguiente, por la segunda parte del Lema 13, $\alpha_1, \alpha_2, ...\alpha_p$ es una R-sucesión en E y por tanto $gr(J; E) \geq p = Dim\ E$.
Sin embargo la desigualdad opuesta se tiene por virtud de (2.4.15) y así la prueba se completa. ||

Proposición 12. *Sea R un anillo semilocal con radical J y $E \neq 0$ una generación finita de R-módulos que satisface $gr(J; E) = DimE$.*
Si ahora $\alpha_1, \alpha_2, ..., \alpha_m$ pertenece a J y

$$Dim[E/(\alpha_1, ..., \alpha_m)E] = DimE - m,$$

entonces $\alpha_1, \alpha_2, ..., \alpha_m$ es una R-sucesión en E.

Prueba. La primer parte del Lema 13 prueba que

$$Dim[E/(\alpha_1, ..., \alpha_i)E] = DimE - i$$

para $0 \leq i \leq m$. Luego el primer ideal pertenece a el submódulo nulo de $E/(\alpha_1, ..., \alpha_i)E$ con dimensión igual a $DimE - i$.
De aquí que, por la segunda parte del Lema 13, $\alpha_1, \alpha_2, ..., \alpha_m$ es una R-sucesión en E. Esto establece la proposición. ||

Teorema 22. *Sea R un anillo semilocal con radical J y $E \neq 0$ un R-módulo con generación finita que satisface $gr(J; E) = DimE$.*
Si ahora P es algún ideal primo que contiene el aniquilador $Ann_R E$ de E entonces

$$gr(P; E) = rank(P/Ann_R E) \quad y$$

$$DimE = rank(P/Ann_R E) + dim\ P.$$

Prueba. Veamos, que $PE \neq E$. De aquí, por Proposición 11,

$$gr(P; E) \leq rank(P/Ann_R E).$$

También, por razones triviales,

$$\begin{aligned} rank(P/Ann_R E) + dim\ P &= rank(P/Ann_R E) + dim(P/Ann_R E) \\ &\leq Dim(R/Ann_R E) \\ &= DimE \end{aligned}$$

esto es por tanto suficiente probar que $gr(P; E) + dim\ P \geq DimE$.
Para este fin sea $\alpha_1, \alpha_2, ..., \alpha_k$ una R-sucesión maximal sobre E en $P \cap J$.
Por el corolario Teorema 20,

$$Dim[E/(\alpha_1, ..., \alpha_k)E] = DimE - k$$

y, por Teorema 21, cada ideal primo pertenece al submódulo nulo de $E/(\alpha_1, ..., \alpha_k)E$ tiene dimensión igual a $DimE - k$.
Además, uno de los ideales primos, digamos P', debe contener $P \cap J$ para destinar que existe una R-sucesión sobre E en $P \cap J$ que es más grande que $\alpha_1, \alpha_2, ..., \alpha_k$.
De esa manera $dimP' = DimE - k$ y ambos $P \subseteq P'$ o $J \subseteq P'$.
Si $P \subseteq P'$, entonces todos los elementos de P es un divisor nulo en $E/(\alpha_1, ..., \alpha_k)E$ y por tanto $\alpha_1, \alpha_2, ..., \alpha_k$ es una R-sucesión maximal sobre E en P. De esta manera $gr(P; E) = k$ y por lo tanto

$$gr(P; E) + dimP \geq k + dimP' = DimE.$$

Por otro lado, si $J \subseteq P'$, entonces P' es un ideal maximal de R y así

$$DimE - k = dimP' = 0.$$

Por consiguiente

$$gr(P; E) + dim\ P \geq gr(P; E) \geq K = DimE$$

como requiere.||

Teorema 23. *Sea R un anillo semilocal con radical J y $E \neq 0$ un R-módulo finitamente generado.*
Entonces las siguientes tres afirmaciones son equivalentes:

(a) $gr(J; E) = DimE = Dim\ R$;

(b) *todo sistema de parámetro es una R-sucesión sobre E;*

(c) *allí es el menor un sistema de parámetro que es una R-sucesión sobre E.*

Observación 3. *Por (2.4.15), tenemos*

$$gr(J; E) \leq DimE \leq Dim\ R.$$

Así (a) es válido si y sólo si $gr(J; E) = Dim\ R$. Nuevamente si $Dim\ R = 0$, entonces el conjunto vacío es sólo un sistema de parámetro.
Esto es considerado como formando una R-sucesión sobre todo R-módulo no nulo.

Prueba. Daremos una demostración cíclica. Primero supongamos que (a) es verdadero y sea $\alpha_1, \alpha_2, ..., \alpha_d$ un sistema de parámetro de R. Entonces $d = DimR$ y, puesto que $E/(\alpha_1, ..., \alpha_d)E$ es un módulo no nulo aniquilado por $(\alpha_1, \alpha_2, ..., \alpha_d)$,

$$Dim[E/(\alpha_1, \alpha_2, ..., \alpha_d)E] = 0 = DimE - d.$$

el cual $\alpha_1, \alpha_2, ..., \alpha_d$ es una R-sucesión sobre E, ahora sigue de la Proposición 12. Así (a) implica (b), es obvio (b) implica (c). Ahora asumamos que $\alpha_1, \alpha_2, ..., \alpha_d$ es un sistema de parámetro que es también una R-sucesión sobre E. Entonces

$$gr(J; E) \geq d = DimR$$

y la ecuación

$$gr(J; E) = DimE = Dim\ R$$

sigue por virtud de la observación hace inmediata la afirmación posterior de el teorema. La prueba esta ahora completa. ||

2.5. Anillo Semi-regular

En esta sección la teoría de grado será aplicada al estudio de una importante clase de anillos Noetherianos. Esta clase convenientemente se describe con la ayuda de dos definiciones preliminares. Sea A un ideal propio en un anillo Noetheiano no-nulo R.

Definición 29. *El ideal A se dice llamar la clase fundamental si puede ser generado por r elementos, donde $r = rankA$.*

A no puede ser generado por menos elementos que $rankA$; de aquí que un ideal de la clase fundamental es en un extremo sistuado respecto del rango. Por consiguiente a convención por lo que el conjunto vacío es considerado como generador el ideal cero, el ideal cero es necesariamente la clase fundamental. En efecto solo el ideal de rango cero tiene esta propiedad.

Definición 30. *El ideal A se dice ser “puro en respecto del rango ” si todo ideal primo perteneciente a A tiene el mismo rango.*

Claramente si A es puro en respecto del rango, entonces todo ideal primo perteneciente a A tiene el mismo rango como A mismo.
También A no tiene ideal primo fijo. Veamos ahora el concepto central de esta sección.

Definición 31. *Un anillo Noetheriano no nulo puede ser llamado “semi-regular” si todo ideal propio de la clase fundamental es puro con respecto del rango.*

Un anillo Semi-regular es también a saber un anillo Macaulay-Cohen.

Teorema 24. *Sea R un anillo local de dimensión $d \geq 0$. Entonces las siguientes tres afirmaciones son equivalentes:*

(a) *R es semi-regular*

(b) *existe un menor sistema de parámetros que es una R-sucesión;*

(c) *todo sistema de parámetro es una R-sucesión.*

Observación 4. *Debe de notar que si $d = 0$, entonces R es simi-regular porque, en este caso, existe sólo un ideal primo.*

Ver también la observación del Teorema 23.
Prueba. Sea M el ideal maximal de R así que $rank\ M = d$. Empezaremos por asumir que (a) es verdadero. Por lo que, existen elementos $\alpha_1, \alpha_2, ..., \alpha_i = i$ pertenecientes a M tal que $rank(\alpha_1, \alpha_2, ..., \alpha_i) = i$, para $0 \leq i \leq d$.
Por consiguiente, $(\alpha_1, \alpha_2, ..., \alpha_i)$ es de la clase fundamental y por ello, puesto que R es simi-regular, todo ideal primo perteneciente a este tiene rango igual a i. Si por ello $i < d$, entonces α_{i+1} no petenece a alguno de estos ideales primos para distintos $(\alpha_1, \alpha_2, ..., \alpha_i, \alpha_{i+1})$ debía tener solo $rank\ i$. Por consiguiente

$$(\alpha_1, \alpha_2, ..., \alpha_i) : \alpha_{i+1} = (\alpha_1, \alpha_2, ..., \alpha_i)$$

que prueba que $\alpha_1, \alpha_2, ..., \alpha_d$ es una R-sucesión. Además $(\alpha_1, \alpha_2, ..., \alpha_d)$ tiene rango igual a d y por ello $\alpha_1, \alpha_2, ..., \alpha_d$ es un sistema de parámetro.
De esta menera se prueba que (a) implica (b). Ahora supongamos que (b) es verdadero. Tomando $E = R$ en Teorema 23, encontramos que todo sistema de parámetro es una R-sucesion. De esta manera (b) implica (c).
Finalmente asumamos que tenemos (c). Entonces, de nuevo usamos el Teorema 23, $gr(M) = Dim\ R$ y así se sigue, del Teorema 22 que

$$dimP + rankP = DimR$$

para todo ideal primo P. Sea $\beta_1, \beta_2, ..., \beta_r$ elementos de R que generan un ideal de *rank* r. Por consideración el ideal primo que pertenece a $(\beta_1, \beta_2, ..., \beta_r)$, vemos una vez que $dim(\beta_1, \beta_2, ..., \beta_r) = d - r$. De esta manera la dimensión de los R-módulos $R/(\beta_1, \beta_2, ..., \beta_r)$ es $DimR - r$.
Podemos por ello aplicar el Teorema 21 (con $E = R$) para deducir que todo ideal primo perteneciente a $(\beta_1, \beta_2, ..., \beta_r)$ tiene dimensión $d - r$. Por este medio todos esos ideales primos tienen *rank* r. Por consiguiente $(\beta_1, \beta_2, ..., \beta_r)$ es puro en respecto del rango y por ello R puede ser probado para ser semi-regular. ||

Corolario 17. *Sea R un anillo local que es semi-regular. Entonces*

$$DimP + rankP = DimR$$

para todo ideal primo P.

En orden vemos que es suficiente observar que, en la trayectoria de la prueba justamente dada, prueba que la relación $DimP + rankP = DimR$ es una consecuencia de la condición (c) en las consideraciones del teorema.

Lema 14. *Sea R un anillo semi-regular y P uno de sus ideales primos. Entonces R_P es un anillo local semi-regular.*

Prueba. Sea $rankP = d$. Tal que, existen elementos $\alpha_1, \alpha_2, ..., \alpha_d$ en P tal que $rank(\alpha_1, \alpha_2, ..., \alpha_i) = i$ para $0 \leq i \leq d$. Puesto que R es semi-regular, todos los ideales pertenecientes a $(\alpha_1, \alpha_2, ..., \alpha_i)$ tienen rango igual a i. De ello resulta que

$$(\alpha_1, \alpha_2, ..., \alpha_i) : \alpha_{i+1} = (\alpha_1, \alpha_2, ..., \alpha_i)$$

siempre que $0 \leq i < d$. Notemos, en el procedimiento anterior, que P es un ideal primo minimal de $\alpha_1, \alpha_2, ..., \alpha_d)$.
Sea $\chi : R \to R_P$ el mapeo canónico. Tal que

$$(\chi(\alpha_1), ..., \chi(\alpha_i)) : \chi(\alpha_{i+1}) = (\chi(\alpha_1), ..., \chi(\alpha_i))$$

para $0 \leq i < d$. De ello resulta que $\chi(\alpha_1), \chi(\alpha_2), ..., \chi(\alpha_d)$ son ambos una R_P-sucesión y un sistems de parámetros en R_P. Este R_P es un anillo local semi-regular es ahora una consecuencia de Teorema 24. Esto completa la prueba. ||

Teorema 25. *Sea R un anillo Noetheriano no-nulo. Entonces R es semi-regular sí y sólo sí R_M es semi-regular para todo ideal maximal M.*

Prueba. Asumamos que R_M es semi-regular para todo ideal maximal M y se deduce de esto que R mismo es semi-regular. Lo recíproco se sigue de Lema 14. Sea $(\alpha_1, \alpha_2, ..., \alpha_r)$ r elementos que generan un ideal de *rank* r. Entonces todo ideal primo *minimal* de $(\alpha_1, \alpha_2, ..., \alpha_r)$ tiene *rank* r.
Supongamos ahora que P es un ideal primo arbitrario perteneciente a $(\alpha_1, \alpha_2, ..., \alpha_r)$.
El teorema resulta si podemos probar que el rango de P es igual a r.
Existe un ideal maximal M tal que $(\alpha_1, \alpha_2, ..., \alpha_r) \subseteq P \subseteq M$.
De paso el anillo R_M de fracciones, encontramos, que $(\alpha_1, \alpha_2, ..., \alpha_r)$ extendido a un ideal de la clase fundamental de quienes el rango es r y que tiene P_M como uno de sus ideales. Puesto que R_M es semi-regular, de ello resulta que $P_M = r$.
Sin embargo $rankP_M = rank\ P$. Por consiguiente $rank\ P = r$ y el teorema esta probado. ||

El siguiente resultado proporciona una generalización del Lema 14.

Teorema 26. *Sea R un anillo semi-regular y S un subconjunto no vacío multiplicativamente cerrado, el subconjunto de R no contiene el elemento cero. Entonces R_S es también un anillo semi-regular.*

Prueba. Empezaremos negando que R_S es un anillo Noetheriano no nulo.
Sea M un ideal maximal de R_S. Entonces $M = P_S$, donde P es algún ideal primo de R que no satisface S. Por el Teorema 25, es suficiente probar que $(R_S)_M$, que es $(R_S)_{P_S}$ es semi-regular.
Sin embargo, $(R_S)_{P_S}$ es anillo-isomorfo a R_P y sabemos que R_P es semi-regular por virtud de Lema 14. Esto completa la prueba. ||

Teorema 27. *Sea R un anillo semi-regular y P', P ideales primos de R que satisfacen $P' \subseteq P$. Entonces $rankP = rank(P/P') + rankP'$*

si localizamos a P, entonces lo requerido en el resultado se sigue inmediatamente de Lema 14 y el Teorema 24.

Teorema 28. *Sea R un anillo semi-regular y A un ideal de la clase fundamental. Entonces R/A es también un anillo semi-regular.*

Prueba. Sea $r = rankA$. Entonces, puesto que A pertenece a la clase fundamental, existen elementos $\alpha_1, \alpha_2, ..., \alpha_r$ que genera A. Sea $\bar{R} = R/A$ y asumamos que $\beta_1, \beta_2, ..., \beta_s$ pertenecen a R y tal que

$$rank(\bar{\beta}_1, \bar{\beta}_2, ..., \bar{\beta}_s) = s.$$

Aquí $\bar{\beta}_i$ denota la imagen natural de β_i en $\bar{R}$. El ideal primo perteneciente a el $\bar{R}$-ideal $(\bar{\beta}_1, \bar{\beta}_2, ..., \bar{\beta}_s)$ son justamente los ideales Π/A, donde Π es un ideal primo característico perteneciente a

$$(\alpha_1, ..., \alpha_r, \beta_1, ..., \beta_s).$$

Para establecer el teorema debemos probar que $rank(\Pi/A) = s$ en todo caso.
Sea P un ideal primo *minimal* de $(\alpha_1, ..., \alpha_r, \beta_1, ..., \beta_s)$.
Entonces P/A es un ideal primo minimal de $(\bar{\beta}_1, ..., \bar{\beta}_s)$.
Por consiguiente $rank(P/A) \leq s$, tenemos en hecho $rank(P/A) = s$.
De ello resulta que existe un ideal primo minimal P' de A tal que $A \subseteq P' \subseteq P$ y $rank(P/P') = s$.
Sin embargo todos los ideales primos pertenecientes a A tiene rango igual a r y así , en particular, $rankP' = r$. De aquí, por el Teorema 27,

$$rankP = rankP' + rank(P/P') = r + s.$$

Esto prueba que

$$rank(\alpha_1, ..., \alpha_r, \beta_1, ..., \beta_s) = r + s$$

y demuestra que el R-ideal $(\alpha_1, ..., \alpha_r, \beta_1, ..., \beta_s)$ es de la clase fundamental.
Ahora asumamos que Π es un ideal primo arbitrario perteneciente a

$$(\alpha_1, ..., \alpha_r, \beta_1, ..., \beta_s).$$

puesto que R es semi-regular y el ideal es de la clase fundamental, podemos concluir que $\Pi = r + s$. Luego podemos escoger un ideal primo minimal P^* de A tal que $P^* \subseteq \Pi$ y

$$rank(\Pi/P^*) = rank(\Pi/A).$$

entonces, usando el Teorema 27 y el hecho que $rank\ P* = r$, obtenemos

$$rank(\Pi/A) = rank\ \Pi - rank\ P^* = r + s - r = s$$

esto completa la prueba. ||

2.6. Propiedades generales de los anillos polinomiales

Como usualmente, R denota un anillo conmutativo con un elemento identidad y $R[X_1, X_2, ..., X_n]$ el anillo de polinomio en $X_1, X_2, ..., X_n$ con coeficientes en R. Por consiguiente un elemento característico f de $R[X_1, X_2, ..., X_n]$ tiene representación *única*

$$f = \sum r_{\mu_1,\mu_2 \ldots \mu_n} X_1^{\mu_1} X_2^{\mu_2} \ldots X_n^{\mu_n}, \tag{2.6.16}$$

donde los $r_{\mu_1,\mu_2 \ldots \mu_n}$ pertenece a R y sólo un número finito de ellos son diferentes de cero. Sea A un ideal del anillo R. *En orden el polinomio f, de*

(2.6.16), debe pertenecer a la extensión $AR[X_1, X_2, ..., X_n]$ de A, estos son ambos necesarios y suficientes para todos los coeficientes $r_{\mu_1,\mu_2...\mu_n}$ pertenecen a A. Una consecuencia inmediata de esta observación es la relación

$$AR[X_1, X_2, ..., X_n] \cap R = A \tag{2.6.17}$$

supongamos ahora que $\{A_i\}_{i\in I}$ es una familia de ideales de R.
Entonces la misma observación prueba que

$$\left(\bigcap_{i\in I} A_i\right) R[X_1, X_2, ..., X_n] = \bigcap_{i\in I}(A_i R[X_1, X_2, ..., X_n]). \tag{2.6.18}$$

como antes, sea A un ideal de R. Si f es el polinomio descrito en (2.6.16) y $c \in R$, entonces cf pertenece a $AR[X_1, X_2, ..., X_n]$ sí y sólo sí $cr_{\mu_1,\mu_2,...,\mu_n} \in A$; esto es sí y sólo sí $r_{\mu_1,\mu_2,...,\mu_n} \in (A : c)$, de cada coeficiente $r_{\mu_1,\mu_2,...,\mu_n}$.
por consiguiente

$$AR[X_1, X_2, ..., X_n] : c = (A : c)R[X_1, X_2, ..., X_n] \tag{2.6.19}$$

si C también un R-ideal. Entonces $A : C = \bigcap_{c\in C}(A : c)$ y, usando (2.6.19), afirmamos que

$$\begin{aligned} AR[X_1, ..., X_n] : CR[X_1, ..., X_n] &= \bigcap_{c\in C}(AR[X_1, X_2, ..., X_n] : c) \\ &= \bigcap_{c\in C}((A : c)[X_1, X_2, ..., X_n]) \end{aligned}$$

por lo tanto se sigue, de (2.6.18), que

$$AR[X_1, ..., X_n] : CR[X_1, ..., X_n] = (\bigcap_{c\in C}(A : c))R[X_1, ..., X_n]$$

que puede reescribirse como

$$AR[X_1, ..., X_n] : CR[X_1, ..., X_n] = (A : C)R[X_1, ...X_n]. \tag{2.6.20}$$

a ún asumimos que A es un R ideal, sea $\phi : R \to R/A$ el mapeo natural.
Se obtiene un anillo epimorfismo

$$R[X_1, X_2, ..., X_n] \to (R/A)[X_1, X_2, ..., X_n]$$

por la operación con ϕ en los coeficientes de cada polinomio en $R[X_1, X_2, ..., X_n]$.
El núcleo de este epimorfismo es claramente $AR[X_1, X_2, ..., X_n]$.
Consecuentemente se induce un anillo isomorfismo

$$R[X_1, X_2, ..., X_n]/AR[X_1, X_2, ..., X_n] \approx (R/A)[X_1, X_2, ..., X_n] \tag{2.6.21}$$

este isomorfismo es frecuentemente usado para identificar los dos anillos que ocurren en (2.6.21). Otra útil identificación puede originarse en el siguiente camino. Sea S un conjunto no vacío multiplicativo cerrado subconjunto de R. Entonces es algún subconjunto multiplicativo cerrado de $R[X_1, X_2, ..., X_n]$ y por tanto podemos formar el anillo $R[X_1, X_2, ..., X_n]_S$ de fracciones. Sea

$$f = \sum r_{v_1,v_2...v_n} X_1^{v_1} X_2^{v_2} ... X_n^{v_n}$$

es un elemento característico de $R[X_1, X_2, ..., X_n]$.
Ahora obtenemos un anillo-isomorfismo

$$R[X_1, X_2, ..., X_n]_S \approx R_S[X_1, X_2, ..., X_n] \qquad (2.6.22)$$

por medio del mapeo

$$\left[\frac{f}{s}\right] \to \sum \left[\frac{r_{v_1,v_2...v_n}}{s}\right] X_1^{v_1} X_2^{v_2} ... X_n^{v_n}$$

aquí, desde luego, s denota un elemento de S. Sea D el monoide consistente de toda sucesión $(v_1, v_2, ..., v_n)$ de n enteros no negativos, esto es entendible que la adición de tal sucesión es definida por

$$(v_1, v_2, ..., v_n) + (v_1', v_2', ..., v_n') = (v_1 + v_1', v_2 + v_2', ..., v_n + v_n').$$

el monoide D es menor torsión. Además puede ser considerado como un anillo D-grado en que el elemento homogéneo de grado $(v_1, v_2, ..., v_n)$ son dados la forma $rX_1^{v_1} X_2^{v_2} ... X_n^{v_n}$ donde r pertenece a R. Sea A un ideal de R.
Entonces $AR[X_1, X_2, ..., X_n]$ es un ideal homogéneo y por tanto,

$$Rad(AR[X_1, ..., X_n])$$

es también homogéneo, *Ahora sostenemos que*

$$(Rad\ A)R[X_1, X_2, ..., X_n] = Rad(AR[X_1, X_2, ..., X_n]) \qquad (2.6.23)$$

efectivamente es claro que el lado izquierdo es contenido en el lado derecho. Para probar la inclusión opuesta, es suficiente probar que si un elemento homogéneo $rX_1^{v_1} X_2^{v_2} ... X_n^{v_n}$ pertenece a $Rad(AR[X_1, X_2, ..., X_n])$, entonces $r \in RadA$. Sin embargo, si $(rX_1^{v_1} X_2^{v_2} ... X_m^{v_n})^m \in AR[X_1, ..., X_n]$, entonces $r^m \in A$ y por tanto $r \in Rad\ A$ como se ha requerido.

Proposición 13. *Sea P un ideal primo de R. Entonces $PR[X_1, X_2, ..., X_n]$ es un ideal primo de el anillo polinomial $R[X_1, X_2, ..., X_n]$.*

Prueba. Primero notaremos que $PR[X_1, X_2, ..., X_n]$ es un ideal homogéneo propio de $R[X_1, X_2, ..., X_n]$.
De aquí, es suficiente determinar la propiedad característica de un ideal primo dada en el caso de elementos *homogéneos*. Sin embargo esto es obvio. ||

Corolario 18. *Si R es un dominio integral, entonces el anillo polinomial*

$$R[X_1, X_2, ..., X_n]$$

es también un dominio integral.

Este es el caso especial de Proposición 13 en que P es el ideal nulo. Nuestro siguiente resultado concierne una importante propiedad de divisores nulos en un anillo polinomial.

Proposición 14. *Sea $f(X_1, X_2, ..., X_n)$ un divisor nulo en el anillo polinomial $R[X_1, X_2, ..., X_n]$.*
Entonces existe c en R tal que

$$c \neq 0$$

y $cf(X_1, X_2, ..., X_n) = 0$. Prueba. Podemos observar que $R[X_1, X_2, ..., X_n]$ es grado por el monoide consiste de toda sucesión de n enteros no negativos. Este monoide es menor torsión. Por ello puede ser dado un orden total que es compatible con su estructura monoide. Sea

$$f(X_1, ..., X_n) = \alpha X_1^{\mu_1} X_2^{\mu_2} ... X_n^{\mu_n} + \beta X_1^{\nu_1} X_2^{\nu_2} ... X_n^{\nu_n} + ... + \omega X_1^{\sigma_1} X_2^{\sigma_2} ... X_n^{\sigma_n}$$

donde $\alpha, \beta, ..., \omega$ son en R y

$$(\mu_1, \mu_2, ..., \mu_n) > (\nu_1, \nu_2, ..., \nu_n) > ... > (\sigma_1, \sigma_2, ..., \sigma_n).$$

por hipótesis, existe $g(X_1, X_2, ..., X_n) \neq 0$ tal que

$$f(X_1, ..., X_n) g(X_1, ..., X_n) = 0$$

escojamos $g(X_1, X_2, ..., X_n)$ así que se satiaface esta condición y, en adición, tenemos la pequeña posibilidad de un número de términos no nulos. Sea

$$g(X_1, X_2, ..., X_n) = cX_1^{m_1} X_2^{m_2} ... X_n^{m_n} + ...,$$

donde $c \in R,\ c \neq 0$, y $X_1^{m_1} X_2^{m_2} ... X_n^{m_n}$ es el alto producto potencia actual que ocurre en $g(X_1, X_2, ..., X_n)$. Puesto que $f(X_1, ..., X_n) g(X_1, ..., X_n) = 0$ vemos, por considerar el término de grado $(\mu_1 + m_1, \mu_2 + m_2, ..., \mu_n + m_n)$, que $\alpha c = 0$. De esa manera $\alpha g(X_1, X_2, ..., X_n)$ tiene menos términos no nulo que $g(X_1, X_2, ..., X_n)$ y $f(X_1, ..., X_n)\alpha g(X_1, ..., X_n) = 0$. De aquí, por escoger $g(X_1, ..., X_n)$, debemos tener $\alpha g(X_1, ..., X_n) = 0$. Luego observamos que

$$[f(X_1, X_2, ..., X_n) - \alpha X_1^{\mu_1} X_2^{\mu_2} ... X_n^{\mu_n}] g(X_1, X_2, ..., X_n) = 0$$

que es

$$(\beta X_1^{\nu_1} X_2^{\nu_2} ... X_n^{\nu_n} + ... + \omega X_1^{\sigma_1} X_2^{\sigma_2} ... X_n^{\sigma_n}) g(X_1, X_2, ..., X_n) = 0$$

se calcula considerando del término de grado

$$(\nu_1 + m_1, \nu_2 + m_2, ..., \nu_n + m_n)$$

prueba que $\beta c = 0$. De esa manera $\beta g(X_1, X_2, ..., X_n)$ tiene menos términos no nulos que $g(X_1, X_2, ..., X_n)$ y $f(X_1, ..., X_n)\beta g(X_1, ..., X_n) = 0$.
Consecuentemente, por el escogido de $g(X_1, X_2, ..., X_n)$. Tenemos

$$\beta g(X_1, ..., X_n) = 0.$$

siguiendo el mismo proceso, probaremos en la sucesión, que

$$\alpha c = 0, \ \beta c = 0, ..., \omega c = 0.$$

por consiguiente $cf(X_1, X_2, ..., X_n) = 0$ y la prueba se completa.||

Probaremos ahora que un ideal primario del anillo R queda primario cuando este es extendido a $R[X_1, X_2, ..., X_n]$.

Proposición 15. *Sea Q un ideal P-primario de el anillo R. Entonces*

$$QR[X_1, X_2, ..., X_n]$$

es un ideal primario del anillo polinomial $R[X_1, X_2, ..., X_n]$ y el ideal primo que pertenece a $PR[X_1, X_2, ..., X_n]$.

Prueba. Es suficiente probar que $QR[X_1, X_2, ..., X_n]$ es un ideal primario, para entonces la otra afirmación se sigue inmediatamente de (2.6.23).
Ahora $QR[X_1, X_2, ..., X_n]$ es un ideal homogéneo propio.
De aquí se verifica que esta tiene la propiedad característica de un ideal primario que puede afirmar nuestra atención a elementos homogéneos. Sin embargo en este caso la verificación es trivial. ||

Proposición 16. *Sea A un ideal de R y supongamos que este tiene una descomposición primaria*

$$A = Q_1 \cap Q_2 \cap ... \cap Q_s \tag{2.6.24}$$

en R.
Entonces
$AR[X_1, ..., X_n]$

$$= Q_1R[X_1, ..., X_n] \cap Q_2R[X_1, ..., X_n] \cap ... \cap Q_sR[X_1, ..., X_n] \qquad (2.6.25)$$

es una descomposición primaria de $AR[X_1, X_2, ..., X_n]$ en $R[X_1, X_2, ..., X_n]$. Además, si (2.6.24) es una descomposición normal, entonces así tambíen es (2.6.25). Esto prueba que si $P_i(1 \leq i \leq t)$ son los ideales primos pertenecientes a A, entonces el $P_iR[X_1, X_2, ..., X_n]$, donde $1 \leq i \leq t$, son los ideales primos pertenecientes a $AR[X_1, X_2, ..., X_n]$.

Prueba. Supongamos que el ideal Q_i pertenece al ideal primo P_i. Entonces, por Propocición 15, $Q_iR[X_1, X_2, ..., X_n]$ es también primario y su radical es $P_iR[X_1, X_2, ..., X_n]$. Luego, la relación (2.6.25) sigue de (2.6.24) por virtud de (2.6.18). Estas dos observaciones establecen la primera afirmación.
Ahora asumamos que (2.6.24) es una descomposición normal.
Inmediatamente se sigue; de (2.6.17) que los ideales primos $P_iR[X_1, X_2, ..., X_n]$ son distintos. Además podemos tener

$$Q_iR[X_1, X_2, ..., X_n] \supseteq \bigcap_{j \neq i} Q_jR[X_1, X_2, ..., X_n]$$

porque, toma sobre intersecciónes con R, este produce $Q_i \supseteq \bigcap_{j \neq i} Q_j$ que es contrario a la suposición de (2.6.24) es una descomposición normal. ||

Proposición 17. *Sea R un anillo Noetheriano y P un ideal primo de R. Entonces $PR[X_1, X_2, ..., X_n]$ es un ideal primo del anillo polinomial*

$$R[X_1, X_2, ..., X_n]$$

y este tiene el mismo rango como P.

Prueba. Primero notemos que,

$$R[X_1, X_2, ..., X_n]$$

es un anillo Noetheriano y, por Proposición 13, $PR[X_1, X_2, ..., X_n]$ es un ideal primo. Sea *rank* $P = r$. Entonces existe una estricta sucesión decreciente

$$P \supset P_1 \supset P_2 \supset ... \supset P_r$$

de $r+1$ ideales primos del anillo R. Esto sigue, de la Proposición 13 y (2.6.17), que

$$PR[X_1, ..., X_n] \supset P_1R[X_1, ..., X_n] \supset ... \supset P_rR[X_1, ..., X_n]$$

es alguna sucesión descendente estricta de ideales primos. Entonces

$$rank(PR[X_1, ..., X_n]) \geq r.$$

Luego, existe r elementos $\alpha_1, \alpha_2, ..., \alpha_r$ tal que P es un ideal primo minimal de $(\alpha_1, \alpha_2, ..., \alpha_r)$. De aquí por Proposición 16, $PR[X_1, ..., X_n]$ es un ideal primo minimal de $(\alpha_1, \alpha_2, ..., \alpha_r)R[X_1, ..., X_n]$. Por tanto se sigue, que

$$rank(PR[X_1, X_2, ..., X_n]) \leq r.$$

Esto completa la prueba del teorema. $||$

Supongamos que R es un anillo (conmutativo y posee un elemento identidad) y $X_1, X_2, ..., X_n$ son indeterminados. Para $1 \leq i \leq n$ sea

$$R_i = R[X_1, X_2, ..., X_i]$$

y sea $R_0 = R$. Entonces,

$$R_{i+1} = R_i[X_{i+1}].$$

En otros términos, $R[X_1, X_2, ..., X_{i+1}]$ puede considerarse como el anillo de polinomios en X_{i+1} dado con coeficientes polinomiales en $X_1, X_2, ..., X_i$. Esta útil observación nos permite, en ocasión, a reducir un problema con respecto a polinomios en varias variables a el caso donde allí es solamente una sola variable. En vista de esto, probaremos tomando la oportunidad para hacer algúnas observaciones elementales con respecto a polinomios en una variable. La misma variable será denotada por X. Sea

$$f(X) = a_0 + a_1X + ... + a_mX^m$$

pertenece a $R[X]$. La máxima potencia de X que tiene un coeficiente no nulo es llamado el *grado de* $f(X)$.
Este grado es denotado por $\partial^0 f(X)$ o simplemente $\partial^0 f$. De esta manera si $a_m \neq 0$, entonces $\partial^0 f = m$.
En este caso a_m es llamado el *primer coeficiente* y a_mX^m los *primeros términos* de $f(X)$. Claramente si $f(X)$ y $g(X)$ ambos pertenecen a $R[X]$, entonces

$$\partial^0(f+g) \leq max(\partial^0 f, \partial^0 g) \tag{2.6.26}$$

y efectivamente es igual si sucede que $\partial^0 f \neq \partial^0 g$.
Sea $\partial^0 f(X) = m$ y $\partial^0 g(X) = n$.
Entonces $f(X) = a_0 + a_1X + a_2X^2 + ... + a_mX^m$ donde $a_m \neq 0$, y
$g(X) = b_0 + b_1X + b_2X^2 + ... + b_mX^m$ donde $b_n \neq 0$. Ahora

$$f(X)g(X) = (a_0b_0) + (a_0b_1 + a_1b_0)X + ... + (a_mb_n)X^{m+n}.$$

Desde luego puede suceder que $a_m b_n = 0$, pero en algún caso $\partial^0(fg) \leq m+n$, que es

$$\partial^0(fg) \leq \partial^0 f + \partial^0 g. \tag{2.6.27}$$

sin embargo $a_m b_n \neq 0$, entonces obtenemos

$$\partial^0(fg) = \partial^0 f + \partial^0 g, \tag{2.6.28}$$

en tal caso probaremos diciendo que *la fórmula de grado es dada por $f(X)$ y $g(X)$*. Es importante notar que la fórmula de grado cumple las siguientes condiciones:

1. Cada $f(X)$ o $g(X)$ tiene un primer coeficiente que no es un divisor de cero.

2. Cada $f(X)$ o $g(X)$ tiene un primer coeficiente que es una unidad.

3. El anillo R, de coeficientes, es un dominio integral.

Es uno respecto en que la discusión de arriba es incompleta. Puesto que el polinomio nulo o cero no tiene coeficiente no nulo, su grado no es definido. Sin embargo es conveniente asignar el polinomio nulo de grado convencional *menos infinito*. Si esto es hecho entonces (2.6.26), (2.6.27) y, las condiciónes apropiadas abajo (2.6.28) permanecen siendo válidas igual si el polinomio nulo es presentado, siempre, claro, que cierta convención natural respecto a el uso de cantidad infinita son observados. Aquí las condiciones son exactamente las mismas como en álgebra elementeal así no elaboraremos este punto.

Lema 15. *Sea $g(X)$ un polinomio no nulo (con coeficientes en R) del cual el primer coeficiente es unidad. Si ahora $f(X)$ pertenece a $R[X]$, entonces $f(X)$ tiene única representación en la forma*

$$f(X) = q(X)g(X) + r(X),$$

donde $q(X)$, $r(X)$ pertenece a $R[X]$ y $\partial^0 r(X) < \partial^0 g(X)$.

Prueba. Empezamos probando que una representación semejante es alguna posible. *Asumamos lo contrario.* Entonces existe un polinomio menor que puede ser expresado en la forma deseada. Entre tal polinomio seleccionamos uno, digamos $\phi(X)$, del cual el grado es posiblemente pequeño. Sea $\partial^0\phi = n$ y $\partial^0 g = m$. Entonces $n \geq m$ para distintos

$$\phi(X) = 0g(X) + \phi(X)$$

tendría que ser una representación de el tipo en cuestión.
Sea

$$g(X) = a_0X^m + ... + a_m \text{ y } \phi(X) = b_0X^n + ... + b_n.$$

Por hipótesis, a_0 es una unidad.
Podemos por tanto formar

$$\phi_1(X) = \phi(X) - a_0^{-1}b_0X^{n-m}g(X)$$

que es un polinomio tiene grado menor que $\phi(X)$. Por consiguiente existe $q_1(X)$ y $r_1(X)$ en $R[X]$ tal que

$$\partial^0 r_1(X) < \partial^0 g(X) \text{ y } \phi_1(X) = q_1(X)g(X) + r_1(X).$$

pero entonces

$$\phi(X) = \left\{q_1(X) + a_0^{-1}b_0X^{n-m}\right\} g(X) + r_1(X)$$

y ahora tenemos una contradicción porque es una representación de $\phi(X)$ de el tipo requerido. Será probado que algún elemento de $R[X]$ puede ser representado en la manera descrita y así sólo necesita ser probado que la representación es única. Supongamos por tanto que

$$q(X)g(X) + r(X) = q'(X)g(X) + r'(X)$$

donde $q(X),\ q'(X),\ r(X),\ r'(X)$ estan todos en $R[X]$ y

$$\partial^0 r(X) < \partial^0 g(X),\ \partial^0 r'(X) < \partial^0 g(X).$$

Deseamos probar que ambos $q(X) = q'(X)$ y $r(X) = r'(X)$. Sin embargo, una vez el primero se prueba, el segundo se sigue inmediatamente. Asumamos que $q(X) \neq q'(X)$.
Entonces $q(X) - q'(X)$ no es el polinomio nulo y

$$r'(X) - r(X) = \{q(X) - q'(X)\}\, g(X).$$

ahora el primer coeficiente de $g(X)$ es una unidad; de aquí que la fórmula de grado puede ser aplicado a el lado derecho. Esto produce

$$\partial^0 \{r'(X) - r(X)\} = \partial^0 \{q(X) - q'(X)\} + \partial^0 g(X) \geq \partial^0 g(X)$$

porque, puesto que $q(X) - q'(X)$ no es el polinomio nulo, su grado no es negativo. Sin embargo

$$\partial^0 \{r'(X) - r(X)\} \leq max\left\{\partial^0 r'(X), \partial^0 r(X)\right\} < \partial^0 g(X).$$

Esto da una contradicción y establece el lema. ||

Teorema 29. *Sea F un campo. Entonces cada ideal del anillo polinomial $F[X]$ puede ser generado por algún elemento.*

Prueba. Sea A un ideal de $F[X]$. Puesto que el ideal nulo es algún generador separado, asumimos que $A \neq (0)$. En lo que resulta suponemos que $\phi(X)$ es un polinomio no nulo que pertenece a A y, sujeto a esta condición, se asume tiene el grado más pequeño posible. Será probado que $A \subseteq (\phi)$.
Puesto que la inclusión opuesta es obvia, esto establece el teorema. ||

Supongamos que $f(X) \in A$. Por Lema 15, podemos expresar $f(X)$ en la forma

$$f(X) = q(X)\phi(X) + r(X),$$

donde $q(X)$ y $r(X)$ pertenece a $F[X]$ y $\partial^0 r(X) < \partial^0 \phi(X)$. Pero entonces $r(X) \in A$, de donde, por la seclección de $\phi(X)$, vemos que $r(X) = 0$. De esta manera $f(X)$ pertenece a (ϕ) y, como ya explica, el teorema resulta. ||

Corolario 19. *Sea F un campo. Entonces $F[X]$ no es un campo pero todo ideal primo no nulo es un ideal maximal.*

Prueba. Es claro que X no es una unidad en $F[X]$. Consecuentemente $F[X]$ no es un campo. Ahora supongamos que $P_1 \subset P_2$ (inclusión estricta), donde $P_1,\ P_2$ son ideales primos. Entonces, por el teorema, existe polinomios $\phi_1,\ \phi_2$ tal que $P_1 = (\phi_1)$ y $P_2 = (\phi_2)$. Puesto que ϕ_1 pertenece a P_2 tenemos
$\phi_1 = \phi_2\psi$ donde $\psi \in F[X]$.
Pero entonces $\phi_2\psi \in P_1$ y $\phi_2 \notin P_1$.
Por consiguiente $\psi \in P_1$, digamos $\psi = \phi_1\psi'$ donde $\psi' \in F[X]$.
De esta manera $\phi_1 = \phi_1\phi_2\psi'$. *Ahora afirma que* $\phi_1(0)$. Para distinto $1 = \phi_2\psi'$ de lo cual, porque la fórmula de grado tiene en $F[X],\ \phi_2$ es una constante no nula y de aquí una unidad. Sin embargo esto es imposible porque $P_2 = (\phi_2)$ es un ideal propio. De ello resulta que ϕ_1 es el polinomio nulo y por tanto $P_1 = (0)$. El corolario es de esta manera establecido.||

Teorema 30. *Sea R un anillo Noheteriano y $X_1, X_2, ..., X_n$ indeterminantes. Entonces*

$$Dim\ R[X_1, X_2, ..., X_n] = Dim\ R + n.$$

Prueba. Es suficiente probar el teorema para el caso $n = 1$. Por tanto asumimos que tenemos esta condición y, en orden simplifica la notación, denotaremos sólo la variable por X. Sea P un ideal primo de R.
Entonces, por Proposición 17,

$$rank\ (PR[X]) = rank\ P.$$

De ello resulta que $Dim\ R[X] \geq Dim\ R$ que establece el teorema en el caso donde $Dim\ R = \infty$. Donde ahora suponemos que $Dim\ R < \infty$. Existe un ideal maximal M de R que satisface $rank\ M = Dim\ R$ y es por tanto

$$rank(MR[X]) = Dim\ R.$$

Ahora $R/M = F$ (digamos) es un campo y, por (2.6.21), $R[X]/MR[X]$ es anillo-isomorfo a $F[X]$. Sin embargo, por el Teorema 29,
$F[X]$ no es un campo y por tanto $MR[X]$ no es un ideal maximal de $R[X]$.
De ello resulta que

$$Dim\ R[X] \geq Dim\ R + 1.$$

Luego, sea Π el ideal maximal de $R[X]$. Para completar la prueba es suficiente probar que $rank\ \Pi$ no es excedido $Dim\ R + 1$. Sea $P = \Pi \cap R$. Entonces P es un ideal primo de R y su complemento S, en R, es un conjunto multiplicativo cerrado no vacío. Ahora identificamos $R[X]_S$ con $R_S[X]$ por medio de (2.6.22). Entonces Π_S es un ideal maximal de $R_S[X]$, R_S es un anillo local, y $\Pi_S \cap R_S$ es el ideal maximal de R_S. Además Π_S y Π tienen el mismo rango mientras

$$Dim\ R_S = rank\ P \leq Dim\ R.$$

consecuentemente es suficiente probar que

$$rank\ \Pi_S \leq Dim\ R_S + 1.$$

esta conclusión puede volver a ser planteada de la siguiente forma: *cuando prueba que rank π es mayor que Dim $R + 1$, podemos asumir que (i) R es un anillo local y (ii) Π contracta a el ideal maximal de R.*
En lo que sigue suponemos que tenemos esta situación.
Sea M el ideal maximal de R, así que $\pi \cap R = M$, y sea $\alpha_1, \alpha_2, ..., \alpha_d$ un sistema de parámetros de R. Sabemos que el anillo $R[X]/MR[X]$ y $(R/M)[X]$ puede ser identificado y, por Teorema 29 cada ideal de $(R/M)[X]$, en particular el ideal $\Pi/MR[X]$, es alguno generado.
De esta manera existe $f \in R[X]$ tal que

$$MR[X] + fR[X] = \Pi.$$

Sea Π' un ideal primo arbitrario de $R[X]$ que contiene $\alpha_1, \alpha_2, ..., \alpha_d f$.
Entonces $\Pi' \cap R$ es un R-ideal primo contiene el sistema de parámetro $\alpha_1, \alpha_2, ..., \alpha_d$. Esto prueba que $\Pi' \cap R = M$ y por tanto Π' contiene

$$MR[X] + fR[X] = \Pi.$$

esto prueba que Π debe ser un ideal primo minimal de $(\alpha_1, \alpha_2, ..., \alpha_d, f)$.
Por lo tanto,

$$rank\ \Pi \leq d + 1 = Dim\ R + 1$$

la prueba de el teorema es ahora completa. ||

2.7. Anillos Polinomiales Semi-locales

Teorema 31. *Sea R un anillo semi-regular. Entonces el anillo polinomial $R[X_1, X_2, ..., X_n]$ es también semi-regular.*

Prueba. Es claro y suficiente probar el teorema para el caso en que hay sólo una variable. En lo que sigue asumamos que tenemos esta situación y denotaremos sólo la variable por X.
Obviamente $R[X]$ es un anillo Noetheriano no nulo.
Sea Π un ideal maximal de $R[X]$ si podemos demostrar que el anillo de fracciones de $R[X]$ con respecto a Π es semi-regular, entonces el resultado requerido se sigue por virtud de Teormea 25.
Sea $P = \Pi \cap R$ y denotemos el componente de P en R por S.
Entonces P es un R-ideal primo y S es un subconjunto (no vacío) multiplicativamente cerrado de $R[X]$. Además, $R[X]_\Pi$ y el anillo de fracciones de $R[X]_S$ con respecto a Π_S son isomorfos.
Consecuentemente es suficiente probar que el último es semi-regular.
Ahora usaremos (2.6.22) en orden para identificar $R[X]_S$ con $R_S[X]$.
Esto es comprensivo, Π_S es un ideal maximal de $R_S[X]$, R_S es un anillo local semi-regular, y Π_S contrae, en R_S a el ideal maximal de este anillo.
La observación de arriba prueba que, para el propósito de probar que $R[X]_\Pi$ es un anillo semi-regular, podemos ahora añadir la suposición que R es un anillo local (semi-regular) y que el ideal maximal Π de $R[X]$ contrae a el ideal maximal M (digamos) de R.
Esta suposición se hace en lo siguiente. Sea $\alpha_1, \alpha_2, ..., \alpha_d$ un sistema de parámetros de R. Por Teorema 24,

$$(\alpha_1, \alpha_2, ..., \alpha_i)R : \alpha_{i+1} = (\alpha_1, \alpha_2, ..., \alpha_i)R \text{ para } 0 \leq i < d.$$

de aquí, por (2.6.19),

$$(\alpha_1, \alpha_2, ..., \alpha_i)R[X] : \alpha_{i+1} = (\alpha_1, \alpha_2, ..., \alpha_i)R[X]$$

así que $\alpha_1, \alpha_2, ..., \alpha_d$ es también una $R[X]$-sucesión. Note que, puesto que M es sólo ideal primo perteneciente a $(\alpha_1.\alpha_2, ..., \alpha_d)R$, $MR[X]$ es sólo ideal primo perteneciente a $(\alpha_1, \alpha_2, ..., \alpha_d)R[X]$.
Aquí tenemos que hacer uso de Proposición 16.
Luego, $\Pi/MR[X]$ es un ideal maximal de el anillo $R[X]/MR[X]$ y este anillo puede ser identificado con $(R/M)[X]$ por virtud de (2.6.21).
Además R/M es un campo; consecuentemente $\Pi/MR[X]$ es un ideal principal no nulo.
De esta manera existe $f \in R[X]$ tal que

$$f \notin MR[X] \text{ y } MR[X] + fR[X] = \Pi.$$

Esto prueba que. Π es un ideal primo minimal de $(\alpha_1, ..., \alpha_d, f)$, mientras tanto de $f \notin MR[X]$ concluimos que

$$(\alpha_1, ..., \alpha_d)R[X] : f = (\alpha_1, ..., \alpha_d)R[X].$$

por consiguiente $\alpha_1, ..., \alpha_d, f$ es una $R[X]$-sucesión y $rank\ \Pi = d + 1$. Ahora estamos listos para pasar a el anillo $R[X]_\Pi$. Sea $\alpha_1^*, ..., \alpha_d^*, f^*$ las imágenes de $\alpha_1, ..., \alpha_d, f$ bajo el mapeo canónico

$$R[X] \rightarrow R[X]_\Pi$$

observamos, en primer lugar, que $R[X]_\Pi$ es un anillo local de dimensión $d+1$. Luego, la extensión de

$$(\alpha_1, ..., \alpha_d, f)R[X] \text{ en } R[X]_\Pi$$

es generado por $\alpha_1^*, ..., \alpha_d^*, f^*$. Prueba que sólo el ideal primo perteneciente a esta extensión es el ideal maximal de $R[X]_\Pi$.
De esta manera $\alpha_1^*, ..., \alpha_d^*, f^*$ es un sistema de parámetros en $R[X]_\Pi$.
Finalmente, tenemos

$$(\alpha_1^*, ..., \alpha_i^*)R[X]_\Pi : \alpha_{i+1}^* = (\alpha_1^*, ..., \alpha_i^*)R[X]_\Pi$$

para $0 \leq i \leq d$, y

$$(\alpha_1^*, ..., \alpha_d^*)R[X]_\Pi : f^* = (\alpha_1^*, ..., \alpha_d^*)R[X]_\Pi$$

Por consiguiente el sistema de parámetros $\alpha_1^*, ..., \alpha_d^*, f^*$ es sólo una $R[X]_\Pi$-sucesión.
Ahora se sigue, de Teorema 24, que $R[X]_\Pi$ es un anillo local semi-regular y que esto completa la prueba. ||

Teorema 32. *Sea F un campo. Entonces el anillo polinomial $F[X_1, X_2, ..., X_n]$ es semi-regular y su dimensión es n.*

Prueba. Puesto que un campo es obviamente cero-dimensional y semi-regular, el Teorema 32 es una consecuencia inmediata del Teorema 30 y 31

Capítulo 3

Teoría de Multiplicidad

3.1. Consideraciones preliminares

Sea R un anillo con un elemento identidad. En lo que resulta, el término R-módulo será siempre un R-módulo izquierdo.
Si un R-módulo E satisface la condición maximal para submódulos, entonces E será llamado un R-módulo Noetheriano.
Esto es en conformidad con la definición ya introducida en conexión con anillos conmutativos.
Hay ciertos términos y ciertas construcciones, ya empleadas en el caso conmutativo, que debe ser adaptado a nuestro presente propósito. Sea E un R-módulo y B un ideal izquierdo.
Denotemos por BE el submódulo de E que consiste de todo elemento que puede ser expresado en la forma $b_1e_1 + b_2e_2 + ... + b_se_s$, donde $b_i \in B$ y $e_i \in E$. Si ahora A es un ideal izquierdo, entonces, se verifica fácilmente que, $(AB)E = A(BE)$. Podemos por tanto omitir los corchetes y escribir ABE para el módulo.
Notese que se hace significado a decir de la m-potencia A^m de A.
Más general, si $A_1, A_2, ..., A_m$ son ideales izquierdos, entonces el producto extensión $A_1A_2...A_m$ es bien definido y así también un ideal izquierdo.

Definición 32. *Un elemento γ de R es llamado un "elemento central" si $\gamma r = r\gamma$ para todo r en R.*

Por ejemplo, ambos 0_R o 1_R son elemetos centrales. Una simple verificación prueba que el elemento central de R forma un anillo. Este anillo es llamado el *centro* de R, y tiene el mismo elemento identidad como R mismo.
Sea G un conjunto de elementos centrales de R. Entonces el ideal izquierdo generado por por G coincide con el ideal derecho generado por el mismo conjunto.

De aquí que el total de elementos que puede ser expresado en la forma

$$r_1\gamma_1 + r_2\gamma_2 + ... + r_s\gamma_s,$$

donde $r_i \in R$ y $\gamma_i \in G$ es un ideal en ambos lados.
Podemos por ello decir que el ideal generado por un conjunto de elementos centrales sin especificar si este es un ideal izquierdo, un ideal derecho o un ideal en ambos lados como tenemos en mente.

Definición 33. *Un ideal que puede ser generado por un conjunto de elementos centrales será llamado un "ideal central".*

La observación de arriba establece que los ideales centrales son de ambos lados. Sea G y G' conjuntos de elementos centrales y A y A' los ideales centrales que ellos generan.
Entonces $A + A'$ es generado por $G \cup G'$ mientras que AA' es generado por el conjunto de todo producto $\gamma\gamma'$, donde γ pertenece a G y γ' a G'.
De quí la suma y el producto de dos ideales centrales son nuevamente ideales centrales.
Ademaś el conjunto de productos $\gamma\gamma'$ coincide con el correspondiente conjunto obtenido por intercambiar los roles de G y G'.
De aquí $AA' = A'A$ y por ello, en un producto de ideales centrales, el orden de los factores puede ser cambiado en algún camino y este no cambia el valor de el producto.
Supongamos ahora que A es un ideal central dado. Entonces A es un ideal en ambos lados. Nos permite asumir que, como un ideal en ambos lados, es finitamente generado.
Por esto existe un conjunto finito $u_1, u_2, ..., u_s$ de elementos de R tal que A es el ideal más pequeño en ambos lados que los contiene.
En estas circunstancias cada u_i puede ser expresado en la forma

$$u_i = r_{i1}\gamma_{i1} + r_{i2}\gamma_{i2} + ... + r_{in_i}\gamma_{in_i}$$

$(1 \leq i \leq s), donde \gamma_{ij}$ denota el elemento central contenido en A y r_{ij} pertenece a R. Es claro que el ideal central generado por la variable γ_{ij} es A mismo. De aquí A *puede ser generado por un número finito de elementos centrales*
En este camino vemos que la expresión *ideal central finitamente generado* puede ser usada sin esencial ambiguedad.
En el caso de un conjunto finito $\gamma_1, \gamma_2, ..., \gamma_p$ de elementos centrales, podemos en algun momento usar $(\gamma_1, \gamma_2, ..., \gamma_p)$ para denotar el ideal central que genera.
Si ahora $\gamma_1^{'}, \gamma_2^{'}, ..., \gamma_q^{'}$ son también elementos centrales, entonces

$$(\gamma_1, \gamma_2, ..., \gamma_p) + (\gamma_1^{'}, \gamma_2^{'}, ..., \gamma_q^{'}) = (\gamma_1, , ..., \gamma_p, \gamma_1^{'}, ..., \gamma_q^{'})$$

y

$$(\gamma_1, \gamma_2, ..., \gamma_p)(\gamma_1^{'}, \gamma_2^{'}, ..., \gamma_q^{'}) = (\gamma_1\gamma_1^{'}, ..., \gamma_i\gamma_j^{'}, ..., \gamma_p\gamma_q^{'}).$$

se sigue, de la segunda relación, que si $A = (\gamma_1, \gamma_2, ..., \gamma_p)$, entonces A^m es generado por la colección de productos $\gamma_1^{n_1} + \gamma_2^{n_2} + ... + \gamma_p^{n_p}$, donde $n_1, n_2, ..., n_p$ son enteros no negativos que satisfacen $n_1 + n_2 + ... + n_p = m$.
Sea E un R-módulo y $\gamma_1, \gamma_2, ..., \gamma_p$ elementos centrales.
Entonces $(\gamma_1, \gamma_2, ..., \gamma_p)E$ consiste de todo elemento central que puede ser expresado en la forma $\gamma_1 e_1, \gamma_2 e_2, ..., \gamma_p e_p$, donde $e_1, e_2, ..., e_p$ pertenecen a E. Por esta razón a menudo usaremos $\gamma_1 E, \gamma_2 E, ..., \gamma_s E$ como una alternativa para $(\gamma_1, \gamma_2, ..., \gamma_p)E$.
En particular γE es usado en lugar de $(\gamma)E$. Supongamos que tenemos un *epimorfismo* de un anillo R sobre un anillo R'. Es claro que todo elemento central de R es transferido en un elemento central de R'. Por ejemplo, si A es un ideal en ambos lados de R y γ pertenece al centro de R, entonces la imagen natural de γ en el residuo del anillo R/A es un elemento central de ese anillo. Completemos esta sección por algúna relación simple conectada con elementos centrales, submódulos y factor módulo.
Sea $K \subseteq L$ submódulos de un R-módulo E y sea γ, γ' elementos centrales.
El mapeo $E \to E$ en que $e \to e\gamma$ es un endomorfismo de R-módulos. La imagen inversa de K con respecto a este mapeo es denotada por $K :_E \gamma$ así que un elemento e, de E, pertenece a $K :_E \gamma$ si y sólo si $\gamma e \in K$. (Más general, si A es un subconjunto de R, entonces $K :_E A$ denota el conjunto de todos los elementos $e \in E$ tal que $ae \in K$ para todo $a \in A$. Este es un submódulo de E si A pasa a ser un ideal en ambos lados) Evidentemente

$$(K :_E \gamma) :_E \gamma' = K :_E \gamma\gamma' \tag{3.1.1}$$

y, como fácilmente se verifica,

$$\gamma E \cap K = \gamma(K :_E \gamma) \tag{3.1.2}$$

ahora consideraremos el mapeo natural $\phi : E \to E/K$. Puesto que $K + \gamma E$ es mapeo sobre $\gamma(E/K)$, tenemos un isomorfismo

$$E/(K + \gamma E) \approx (E/K)/\gamma(E/K) \tag{3.1.3}$$

también si e pertenece a E, entonces $\phi(e)$ pertenece a $(L/E) :_{E/K} \gamma$
sí y sólo sí e esta en $L :_E \gamma$. De ello resulta que

$$(L :_E \gamma)/K = (L/K) :_{E/K} \gamma \tag{3.1.4}$$

un útil caso especial de esta relación es obtenido por presentar $L = K$.
Esto produce

$$(K :_E \gamma)/K = 0 :_{E/K} \gamma \tag{3.1.5}$$

3.2. Teoremas claves sobre ideales centrales

En esta sección estableceremos algunos resultados básicos que conciernen a ideales centrales y módulos Noetherianos.
El primero de estos es una generalización de el Teorema Artin-Rees.

Teorema 33. *Sea K un submódulo de un R-módulo Noetheriano E y sea A un ideal central. Entonces existe un entero $q \geq 0$ tal que*

$$A^nE \cap K = A^{n-q}(A^qE \cap K) \text{ para todo } n \geq q$$

Prueba. Sea A_0 un ideal de R que puede ser generado por un número *finito* de elementos centrales en A. Entonces $A_0 \subseteq A$ y A_0E es un submódulo de E. Puesto que E es un R-módulo Noetheriano, podemos escojer un A_0 tal que A_0E es un miembro maximal de la familia de todos los submódulos que pueden ser obtenidos en este camino. Ahora supongamos que γ es un elemento central arbitrario contenido en A.
Entonces

$$\gamma E \subseteq (A_0 + R\gamma)E = A_0E$$

y por ello $AE = A_0E$. De ello resulta que

$$A^2E = AA_0E = A_0AE = A_0^2E$$

de donde

$$A^3E = AA_0^2E = A_0^2AE = A_0^3E$$

procediendo en este camino encontraremos que $A^nE = A_0^nE$, para todo $n \geq 0$. Asumamos que existe un entero $q \geq 0$ tal que

$$A_0^nE \cap K = A_0^{n-q}(A_0^qE \cap K),$$

para todo $n \geq q$. Entonces, cuando $n \geq q$,

$$A^nE \cap K = A_0^nE \cap K = A_0^{n-q}(A_0^qE \cap K) \subseteq A^{n-q}(A^qE \cap K)$$

que implica que $A^nE \cap K = A^{n-q}(A^qE \cap K)$. De esta manera para el propósito de la prueba podemos asumir que A es *finitamente generado*. Por lo tanto A es finitamente generado. Finalmente, en selección un conjunto finito $\gamma_1, \gamma_2, ..., \gamma_s$ de elementos para generar A, es necesario ordenar que cada γ_i es un elemento central de R. ||

El siguiente resultado corresponde a el Teorema Intersección de Krull. Cuando encontramos este resultado antes, la prueba dada puede usarse de la teoría de descomposición primaria y este no es válido para nuestras presentes circunstancias. Sin embargo, podemos obtener aproximadamente esta dificultad con la ayuda del Teorema 33.

Teorema 34. *Sea E un R-módulo Noetheriano y A un ideal central. Entonces un elemento e, de E, pertence a $\cap_{n=1}^{\infty} A^n E$ si y sólo si $e = \alpha e$ para algún elemento α perteneciente a A.*

Prueba. Si $e = \alpha e$, donde $\alpha \in A$, entonces $e = \alpha^n e$ para todo n y por ello e pertenece a la intersección. Ahora asumamos que e está en $\cap_{n=1}^{\infty} A^n E$. Por Teorema 33, existe un entero $q \geq 0$ tal que

$$A^n E \cap Re = A^{n-q}(A^q E \cap Re)$$

para todo $n \geq q$. Tomamos $n = q + 1$ encontramos que $Re = A(Re)$. Por consiguiente $e \in A(Re)$ y por ello $e = \alpha e$ para algún $\alpha \in A$. Esto completa la prueba. || Por otra parte la dificultad es que, para anillos no comutativos,

el concepto del radical de Jacobson presenta problemas que no se encuentran en el caso conmutativo. En hecho, define el radical de Jacobson de un anillo general R como la intersección de todos sus ideales izquierdos maximales. Aquí serán llamados el radical izquierdo de Jacobson y que, por la analogía, debe ser un segundo radical de Jacobson para ser distinguido por el adjetivo "derecho". Sin embargo, la intersección de todos los ideales maximales izquierdos siempre coincide con la intersección de todos los ideales maximales derechos.

Por esta razón, el propósito de distinción se vuelve innecesario muy rápidamente. Antes de proceder, notemos que *todo ideal propio izquierdo de R es contenido en un ideal maximal izquierdo.*

En efecto si I es un ideal izquierdo diferente de R mismo, entonces el conjunto Ω de ideales propios izquierdos contenidos en I forman un sistema inductivo no vacío donde sus miembros son de orden parcial por la relación de inclusión. El lema de Zorn's prueba que existe un miembro maximal, digamos L, de Ω. Claramente L es un ideal maximal izquierdo de R e I es contenido en L.

Proposición 18. *Si x pertencece al radical de Jacobson J, de R, entonces $1 + x$ tiene un inverso en ambos lados.*

Prueba. Tenemos que probar que existe un elemento, ρ de R, tal que

$$\rho(1 + x) = (1 + x)\rho = 1.$$

claramente $1 + x$ no esta contenido en algún ideal maximal izquierdo así el mismo es verdadero para $R(1 + x)$. Se deriva que $R(1 + x) = R$ y por ello $\rho(1 + x) = 1$ para un elemento conveniente ρ de R. Luego

$$\rho = 1 - \rho x = 1 + x'$$

Aquí $x' = -\rho x$ pertenece a J por que J es desde luego un ideal izquierdo. Repitiendo el argumento ahora vemos que existe un elemento ρ' tal que $\rho^{'}(1+x') = 1$, i.e. $\rho'\rho = 1$. Finalmente

$$\rho' = \rho'(\rho(1+x)) = (\rho'\rho)(1+x) = 1+x$$

y por ello $(1+x)\rho = \rho'\rho = 1$. Esto completa la prueba. $||$

Lema 16. *Si $x \in J$, donde J es el radical de Jacobson de R, y sea r un elemento arbitrario del anillo. Entonces $xr \in J$.*

Prueba. Sea L un ideal maximal izquierdo. El lema resultará si probamos que xr pertencece a L. Asumamos lo contrario. Entonces $Rxr + L$ es un ideal izquierdo que contiene estrictamente a L. Aquí $Rxr = L = R$ y por ello

$$\rho xr + \lambda = 1$$

para elementos convenientes $\rho \in R$ y $\lambda \in L$. Sea $y = \rho x$. Entonces $y \in J$ y $1 - yr = \lambda$. Ahora

$$(1-ry)r = r(1-yr) = r\lambda$$

y, por Proposición 18, $1 - ry$ tiene un inverso en ambos lados.
Si multiplicamos en ambos lados la ecuacion $(1-ry)r = r\lambda$ sobre el izquierdo por este inverso, entonces se ve que $r \in L$.
Por consiguiente $1 = \lambda + yr$ pertenece a L y ahora tenemos una contradicción porque L es un ideal propio. $||$

Teorema 35. *La intersección de todos los ideales maximales izquierdos de R coincide con la intersección de todos sus ideales maximales derechos.*

Prueba. Probaremos que la intersección, digamos J, de todos los ideales maximales izquierdos es contenida en la intersección de todos los ideales maximales derechos. El teorema resultara por simetría.
Si x pertenece a J y sea Q un ideal maximal arbitrario derecho. Es ahora suficiente probar que x pertenece a Q. Asumamos que $x \notin Q$.
Entonces $Q + xR = R$ y por ello $1 = q + xr$ para elementos convenientes $q \in Q$ y $r \in R$. Por Lema 16, $xr \in J$ y así, por Proposición 18, $1 - xr = q$ tenemos un inverso en ambos lados digamos q^{-1}.
Pero entonces $qq^{-1} = 1$ pertenece al ideal izquierdo Q y ahora tenemos la contradiccción porque Q es un ideal propio. Esto completa la prueba.$||$

Teorema 36. *Sea E un R-módoulo Noetheriano y A un ideal central contenido en el radical de Jacobson J de R. Entonces $\bigcap_{n=1}^{\infty} A^n E = 0$.*

Prueba. Si e pertenece a $\bigcap A^n E$. Entonces, por Teorema 34, tenemos $e = \alpha e$ para algún elemento α que pertenece a A y por ello también a J. De esta manera $(1-\alpha)e$=0 y, por Proposición 18, $1-\alpha$ tenemos un inverso en ambos lados. Si multiplicamos la relación $(1-\alpha)e = 0$ por este inverso, vemos que $e = 0$. Esto completa la prueba. ||

3.3. Sistemas de multiplicidad

Sea E un R-módulo y sea $\gamma_1, \gamma_2, ..., \gamma_s$ $(s \geq 0)$ elemento central de R. Lo que haremos es definir, bajo seguras condiciones, el sistema de multiplicidad $\gamma_1, \gamma_2, ..., \gamma_s$ sobre (o en relación a) el módulo E. En orden tiene un conciso camino de referencia a esta condición, tenemos la siguiente defінción.

Definición 34. *El elemento central* $\gamma_1, \gamma_2, ..., \gamma_s$ $(s \geq 0)$ *se dice forma un "sistema de multiplicidad" sobre* E*, si el R-módulo* $E/(\gamma_1 E, \gamma_2 E, ..., \gamma_s E)$ *tiene longitud finita. Donde* $s = 0$ *esta condición es sobreentendida como significado que* $L_R(E)$ *es finito.*

Antes procedemos a enumerar las propiedades básicas de un sistema de multiplicidad, estableciendo una desigualdad elemental concerniente a lo largo de módulos que es prueba útil en algunas ocasiónes.
La desigualdad es debido a D.J. Wright.

Proposición 19. *Sea* E *un R-módulo y* $\gamma_1, \gamma_2, ..., \gamma_s$ *elementos centrales de* R*.*

Entonces $L_R\left\{E/(\gamma_1^{n_1}E + \gamma_2^{n_2}E + ..., +\gamma_s^{n_s}E)\right\} \leq n_1 n_2 ... n_s L_R(E/(\gamma_1 E{+}\gamma_2 E{+}...{+}\gamma_s E))$

para enteros positivos arbitrarios $n_1, n_2, ..., n_s$

Observación 5. *En este resultado no es necesario para longitudes que tienden a ser finitas.*

Prueba. Es claro y suficiente probar que

$$L_R\left\{E/(\gamma_1^{n_1}E + \gamma_2 E + ... + \gamma_s E)\right\} \leq n_1 L_R(E/(\gamma_1 E + \gamma_2 E + ... + \gamma_s E))$$

para algunas veces será establecido el resutado más general repitiendo las aplicaciónes de el caso especial. Si $E' = E/(\gamma_2 E + ... + \gamma_s E)$.
Entonces, por (3.1.3), tenemos un isomorfismo

$$E'/\gamma_1^{n_1}E' \approx E/(\gamma_1^{n_1}E + \gamma_2 E + ... + \gamma_s E)$$

por consiguiente

$$L_R\left\{E'/\gamma_1^{n_1}E'\right\} = L_R\left\{E/(\gamma_2^{n_2}E, ..., \gamma_s^{n_s}E)\right\}$$

y así lo que se probará puede ser escrito como

$$L_R\left\{E'/\gamma_1^{n_1}E'\right\} \leq n_1 L_R\left\{E'/\gamma_1 E'\right\}.$$

Esta conclusión puede igual bien ser descrita diciendo que necesitamos solo considerar en caso en que $s = 1$. Sea $\gamma = \gamma_1$ y $n = n_1$.
Tenemos que probar $L_R(E/\gamma^n E)$ no excede $nL_R(E/\gamma E)$. Pero

$$L_R(E/\gamma^n E) = \sum_{i=1}^{n} L_R(\gamma^{i-1}E/\gamma^i E)$$

así es solamente necesario probar que

$$L_R(\gamma^{i-1}E/\gamma^i E) \leq L_R(E/\gamma E).$$

luego, la multiplicación por γ^{i-1} produce un epimorfismo $E \to \gamma^{i-1}E$. La imagen inversa de $\gamma^i E$ con respecto a este mapeo es $(0 :_E \gamma^{i-1}) + \gamma E$.
Así tenemos un isomorfismo

$$\gamma^{i-1}E/\gamma^i E \approx E/(0 :_E \gamma^{i-1} + \gamma E)$$

y por ello

$$L_R\left\{\gamma^{i-1}E/\gamma^i E\right\} = L_R\left\{E/(0 :_E \gamma^{i-1} + \gamma E)\right\} \leq L_R\left\{E/\gamma E\right\}$$

esto completa la prueba.||

Sea $\gamma_1, \gamma_2, ..., \gamma_s$ un sistema de multiplicidad sobre E. Haremos un número de observaciones simples.

(a) Los elementos $\gamma_1, \gamma_2, ..., \gamma_s$ permanecen en un sistema de multiplicidad sobre E si cambiamos su orden en alguna manera. También continua formando un sistema de multiplicidad sobre E si suprimimos algún γ_i para que $\gamma_i E = 0$

(b) Para enteros positivos arbitrarios $n_1, n_2, ..., n_s$ los elementos centrales $\gamma_1^{n_1}, \gamma_2^{n_2}, ..., \gamma_s^{n_s}$ también forman un sistema de multiplicidad sobre E. Al ver esto sólo podemos observar que, por la proposición 19,

$$L_R\left\{E/(\gamma_1^{n_1}E + ... + \gamma_s^{n_s}E)\right\} \leq n_1 n_2 ... n_s L_R\left\{E/(\gamma_1 E + \gamma_2 E + ... + \gamma_s E)\right\}$$

puesto que la segunda expresión es finita, se establece (b).

(c) Si E' es un módulo factor de E, entonces $\gamma_1, \gamma_2, ..., \gamma_s$ es un sistema de multiplicidad sobre E'.

Podemos probar esto como sigue. Sea $E' = E/K$. Entonces

$$\gamma_1 E' + \gamma_2 E' + ... + \gamma_s E'$$

es justemente $(K + \gamma_1 E + ... + \gamma_s E)/K$ y así tenemos un isomorfismo

$$E'/(\gamma_1 E' + \gamma_2 E' + ... + \gamma_s E') \approx E/(K + \gamma_1 E + ... + \gamma_s E)$$

de ello resulta que

$$L_R \{E'/(\gamma_1 E' + ... + \gamma_s E')\} = L_R \{E/(K + \gamma_1 E + ... + \gamma_s E)\} \leq L_R \{E/(\gamma_1 E + ... + \gamma_s E)\}$$

y este es finito. Así (c) es demostrado. Esto no será verdadero, sin sumar una condición extra, los $\gamma_1, \gamma_2, ..., \gamma_s$ son necesariamente un sistems de multiplicidad sobre todo submódulo de E. Sin embargo tenemos el siguiente resultado.

Lema 17. *Sea $0 \to E' \to E \to E'' \to 0$ una sucesión exacta de R-módulos y sea $\gamma_1, \gamma_2, ..., \gamma_s$ elementos centrales. Entonces*

$$L_R \{E/(\gamma_1 E + ... + \gamma_s E)\} \leq L_R \{E'/(\gamma_1 E' + ... + \gamma_s E')\} + L_R \{E''/(\gamma_1 E'' + ... + \gamma_s E'')\}$$

Puesto que si $\gamma_1, \gamma_2, ..., \gamma_s$ es un sistema de multiplicidad sobre ambos E' y E'', entonces son también un sistema de multiplicidad sobre E.

Prueba. Sin pérdida de generalidad podemos suponer que E' es un submódulo de E y $E'' = E/E'$. Entonces

$$\gamma_1 E'' + \gamma_2 E'' + ... + \gamma_s E'' = (E' + \gamma_1 E + ... + \gamma_s E)/E'$$

y por ello

$$L_R \{E''/(\gamma_1 E'' + ... + \gamma_s E'')\} = L_R \{E/(E' + \gamma_1 E + ... + \gamma_s E)\}$$

porque los módulos que ocurren en esta ecuación son isomorfismos.

$$\begin{aligned} &L_R \{E/(\gamma_1 E + ... + \gamma_s E)\} \\ &\qquad = L_R \{E/(E' + \gamma_1 E + ... + \gamma_s E)\} \\ &\qquad\qquad\qquad + L_R \{(E' + \gamma_1 E + ... + \gamma_s E)/(\gamma_1 E + ... + \gamma_s E)\} \\ &\qquad = L_R \{E''/(\gamma_1 E'' + ... + \gamma_s E'')\} + L_R \{E'/(E' \cap (\gamma_1 E + ... + \gamma_s E))\} \end{aligned}$$

De aquí tenemos que hacer uso del isomorfismo

$$(E' + \gamma_1 E + ... + \gamma_s E)/(\gamma_1 E + ... + \gamma_s E) \approx E'/(E' \cap (\gamma_1 E + ... + \gamma_s E))$$

Nuevamente

$$\gamma_1 E' + \gamma_2 E' + ... + \gamma_s E' \subseteq E' \cap (\gamma_1 E + ... + \gamma_s E) \subseteq E' \text{ y así}$$

$$L_R \{E'/(E' \cap (\gamma_1 E + ... + \gamma_s E))\} \leq L_R \{E'/(\gamma_1 E' + ... + \gamma_s E')\}$$

y el lema se establece ||

Proposición 20. *Sea $0 \to E' \to E \to E''$ una sucesión exacta de un R-módulo Noetheriano y sea $\gamma_1, \gamma_2, ..., \gamma_s$ elementos centrales.*
Entonces $\gamma_1, \gamma_2, ..., \gamma_s$ es un sistema de multiplicidad sobre E sí y sólo sí es un sistema multiplicativo sobre ambos E' y E''

Prueba. Asumamos que $\gamma_1, \gamma_2, ..., \gamma_s$ es un sistema de multiplicidad sobre E y deduce que es también un sistema de multiplicidad sobre E'.
Es suficiente porque todas las otras afirmaciones contenidas en la condiciones de la proposición ya están establecidas.
Sin pérdida de generalidad podemos asumir que E' es un submódulo de E. Sea $A = \gamma_1 R, \gamma_2 R, ..., \gamma_s R$. Entonces, por Teorema 33, existe un entero no negativo q tal que

$$A^{q+1} E \cap E' = A(A^q E \cap E') \subseteq AE'.$$

por consiguiente

$$\begin{aligned} L_R \{E'/(\gamma_1 E' + ... + \gamma_s E')\} \qquad &= L_R \{E'/AE'\} \\ &\leq \left\{E'/(A^{q+1} E \cap E')\right\} \\ &= L_R \left\{(A^{q+1} E + E')/A^{q+1} E\right\} \\ &\leq L_R \left\{E/A^{q+1} E\right\} \end{aligned}$$

porque, el módulo $E'/(A^{q+1} E \cap E')$ y $(A^{q+1} E + E')/A^{q+1} E$ son isomorfismos.
Ahora

$$\gamma_1^{q+1} E + \gamma_2^{q+1} E + ... + \gamma_s^{q+1} E$$

está contenido en $A^{q+1} E$. Por consiguiente

$$\begin{aligned} L_R \{E'/(\gamma_1 E' + ... + \gamma_s E')\} \qquad &\leq L_R \left\{E/(\gamma_1^{q+1} E + ... + \gamma_s^{q+1} E)\right\} \\ &\leq (q+1)^s L_R \{E'/(\gamma_1 E + ... + \gamma_s E)\} \\ &< \infty \end{aligned}$$

por virtud de Proposición 19. Prueba que $\gamma_1, \gamma_2, ..., \gamma_s$ es un sistema de multiplicidad sobre E'. ||

Concluimos esta sección con una observación con respecto a el comportamiento de sistemas de multiplicidad del anillo de operación.

Sea $\gamma_1, \gamma_2, ..., \gamma_s$ un sistema de multiplicidad sobre un R-módulo E y sea I un ideal en ambos lados tal que $IE = 0$. Sea $\bar{R} = R/I$.
Entonces, E tiene una estructura bien definida como un $\bar{R}$-módulo. Denota la imagen natural de γ_i en $\bar{R}$ por $\bar{\gamma}_i$.
Entonces $\bar{\gamma}_i$ es un elemento central de $\bar{R}$ y

$$E/(\gamma_1 E + \gamma_2 E + ... + \gamma_s E) = E/(\bar{\gamma_1} E + \bar{\gamma_2} E + ... + \bar{\gamma}_s E)$$

porque $\gamma_i E = \bar{\gamma}_i E$. Lo que tenemos aquí son ambos sus R-módulos y sus $\bar{R}$-submódulos coincide. Por consiguiente

$$L_{\bar{R}} \{E/(\bar{\gamma}_1 E + ... + \bar{\gamma}_s E)\} = L_R \{E/(\gamma_1 E + ... + \gamma_s E)\} < \infty$$

de aquí que $\bar{\gamma}_1, \bar{\gamma}_2, ..., \bar{\gamma}_s$ es un sistema de multiplicidad sobre E, cuando E es considerado como un $\bar{R}$-módulo.

3.4. El símbolo de multiplicidad

Sea E un R-módulo Noetheriano y $\gamma_1, \gamma_2, ..., \gamma_s$ un sistema de multiplicidad sobre E. Ahora definimos la multiplicidad de $\gamma_1, \gamma_2, ..., \gamma_s$ sobre (o con respecto a) E. Esta multiplicidad vuelve a ser un entero no negativo y usamos el símbolo $e_R(\gamma_1, \gamma_2, ..., \gamma_s|E)$ para denotarlo. La definición de el símbolo de multiplicidad usa inducción sobre s. Primero supongamos que $s = 0$.
En este caso el conjunto vacío es un sistema de multiplicidad sobre E y por ello, por nuestra convención, $L_R(E)$ es finito. Podemos por ello poner

$$e_R(.|E) = L_R(E) \tag{3.4.6}$$

ahora supongamos que $s \geq 1$ y que el símbolo de multiplicidad será definido por módulos Noetherianos y sistemas de multiplicidad con sólo $s-1$ elementos. El factor módulo $E|\gamma_1 E$ y el submódulo $0 :_E \gamma_1$ son Noetherianos.
Luego, $\gamma_1, \gamma_2, ..., \gamma_s$ es un sistema de multiplicidad sobre E, los γ_i también forman un sistema de multiplicidad sobre los dos módulos derivados de esto. Pero γ_1 aniquila $E|\gamma_1 E$. De aquí si removemos γ_1 los elementos restantes aún forman un sistema de multiplicidad sobre este módulo. De esta manera $\gamma_2, \gamma_3, ..., \gamma_s$ es un sistema de multiplicidad sobre $E/\gamma_1 E$ y una consideración similar prueba que $\gamma_2.\gamma_3, ..., \gamma_s$ es un sistema de multiplicidad sobre $0 :_E \gamma_1$.
Por consiguiente, por virtud de nuestra suposición, $e_R(\gamma_2, \gamma_3, ..., \gamma_s|E/\gamma_1 E)$ y $e_R(\gamma_2, \gamma_3, ..., \gamma_s|0 :_E \gamma_1)$ son ambos definidos y así podemos escribir

$$e_R(\gamma_1, \gamma_2, ..., \gamma_s|E) = e_R(\gamma_2, \gamma_3, ..., \gamma_s|E/\gamma_1 E) - e_R(\gamma_2, \gamma_3, ..., \gamma_s|0 :_E \gamma_1) \tag{3.4.7}$$

el símbolo de multiplicidad general es ahora completamente determinado por medio de (3.4.6) y (3.4.7). Es claro que $e_R(\gamma_1, ..., \gamma_s)|E$ es un entero aunque no tenemos fundamentos, aún como para decir que es no negativo. Es obvio, también, que el valor de símbolo de multiplicidad no es cambiado si reemplazamos E por algún módulo que es isomorfo a este.
Además $e_R(\gamma_1, ..., \gamma_s|E)$ tiene el valor de cero cuando E es un módulo nulo. Notemos alguna otra propiedad fundamental.
Supongamos que E es un R-módulo Noetheriano y $\gamma_1, \gamma_2, ..., \gamma_s$ es un sistema de multiplicidad sobre E. También que I es un ideal en ambos lados y que $IE = 0$.
Sea $\bar{R} = R/I$ y $\bar{\gamma}_i$ denota la imagen natural de γ_i en $\bar{R}$. Entonces E es un $\bar{R}$-módulo y como tal es Noetheriano porque el $\bar{R}$-submódulo de E son justamente los mismos como sus R-submódulos.
Además, como vemos al final de la última sección, $\bar{\gamma}_1, \bar{\gamma}_2, ..., \bar{\gamma}_s$ es un sistema de multiplicidad sobre el $\bar{R}$-módulo E.
Por consiguiente ambos $\gamma_1, \gamma_2, ..., \gamma_s$ y $\bar{\gamma}_1, \bar{\gamma}_2, ..., \bar{\gamma}_s$ tienen un sistema de multiplicidad sobre E. *Pedimos que*

$$e_R(\gamma_1, \gamma_2, ..., \gamma_s|E) = e_{\bar{R}}(\bar{\gamma}_1, \bar{\gamma}_2, ..., \bar{\gamma}_s) \tag{3.4.8}$$

si $s = 0$, entonces alli no hay problema porque (3.4.8) simplemente afirma que $L_R(E)$ y $L_{\bar{R}}(E)$ son iguales. Ahora supongamos que $s > 0$ y que el resultado en cuestión se prueba en el caso de sistema de multiplicidad con $s - 1$ elementos.
Entonces, puesto que $E/\gamma_1 E = E/\bar{\gamma}_1 E$ y $0 :_E \gamma_1 = 0 :_E \bar{\gamma}_1$, de ello resulta que

$$\begin{aligned} e_R(\gamma_1, \gamma_2, ..., \gamma_s|E) \qquad &= e_R(\gamma_2, ..., \gamma_s|E/\gamma_1 E) - e_R(\gamma_2, ..., \gamma_s|0 :_E \gamma_1) \\ &= e_{\bar{R}}(\bar{\gamma}_2, ..., \bar{\gamma}_s|E/\gamma_1 E) - e_{\bar{R}}(\bar{\gamma}_2, ..., \bar{\gamma}_s|0 :_E \gamma_1) \\ &= e_{\bar{R}}(\bar{\gamma}_2, ..., \bar{\gamma}_s|E/\bar{\gamma}_1 E) - e_{\bar{R}}(\bar{\gamma}_2, ..., \bar{\gamma}_s|0 :_E \bar{\gamma}_1) \\ &= e_{\bar{R}}(\bar{\gamma}_1, \bar{\gamma}_2, ..., \bar{\gamma}_s|E) \end{aligned}$$

de esta manera (3.4.8) es establecido. El símbolo de multiplicidad tiene una importante propiedad aditiva. El siguiente lema será util en establecer este hecho.

Lema 18. . *Sea* $0 \to E' \to E \to E'' \to 0$ *una sucesión exacta de R-módulos y sea* γ *un elemento central. Entonces una sucesión exacta es de la forma*

$$0 \to 0 :_{E'} \gamma \xrightarrow{\phi'} 0 :_E \gamma \xrightarrow{\psi'} 0 :_{E''} \gamma \xrightarrow{f} E'/\gamma E' \xrightarrow{\phi^*} E/\gamma E \xrightarrow{\psi^*} E''/\gamma E'' \to 0 \tag{3.4.9}$$

Prueba. Sin pérdida de generalidad podemos suponer que E' es un submódulo de E y $E'' = E/E'$. En el cual resulta que $\phi : E' \to E$ denota el mapeo inclusión y $\psi : E \to E''$ el mapeo natural de E sobre el factor módulo $E/E' = E''$.
Entonces $\phi(0 :_{E'} \gamma)$ es contenido en $0 :_{E'} \gamma$ y $\phi(\gamma E') \subseteq \gamma E$. De esta manera, ϕ desarrolla un mapeo ϕ' de $0 :_{E''} \gamma$ en $0 :_E \gamma$ y ésta induce un mapeo

$$\phi^* : E'/\gamma E' \to E/\gamma E$$

del mismo modo $\psi(0 :_E \gamma)$ es contenido en

$$0 :_{E''} \gamma \text{ y } \psi(\gamma E) \subseteq \gamma E''$$

de esta manera de ψ obtenemos el mapeo

$$0 :_E \gamma \to 0 :_{E''} \gamma \text{ y } E/\gamma E \to E''/\gamma E''$$

que denotaremos por γ' y $\gamma*$ respectivamente.
Luego definimos el mapeo de f. Si e'' pertenece a $0 :_{E''} \gamma$. Es posible escojer $e \in E$ así que $\psi(e) = e''$ y entonces, porque $\gamma e'' = 0$, tenemos $\psi(\gamma e)$ y por ello $\gamma e \in E'$. Ahora escribimos

$$f(e'') = \text{ imagen de } \gamma e \text{ en } E'/\gamma E' \tag{3.4.10}$$

y observamos que si $e_1 \in E$ también se tiene la propiedad que $\psi(e_1) = e''$, entonces $e - e_1$ pertenece a E' y por ello $\gamma e - \gamma e_1$ pertenece a $\gamma E'$. De esta manera γe y γe_1 tenemos la misma imagen en $E'/\gamma E'$ que prueba que f es bien definido por (3.4.10). Fácilmente verificamos que f es R-lineal.
Ahora el mapeo en (3.4.9) tiene todo definido, es necesario comprobar que la sucesión es exacta. La mayor parte de esto es muy simple. Verifiquemos que $kerf = Im\psi'$, $Imf = ker\phi^*$. Por (3.4.10), $f(e'') = 0$ sí y sólo sí $\gamma e \in \gamma E'$ que es digamos $\gamma(e - e') = 0$ para algún e' en E'. De esta manera $e'' \in kerf$ donde y sólo donde existe $\xi \in E$ tal que $\gamma\xi = 0$ y $\psi(\xi) = e''$. En otros términos, e'' está en $Kerf$ donde y sólo donde es la imagen, bajo ψ, de un elemento de $0 :_E \gamma$.
Esto prueba que $kerf = Im\psi'$.
De (3.4.10) vemos que $\phi^* f(e'') = 0$. Por consiguiente $Imf \subseteq ker\phi^*$.
Ahora asumamos que $\eta \in ker\phi^*$ y sea η la imagen de e' en $E'/\gamma E'$. Entonces $\phi^*(\eta)$ es la imagen de e' en $E/\gamma E$ de donde, puesto que $\phi^*(\eta) = 0,\ e' = \gamma e$ para algún e en E.
Sea $e'' = \psi(e)$. Entonces $\gamma e'' = \psi(\gamma e) = \psi(e') = 0$ que prueba e'' pertencea a $0 :_{E''} \gamma$.
Además, por (3.4.10), $f(e'')$ es la imagen de $\gamma e = e'$ en $E'/\gamma E''$, que es digamos $f(e'') = \eta$. De esta manera $\eta \in Imf$ y por ello $Ker\phi^* \subseteq Imf$. Lo que prueba el lema. ||

Teorema 37. *Sea* $0 \to E' \to E \to E'' \to 0$ *una sucesión exacta de R-módulos Noetherianos y supongamos que* $\gamma_1, \gamma_2, ..., \gamma_s$ *es un sistema de multiplicidad sobre cada término. Entonces*

$$e_R(\gamma_1, ..., \gamma_s|E) = e_R(\gamma_1, ..., \gamma_s|E') + e_R(\gamma_1, ..., \gamma_s|E'')$$

es conveniente probar el Teorema 37 y el siguiente corolario junto.

Corolario 20. *Sea* $0 \to E_p \to \cdots \to E_1 \to E_0 \to 0$ *una sucesión exacta de R-módulos Noetherianos y supongamos que* $\gamma_1, \gamma_2, ..., \gamma_s$ *es un sistema de multiplicidad sobre cada término. Entonces*

$$\sum_{i=0}^{p}(-1)^i e_R(\gamma_1, ..., \gamma_s|E_i) = 0$$

Prueba. El teorema y el corolario serán probados simultáneamente usando inducción sobre s. Cuando $s = 0$ no hay problema.
Asumamos que $s \geq 1$ y que ambos el teorema y el corolario sabemos que son verdaderos cuando tenemos un sistema de multiplicidad conteniendo sólo $s - 1$ elementos.
Volvamos ahora al Teorema 37, observamos que, por el Lema 18, tenemos una sucesión exacta

$$0 \to 0 :_{E'} \gamma_1 \to 0 :_E \gamma_1 \to 0 :_{E''} \gamma_1 \to E'/\gamma_1 E' \to E/\gamma_1 E \to E''/\gamma_1 E'' \to 0$$

en esta sucesión todo término es un R-módulo Noetheriano y admite $\gamma_2, \gamma_3, ..., \gamma_s$ como un sistema de multiplicidad. Por consiguiente estamos en una posición para aplicar Corolario 20. Esto produce
$e_R(\gamma_2, ..., \gamma_s|E/\gamma_1 E) - e_R(\gamma_2, ..., \gamma_s|0 :_E \gamma_1)$

$$\begin{aligned} &= e_R(\gamma_2, ..., \gamma_s|E'/\gamma_1 E') - e_R(\gamma_2, ..., \gamma_s|0 :_{E'} \gamma_1) \\ &\quad + e_R(\gamma_2, ..., \gamma_s|E''/\gamma_1 E'') - e_R(\gamma_2, ..., \gamma_s|0 :_{E''} \gamma_1) \end{aligned}$$

pero puede ser escrito como

$$e_R(\gamma_1, ..., \gamma_s|E) = e_R(\gamma_1, ..., \gamma_s|E') + e_R(\gamma_1, ..., \gamma_s|E')$$

en vista de (3.4.7).

Corolario 21. *Sea* $E_1,\ E_2$ *submódulo Noetheriano de un R-módulo E y sea* $\gamma_1, \gamma_2, ..., \gamma_s$ *un sistema de multiplicidad sobre ambos* E_1 *y* E_2*. Entonces* $\gamma_1, \gamma_2, ..., \gamma_s$ *un sistema de multiplicidad sobre el módulo Noetheriano*

$$E_1 + E_2,\ E_1 \cap E_2$$

y

$$e_R(\gamma_1, ..., \gamma_s|E_1 + E_2) + e_R(\gamma_1, ..., \gamma_s|E_1 \cap E_2)$$

$$= e_R(\gamma_1, ..., \gamma_s|E_1) + e_R(\gamma_1, ..., \gamma_s|E_2) \tag{3.4.11}$$

Prueba. El hecho que $E_1 + E_2$ y $E_1 \cap E_2$ son R-módulos Noetherianos resultando, $E_1 \oplus E_2$ un R-módulo Noetheriano. Puesto que tenemos una sucesión exacta

$$0 \to E_1 \to E_1 \oplus E_2 \to E_2 \to 0,$$

la proposición 20 prueba que $\gamma_1, \gamma_2..., \gamma_s$ es un sistema de multiplicidad sobre $E_1 \oplus E_2$. Nuevamente
$E_1 + E_2$ es isomorfo a un factor módulo de $E_1 \oplus E_2$ y $E_1 \cap E_2$ es un submódulo de E_1.
De aquí, nuevamente por virtud de Proposición 3, $\gamma_1, \gamma_2, ..., \gamma_s$ es un sistema de multiplicidad sobre $E_1 + E_2$ y $E_1 \cap E_2$.
Esto prueba que toda la multiplicidad ocurre en (3.4.11) son bien definidos. Considerando la sucesión

$$0 \to E_1 \to E_1 + E_2 \to (E_1 + E_2)/E_1 \to 0.$$

tenemos un isomorfismo

$$(E_1 + E_2)/E_1 \approx E_2/(E_1 \cap E_2)$$

así que la sucesión puede ser reescrita como

$$0 \to E_1 \to E_1 + E_2 \to E_2/(E_1 \cap E_2) \to 0 \tag{3.4.12}$$

también tenemos una sucesión exacta

$$0 \to E_1 \cap E_2 \to E_2 \to E_2/(E_1 \cap E_2) \to 0 \tag{3.4.13}$$

el resultado deseado ahora resulta aplicando el Teorema 37 para (3.4.12) y (3.4.13)

Corolario 22. *Sea E_1 y E_2 submódulos de un R-módulo E tal que E/E_1 y E/E_2 son Noetheriano. Si ahora $\gamma_1, \gamma_2, ..., \gamma_s$ es un sistema de multiplicidad sobre E/E_1 y E/E_2, entonces es también un sistema de multiplicidad sobre el módulo Noetheriano $E/(E_1 \cap E_2)$ y $E/(E_1 + E_2)$.*
Además

$$e_R(\gamma_1, ..., \gamma_s|E/(E_1 \cap E_2)) + e_R(\gamma_1, ..., \gamma_s|E/(E_1 + E_2))$$
$$= e_R(\gamma_1, ..., \gamma_s|E/E_1) + e_R(\gamma_1, ..., \gamma_s|E/E_2) \tag{3.4.14}$$

Prueba. El módulo $E/(E_1 + E_2)$ es Noetheriano y admite $\gamma_1, \gamma_2, ..., \gamma_s$ como un sistema de multiplicidad porque es isomorfo a un módulo factor de E/E_1. Sobre el otro lado $E/(E_1 \cap E_2)$ es Noetheriano.
En efecto la prueba de este resultado demuestra que $E/(E_1 \cap E_2)$ es isomorfo al submódulo de $(E/E_1) \oplus (E/E_2)$ y la suma directa sabemos que es Noetheriano.
Luego, por la proposición 20 la sucesión exacta

$$0 \to E/E_1 \to (E/E_1) \oplus (E/E_2) \to E/E_2 \to 0$$

vemos que $\gamma_1, \gamma_2, ..., \gamma_s$ es un sistema de multiplicidad sobre $(E/E_1) \oplus (E/E_2)$ y de aquí en $E/(E_1 \cap E_2)$. De esta manera la multiplicidad que ocurre en (3.4.14) es bien definida.
El módulo $E_1/(E_1 \cap E_2)$ es isomorfo a $(E_1 + E_2)/E_2$ así podemos reescribir la sucesión exacta

$$0 \to E_1/(E_1 \cap E_2) \to E/(E_1 \cap E_2) \to E/E_1 \to 0$$

como

$$0 \to (E_1 + E_2)/E_2 \to E/(E_1 \cap E_2) \to E/E_1 \to 0 \qquad (3.4.15)$$

también tenemos una sucesión exacta

$$0 \to (E_1 + E_2)/E_2 \to E/E_2 \to E/(E_1 + E_2) \to 0 \qquad (3.4.16)$$

el corolario ahora resulta aplicando el Teorema 37 a la sucesión (3.4.15) y (3.4.16). ||

Lema 19. *Sea E un R-módulo y $\gamma_1, \gamma_2, ..., \gamma_s$ $(s \geq 2)$ un sistema de multiplicidad sobre E Entonces $e_R(\gamma_1, \gamma_2\gamma_3, ..., \gamma_s|E) = e_R(\gamma_2, \gamma_1\gamma_3, ..., \gamma_s|E)$.*

Prueba. Simplemente aplicamos (3.4.7) dos veces y examinamos el resultado para ver si es simétrico en γ_1 y γ_2. Sin embargo la expresión que ocurre porque es un poco complicada. Por esta razón introducimos alguna notación auxiliar que es como sigue. Cuando K es un R-módulo Noetheriano con la propiedad que $\gamma_3, \gamma_4, ..., \gamma_s$ es un sistema de multiplicidad sobre este, escribimos $[K] = e_R(\alpha_3, ..., \alpha_s|K)$. Observamos que si $L \subseteq M$ son submódulos de un R-módulo Noetheriano N y $\gamma_3, \gamma_4, ..., \gamma_s$ es un sistema de multiplicidad sobre N/L, entonces $\gamma_3, \gamma_4, ..., \gamma_s$ es un sistema de multiplicidad sobre cada M/L y N/M, y tenemos

$$[N/L] = [N/M] + [M/L] \qquad (3.4.17)$$

esto es claro si aplicamos la proposición 20 y el Teorema 37 para la sucesión exacta

$$0 \to M/L \to N/L \to N/M \to 0.$$

ahora estamos listos para calcular el principio. Por (3.4.7),

$$e_R(\gamma_1, \gamma_2, ..., \gamma_s|E) = e_R(\gamma_2, \gamma_3, ..., \gamma_s|E/\gamma_1 E) - e_R(\gamma_2, \gamma_3, ..., \gamma_s|0 :_E \gamma).$$

ahora usaremos la misma relación para expresar cada término sobre el lado derecho como la diferencia de multiplicidad 2. Esto dado

$$e_R(\gamma_1, \gamma_2, ..., \gamma_s|E) = [1] - [2] - [3] + [4] \ \text{ donde}$$

$$\begin{aligned}
[1] &= [(E/\gamma_1 E)/\gamma_2(E/\gamma_1 E)],\\
[2] &= [0 :_{E/\gamma_1 E} \gamma_2],\\
[3] &= [(0 :_E \gamma_1)/\gamma_2(0 :_E \gamma_1)],\\
[4] &= [0 :_{(0:_E\gamma_1)} \gamma_2]
\end{aligned}$$

ahora, por (3.1.3), $(E/\gamma_1 E)/\gamma_2(E/\gamma_1 E)$ es isomorfo a $E/(\gamma_1 E + \gamma_2 E)$.
En el otro lado es obvio que $0 :_{(0:_E\gamma_1)} \gamma_2 = (0 :_E \gamma_1) \cap (0 :_E \gamma_2)$.
Por consiguiente

$$\begin{aligned}
[1] &= [E/(\gamma_1 E + \gamma_2 E)] \qquad \text{y}\\
[4] &= [(0 :_E \gamma_1) \cap (0 :_E \gamma_2)]
\end{aligned}$$

ambos que concierne γ_1 y γ_2 simultáneamente. De esta manera sólo trataremos nosotros mismos con $[2] + [3]$. Por (3.1.5), tenemos

$$0 :_{E/\gamma_1 E} \gamma_2 = (\gamma_1 E :_E \gamma_2)/\gamma_1 E$$

y es evidente que $\gamma_1 E \subseteq \gamma_1 E + (0 :_E \gamma_2) \subseteq \gamma_1 E :_E \gamma_2$. De aquí, por (3.4.17),

$$\begin{aligned}
[2] \qquad &= [(\gamma_1 E + (0 :_E \gamma_2))/\gamma_1 E] + [(\gamma_1 E :_E \gamma_2)/(\gamma_1 E + (0 :_E \gamma_2))]\\
&= [(0 :_E \gamma_2)/\gamma_1 E \cap (0 :_E \gamma_2)] + [(\gamma_1 E :_E \gamma_2)/(\gamma_1 E + (0 :_E \gamma_2))]
\end{aligned}$$

tal que,

$$(\gamma_1 E + (0 :_E \gamma_2))/\gamma_1 E$$

es isomorfo a $(0 :_E \gamma_2)/(\gamma_1 E \cap (0 :_E \gamma_2))$.
Luego, por (3.1.2) y (3.1.1),

$$\gamma_1 R \cap (0 :_E \gamma_2) = \gamma_1(0 :_E \gamma_1\gamma_2)$$

de esta manera $[2] = [5] + [6]$, donde $[5] = [(0 :_E \gamma_2)/\gamma_1(0 :_E \gamma_1\gamma_2)]$ y

$$[6] = [(\gamma_1 E :_E \gamma_2)/(\gamma_1 E + (0 :_E \gamma_2))]$$

de nuevo multiplicando por γ_2 produce un homomorfismo de $\gamma_1 E :_E \gamma_2$ sobre $\gamma_2(\gamma_1 E :_E \gamma_2)$ que, por (3.1.2), es el mismo como $\gamma_1 E \cap \gamma_2 E$.
De esta manera tenemos un homomorfismo

$$(\gamma_1 E :_E \gamma_2) \to \gamma_1 E \cap \gamma_2 E$$

del cual el núcleo es $0 :_E \gamma_2$. Ahora $\gamma_1 E + (0 :_E \gamma_2)$ contiene este núcleo y es el mapeo sobre $\gamma_1\gamma_2 E$. De ello resulta, que tenemos un isomorfismo

$$(\gamma_1 E :_E \gamma_2)/(\gamma_1 E + (0 :_E \gamma_2)) \approx (\gamma_1 E \cap \gamma_2 E)/\gamma_1\gamma_2 E$$

por consiguiente $[6] = [(\gamma_1 E \cap \gamma_2 E)/\gamma_1\gamma_2 E]$, es simétrico en γ_1 y γ_2. Esto queda para examinar la suma de [3] y [5]. Evidentemente

$$\gamma_2(0 :_E \gamma_1) \subseteq \gamma_2(0 :_E \gamma_1\gamma_2) \subseteq 0 :_E \gamma_1$$

de aquí, por (3.4.17),

$$[3] + [5] = [7] + \{8\}\,,$$

donde

$$[7] = [\gamma_2(0 :_E \gamma_1\gamma_2)/\gamma_2(0 :_E \gamma_1)]$$

y

$$\{8\} = [(0 :_E \gamma_1)/\gamma_2(0 :_E \gamma_1\gamma_2)] + [(0 :_E \gamma_2)/\gamma_1(0 :_E \gamma_1\gamma_2)].$$

lo último de esto tenemos la simetría deseada. También multiplicando por γ_2 se induce un epimorfismo

$$(0 :_E \gamma_1\gamma_2) \to \gamma_2(0 :_E \gamma_1\gamma_2)$$

que es tal que la imagen inversa de $\gamma_2(0 :_E \gamma_1)$ es $(0 :_E \gamma_1) + (0 :_E \gamma_2)$.
Por consiguiente tenemos un isomorfismo

$$(0 :_E \gamma_1\gamma_2)/((0 :_E \gamma_1) + (0 :_E \gamma_2)) \approx \gamma_2(0 :_E \gamma_1\gamma_2)/\gamma_2(0 :_E \gamma_1)$$

y por ello

$$[7] = [(0 :_E \gamma_1\gamma_2)/((0 :_E \gamma_1) + (0 :_E \gamma_2))]$$

que es otra expresión simétrica.
Recopilando términos encontramos que $e_R(\gamma_1, \gamma_2, ..., \gamma_s|E)$ es igual a

$$[1] + [4] - [6] - [7] - \{8\}$$

y que cada término tiene la propiedad que permanece inalterado γ_1 y γ_2 cuando son intercambiados. Lo que prueba el lema ||

Proposición 21. *Sea E un R-módulo Noetheriano y $\gamma_1, \gamma_2, ..., \gamma_s$ un sistema de multiplicidad sobre E. Si ahora $\{i_1, i_2, ..., i_s\}$ es una pemutación de $\{1, 2, ..., s\}$, entonces $e_R(\gamma_1, \gamma_2, ..., \gamma_s|E) = e_R(\gamma_{i_1}, \gamma_{i_2}, ..., \gamma_{i_s}|E)$*

Observación 6. *. Nos referimos a esta propiedad de el símbolo de multiplicidad como la Propiedad de Cambio.*

Prueba. Es suficiente probar que el valor de $e_R(\gamma_1, ..., \gamma_m, \gamma_{m+1}, ..., \gamma_s|E)$ es inalterado si cambiamos γ_m y γ_{m+1}. Ahora por $m-1$ aplicando (3.4.7) obtenemos una expresión de $e_R(\gamma_1, ..., \gamma_s)|E$ como una suma finita como sigue:

$$e_R(\gamma_1, ..., \gamma_m, \gamma_{m+1}, ..., \gamma_s|E) = \sum_v \epsilon_v e_R(\gamma_m, \gamma_{m+1}, ..., \gamma_s|E_v)$$

aquí cada ϵ_v es igual a ± 1 y cada E_v es un R-módulo Noetheriano que admite $\gamma_m, \gamma_{m+1}, ..., \gamma_s$ como un sistema de multiplicidad. Además, el número ϵ_v y el módulo E_v son determinados solamente por E y $\gamma_1, ..., \gamma_{m-1}$, que dicen ser completamente independientes de $\gamma_m, \gamma_{m+1}, ..., \gamma_s$.
Si intercambiamos γ_m y γ_{m+1} obtenemos

$$e_R(\gamma_1, ..., \gamma_{m+1}, \gamma_m, ..., \gamma_s|E) = \sum_v \epsilon_v e_R(\gamma_{m+1}, \gamma_m, ..., \gamma_s|E_v)$$

donde ϵ_v y E_v tienen el mismo significado como antes. Pero, por Lema 19,

$$e_R(\gamma_m, \gamma_{m+1}, ..., \gamma_s|E_v) = e_R(\gamma_{m+1}, \gamma_m, ..., \gamma_s|E_v)$$

de ello resulta que $e_R(\gamma_1, ..., \gamma_m\gamma_{m+1}, ..., \gamma_s|E) = e_R(\gamma_1, ..., \gamma_{m+1}\gamma_m, ..., \gamma_s|E)$ y con esto la Proposición se establece. $||$

Proposición 22. *Sea E un R-módulo Noetheriano y $\gamma_1, \gamma_2, ..., \gamma_s$ un sistema de multiplicidad sobre E. Asumamos que para algún valor en particular de i tenemos $\gamma_i^m E = 0$, donde m es un entero positivo. Entonces $e_R(\gamma_1, \gamma_2, ..., \gamma_s|E) = 0$*

Prueba. La propiedad de cambio de el símbolo de multiplicidad prueba que podemos asumir que $i = 1$. Hecha esta suposición procedemos aprobar la proposición por inducción sobre m. Primero supongamos que $m = 1$.
Entonces $\gamma_1 E = 0$ y por ello $E/\gamma_1 E = E$ y $0 :_E \gamma_1 = E$.
Por consiguiente, por (3.4.7),

$$e_R(\gamma_1, \gamma_2, ..., \gamma_s|E) = e_R(\gamma_2, ..., \gamma_s|E) - e_R(\gamma_2, ..., \gamma_s|E) = 0$$

ahora asumimos que $m > 1$ y que el resultado deseado se cumple para valores pequeños de la variable inductiva. Por el Teorema 37 y la sucesión exacta

$$0 \to \gamma_1 E \to E \to E/\gamma_1 E \to 0$$

vemos que

$$e_R(\gamma_1, \gamma_2, ..., \gamma_s|E) = e_R(\gamma_1, \gamma_2, ..., \gamma_s|\gamma_1 E) + e_R(\gamma_1, \gamma_2, ..., \gamma_s|E/\gamma_1 E).$$

sin embargo

$$\gamma_1^{m-1}(\gamma_1 E) = 0 \text{ y } \gamma_1(E/\gamma_1 E) = 0.$$

Aquí, por la hipótesis inductiva, ambos

$$e_R(\gamma_1, ..., \gamma_s|\gamma_1 E) \text{ y } e_R(\gamma_1, , ..., \gamma_s|0 :_E \gamma_1) \text{ son cero.}$$

La Proposición resulta ||

Lema 20. *Sea E un R-módulo Noetheriano y γ un elemento central.*
Sea $F_m = E/(0 :_E \gamma_m)$.
Entonces $0 :_{F_m} \gamma = 0$ siempre que m es suficientemente grande.

Prueba. Puesto que E es un R-módulo Noetheriano, la sucesión ascendente

$$0 :_E \gamma \subseteq 0 :_E \gamma^2 \subseteq 0 :_E \gamma^3 \subseteq ...$$

de submódulos de E debe finalizar. Supongamos ahora que m es suficientemente grande para asegurar que

$$0 :_E \gamma^m = 0 :_E \gamma^{m+1}.$$

entonces, por (3.1.5) y (3.1.1),

$$\begin{aligned} 0_{F_m}\gamma \quad &= ((0_E\gamma^m) :_E \gamma)/(0 :_E \gamma^m) = (0_E\gamma^{m+1})/(0 :_E \gamma^m) \\ &= (0_E\gamma^m)/(0 :_E \gamma^m) = 0 \end{aligned}$$

Teorema 38. *Sea E un R-módulo Noetheriano y $\gamma_1, \gamma_2, ..., \gamma_s$ un sistema de multiplicidad sobre E. Entonces*

$$0 \leq e_R(\gamma_1, , ..., \gamma_s|E) \leq L_R\{E/(\gamma_1 E + ... + \gamma_s E)\} \tag{3.4.18}$$

Prueba. Primero probaremos, usando inducción sobre s, $e_R(\gamma_1, , ..., \gamma_s|E)$ es no negativo. Si $s = 0$, entonces es obvio.
Por ello asumamos que $s \geq 1$ y también que el caracter no negativo de multiplicidad es establecido en el caso de sistema de multiplicidad dado sólo $s - 1$ miembros.
Sea $F = E/(0 :_E \gamma^m)$, donde m se escoje suficientemente grande para asegurar que $0_F\gamma_1 = 0$.

Esto es posible por el Lema 20. Luego, aplicando el Teorema 37 a la sucesión exacta

$$0 \rightarrow 0 :_E \gamma_1^m \rightarrow E \rightarrow F \rightarrow 0$$

y se construye usando la proposición 22, vemos que

$$e_R(\gamma_1, \gamma_2, ..., \gamma_s|E) = e_R(\gamma_1, \gamma_2, ..., \gamma_s|F) = e_R(\gamma_2, ..., \gamma_s|F/\gamma_1 F)$$

porque $0 :_F \gamma_1 = 0$. Sin embargo, por la hipótesis inductiva, $e_R(\gamma_2, ..., \gamma_s|F/\gamma_1 F)$ es no negativo y así el mismo es verdadero de $e_R(\gamma_1, \gamma_2, ..., \gamma_s|R)$.
Queda por establecer la segunda desigualdad en (3.4.18). Si $s \geq 1$ tenemos

$$e_R(\gamma_1, \gamma_2, ..., \gamma_s|E) = e_R(\gamma_2, ..., \gamma_s|E/\gamma_1 E) - e_R(\gamma_2, ..., \gamma_s|0 :_E \gamma_1)$$

donde

$$e_R(\gamma_1, \gamma_2, ..., \gamma_s|E) \leq e_R(\gamma_2, ..., \gamma_s|E/\gamma_1 E) \tag{3.4.19}$$

porque $e_R(\gamma_2, ..., \gamma_s|0 :_E \gamma_1)$ es no negativo.
En esta desigualdad sustituimos $\gamma_1, \gamma_2, ..., \gamma_s$ y

$$E \text{ por } \gamma_2, \gamma_3, ..., \gamma_s \text{ y } E/\gamma_1 E = E'.$$

esto prueba que

$$e_R(\gamma_2, \gamma_3, ..., \gamma_s|E/\gamma_1 E) \leq e_R(\gamma_3, ..., \gamma_s|E'/\gamma_2 E')$$

pero, por (3.1.3), $E'/\gamma_2 E'$ es isomorfo a $E/(\gamma_1 E + \gamma_2 E)$. Aquí

$$e_R(\gamma_1, \gamma_2, ..., \gamma_s|E) \leq e_R(\gamma_3, ..., \gamma_s|E(\gamma_1 E + \gamma_2 E))$$

procediendo en este camino finalmente llegamos a la desigualdad

$$e_R(\gamma_1, \gamma_2, ..., \gamma_s|E) \leq e_R(\cdot|E/(\gamma_1 E, ..., \gamma_s E))$$

En vista de (3.4.6) se completa la prueba. ||

Corolario 23. *Si $\gamma_1, \gamma_2, ..., \gamma_s$ es un sistema de multiplicidad sobre un R-módulo Noetheriano E y $\gamma_1 E, \gamma_2 E, ..., \gamma_s E = E$, entonces*

$$e_R(\gamma_1, , ..., \gamma_s|E) = 0$$

Teorema 39. *Sea E un R-módulo Noetheriano y sea*

$$\gamma_1, ..., \gamma_i, ..., \gamma_s \text{ y } \gamma_1, ..., \gamma_i^{'}, ..., \gamma_s$$

un sistema de multiplicidad sobre E.
Entonces $\gamma_1, ..., \gamma_i\gamma_i^{'}, ..., \gamma_s$ es también un sistema de multiplicidad sobre E y $e_R(\gamma_1 + ... + \gamma_i\gamma_i^{'} + ... + \gamma_s|E)$

$$= e_R(\gamma_1 + ... + \gamma_i + ... + \gamma_s|E) + e_R(\gamma_1 + ... + \gamma_i^{'} + ... + \gamma_s|E) \qquad (3.4.20)$$

Prueba. Sea $F = \gamma_1 E + ... + \gamma_i E + ... + \gamma_s E$. Entonces F es un submódulo de E y por ello, por la proposición 20, $\gamma_1, ..., \gamma_i^{'}, ..., \gamma_s$ es un sistema de multiplicidad sobre F. Luego
$L_R \left\{E|(\gamma_1 F + ... + \gamma_i^{'} F + ... + \gamma_s F)\right\}$

$$= L_R \{E/F\} + L_R \left\{F/(\gamma_1 F + ... + \gamma_i^{'} F + ... + \gamma_s F)\right\}$$

y, en esta ecuación, los términos en el lado derecho son finitos. Nuevamente

$$\gamma_1 F + ... + \gamma_i^{'} F + ... + \gamma_s F \subseteq \gamma_1 E + ... + \gamma_i\gamma_i^{'} E + ... + \gamma_s E \subseteq E$$

y así vemos que $L_R \left\{E/(\gamma_1 E + ... + \gamma_i\gamma_i^{'} E + ... + \gamma_s E)\right\} < \infty$.
Por consiguiente $\gamma_1 + ... + \gamma_i\gamma_i^{'} + ... + \gamma_s$ es un sistema de multiplicidad sobre E.
Ahora probemos (3.4.20), podemos suponer que $i = s$. Pero, repitiendo la aplicacion de (3.4.7),

$$e_R(\gamma_1, ..., \gamma_{s-1}, \gamma_s|E) = \sum_v \epsilon_v e_R(\gamma_s|E_v).$$

aquí el lado derecho es una suma finita en que cada ϵ_v tiene el valor ± 1 y los E_v son ciertos R-módulos Noetherianos en que γ_s es, por lo mismo, un sistema de multiplicidad. Además el número ϵ_v y el módulo E_v depende sólo de E y los elementos $\gamma_1, \gamma_2, ..., \gamma_{s-1}$. De ello resulta que

$$e_R(\gamma_1, ..., \gamma_{s-1}, \gamma_s^{'}|E) = \sum_v \epsilon_v e_R(\gamma_s^{'}|E_v) \text{ y } e_R(\gamma_1, ..., \gamma_{s-1}, \gamma_s\gamma_s^{'}|E) = \sum_v \epsilon_v e_R(\gamma_s\gamma_s^{'}|E_v)$$

que el mismo ϵ_v y E_v como antes. Vemos de esto que es sólo necesario probar el teorema en el caso $s = 1$. En lo que sigue asumimos que se cumple ésta condición y, para simplificar la notación, escribimos γ y γ' en lugar de γ_s y $\gamma_s^{'}$. Por definición, tenemos

$$e_R(\gamma|E) = L_R(E|\gamma E) - L_R(0 :_E \gamma)$$

con expresiones similares de $e_R(\gamma'|E)$ y $e_R(\gamma\gamma'|E)$.
Luego multiplicando por γ produce un epimorfismo $E \to \gamma E$ con la propiedad

que la imagen inversa de $\gamma\gamma' E$ es $(0 :_E \gamma) + \gamma' E$.
Por consiguiente tenemos un isomorfismo

$$\gamma E/\gamma\gamma' E \approx E/((0 :_E \gamma) + \gamma' E)$$

donde

$$L_R(\gamma E/\gamma\gamma' E) = L_R(E/\gamma' E) - L_R((0 :_E \gamma + \gamma' E)/\gamma' E).$$

sin embargo $(0 :_E \gamma + \gamma' E)/\gamma' E$ es isomorfo a

$$(0 :_E \gamma)/(\gamma' E \cap (0 :_E \gamma)) = (0 :_E \gamma)/\gamma'(0 :_E \gamma\gamma')$$

y así

$$L_R(\gamma E/\gamma\gamma' E) = L_R(E/\gamma' E) - L_R(0 :_E \gamma) + L_R(\gamma'(0 :_E \gamma\gamma'))$$

que produce

$$L_R(E/\gamma\gamma' E) = L_R(E/\gamma E) - L_R(0 :_E \gamma) + L_R(E/\gamma' E) + L_R(\gamma'(0 :_E \gamma\gamma'))$$

sumando $L_R(E/\gamma E)$ a ambos lados.
Para completar la prueba es suficiente probar que

$$L_R(\gamma'(0 :_E \gamma\gamma')) = L_R(0 :_E \gamma\gamma') - L_R(0 :_E \gamma').$$

sin embargo es claro porque $\gamma'(0 :_E \gamma\gamma')$ es isomorfo a

$$(0 :_E \gamma\gamma')/(0 :_E \gamma')$$

como podemos ver del epimorfismo

$$(0 :_E \gamma\gamma') \to \gamma'(0 :_E \gamma\gamma')$$

producido por medio de multiplicar por γ'. ||

Corolario 24. *Sea E un R-módulo Noetheriano, $\gamma_1, \gamma_2, ..., \gamma_s$ un sistema de multiplicidad sobre E, y $n_1, n_2, ..., n_s$ enteros positivos. Entonces $\gamma_1^{n_1}, \gamma_2^{n_2}, ..., \gamma_s^{n_s}$ también es un sistema de multiplicidad sobre E y*

$$e_R(\gamma_1^{n_1}, \gamma_2^{n_2}, ..., \gamma_s^{n_s}|E) = n_1 n_2 ... n_s e_R(\gamma_1, \gamma_2, ..., \gamma_s|E)$$

esto resulta repitiendo la aplicación del teorema.

Corolario 25. *Sea E un R-módulo Noetheriano, y $\gamma_1, \gamma_2, ..., \gamma_s$ un sistema de multiplicidad sobre E, entonces*

$$0 \leq e_R(\gamma_1, ..., \gamma_s|E) \leq \frac{L_R\left\{(\gamma_1^{n_1}E, ..., \gamma_s^{n_s}E)\right\}}{n_1 n_2 ... n_s}$$

para enteros positivos arbitrarios $n_1, n_2, ..., n_s$.

Prueba. Puesto que $n_1 n_2 ... n_s e_R(\gamma_1, \gamma_2, ..., \gamma_s|E)$ es igual a

$$e_R(\gamma_1^{n_1}, \gamma_2^{n_2}, ..., \gamma_s^{n_s})|E$$

el resultando deseado se sigue del Teorema 38. ||

Corolario 26. *Sea E un R-módulo Noetheriano, y $\gamma_1, \gamma_2, ..., \gamma_s$ un sistema de multiplicidad sobre E. Supongamos que*

$$\gamma_i^m E \subseteq \gamma_1 E + ... + \gamma_{i-1} E + \gamma_{i+1}(E) + ... + \gamma_s E$$

donde m es un entero positivo. Entonces $e_R(\gamma_1, ..., \gamma_s|E) = 0$

Prueba. Por la proposición 21, podemos suponer que $i = 1$. Si ahora $n > m$, entonces $\gamma_1^n E + \gamma_2 E + ... + \gamma_s E = \gamma_2 E + ... + \gamma_s E$ y así, por Cor. 21,

$$0 \leq n e_R(\gamma_1 \gamma_2, ..., \gamma_s|E) \leq L_R\left\{(\gamma_2 E, ..., \gamma_s E)\right\} < \infty$$

el resultado deseado se sigue de dividir directamene por n y entonces n tiende a infinito. ||

Es de considerable interés saber bajo que condiciones la multiplicidad $e_R(\gamma_1, ..., \gamma_s|E)$ y la longitud de $L_R\left\{E/(\gamma_1 E, ..., \gamma_s E)\right\}$ son iguales. Primero damos una condición suficiente para que esto ocurra.

Teorema 40. *Sea E un R-módulo Northeriano y $\gamma_1, \gamma_2, ..., \gamma_s$ un sistema de multiplicidad sobre E.*
Si ahora

$$(\gamma_1 E + \gamma_2 E + ... + \gamma_i E) :_E \gamma_{i+1} = \gamma_1 E + \gamma_2 E + ... + \gamma_i E$$

para $0 \leq i \leq s-1$, entonces

$$e_R(\gamma_1, ..., \gamma_s|E) = L_R\left\{E/(\gamma_1 E, ..., \gamma_s E)\right\}.$$

Prueba. Sea $E_i = E/(\gamma_1 E + ... + \gamma_i E)$. Entonces, por nuestra hipótesis y (3.1.5), tenemos $0 :_{E_i} \gamma_{i+1} = 0$ para $0 \leq i \leq s-1$. También, por (3.1.3), $E_i/\gamma_{i+1}E_i$ y E_{i+1} son isomorfismos. Por consiguiente

$$\begin{aligned} e_R(\gamma_1, \gamma_2, ..., \gamma_s|E) \qquad &= e_R(\gamma_2, \gamma_3 ..., \gamma_s|E_1) \\ &= e_R(\gamma_3, ..., \gamma_s|E_2) \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ &= e_R(\cdot|E_s) \\ &= L_R\left\{E/(\gamma_1 E + ... + \gamma_s E)\right\} \end{aligned}$$

nuestro siguiente resultado proporciona un importante resultado opuesto al Teorema 40.

Teorema 41. *Sea E un R-módulo Noetheriano y $\gamma_1, \gamma_2 ..., \gamma_s$ un sistema de multiplicidad sobre E del cuál los elementos son considerados en el radical de Jacobson de R. Entonces las siguientes dos afirmaciones son equivalentes:*

(a) $e_R(\gamma_1, \gamma_2, ..., \gamma_s|E) = L_R\left\{E/(\gamma_1 E, ..., \gamma_s E)\right\}$;

(b) *para* $0 \leq i \leq s-1$, *tenemos* $(\gamma_1 E + ... + \gamma_i E) :_E \gamma_{i+1} = \gamma_1 E + ... + \gamma_i E$

Prueba. Por el Teorema 40, necesitamos sólo probar que (a) implica (b). Para esto usemos inducción sobre s. Cuando $s = 1$ tenemos

$$e_R(\gamma_1|E) = L_R(E/\gamma_1 E) - L_R(0 :_E \gamma_1)$$

y así, puesto que asumimos (a) verdadero, $L_R(0 :_E \gamma_1) = 0$.
Por consiguiente $0 :_E \gamma_1 = 0$ que es todo lo que necesitamos en este caso.
De aquí asumamos que $s > 1$ y también que la afirmación "(a) implica (b)" se establece en todas circunstancias donde el sistema de multiplicidad tiene sólo $s-1$ elementos.
Sea $n_1, n_2, ..., n_s$ enteros positivos.
Entonces, por el Teorema 38, la Proposición 19, y el Teorema 39 Cor. 20,

$$\begin{aligned} e_R(\gamma_1^{n_1}, ..., \gamma_s^{n_s}|E) \qquad &\leq L_R\left\{E/(\gamma_1^{n_1} E + ... + \gamma_s^{n_s} E)\right\} \\ &\leq n_1 n_2 ... n_s L_R\left\{E/(\gamma_1 E, ..., \gamma_s E)\right\} \\ &= n_1 n_2 ... n_s e_R(\gamma_1, ..., \gamma_s|E) \\ &= e_R(\gamma_1^{n_1}, ..., \gamma_s^{n_s}|E) \end{aligned}$$

de esta manera

$$e_R(\gamma_1^{n_1}, ..., \gamma_s^{n_s}|E) = L_R\left\{E/(\gamma_1^{n_1} E + ... + \gamma_s^{n_s} E)\right\} \tag{3.4.21}$$

para enteros positivos arbitrarios $n_1, n_2, ..., n_s$. Sea $K = E/(0 :_E \gamma_1)$.
Entonces resulta de la sucesión exacta

$$0 \to 0 :_E \gamma_1 \to E \to K \to 0$$

y por la proposición 22, que

$$e_R(\gamma_1^{n_1}, ..., \gamma_s^{n_s}|E) = e_R(\gamma_1^{n_1}, ..., \gamma_s^{n_s}|K)$$

de aquí, por (3.4.21) y el Teorema 38,

$$\begin{aligned} L_R\{E/(\gamma_1^{n_1}E + ... + \gamma_s^{n_s}E)\} \qquad &= e_R(\gamma_1^{n_1}, ..., \gamma_s^{n_s}|K) \\ &\leq L_R\{K/(\gamma_1^{n_1}K + ... + \gamma_s^{n_s}K)\} \\ &= L_R\{E/((0 :_E \gamma_1) + \gamma_1^{n_1}E + ... + \gamma_s^{n_s}E)\} \end{aligned}$$

porque los módulos

$$K/(\gamma_1^{n_1}K + ... + \gamma_s^{n_s}K) \text{ y } E/((0 :_E \gamma_1) + \gamma_1^{n_1}E + ... + \gamma_s^{n_s}E)$$

son isomorfismos. Pero, puesto que

$$\gamma_1^{n_1}E + ... + \gamma_s^{n_s}E = (0 :_E \gamma_1) + \gamma_1^{n_1}E + ... + \gamma_s^{n_s}E$$

y por tanto

$$(0 :_E \gamma_1) \subseteq \gamma_1^{n_1}E + \gamma_2^{n_2}E + ... + \gamma_3^{n_3}E$$

para enteros positivos arbitrarios $n_1, n_2, ..., n_s$.
Sea $A = \gamma_1 R + \gamma_2 R + ... + \gamma_s R$ entonces para cada entero positivo n tenemos

$$(0 :_E \gamma_1) \subseteq \gamma_1^{n_1}E + ... + \gamma_s^{n_s}E \subseteq A^nE.$$

sin embargo, por el Teorema 36, la intersección de todos los

$$A^nE \ (n = 1, 2, 3, ...)$$

es el submódulo cero de E porque A es un ideal central contenido en el radical de Jacobson de R.
Por consiguiente $0 :_E \gamma_1 = 0$.
Sea $\bar{E} = E/\gamma_1 E$. Puesto que $0 :_E \gamma_1 = 0$ y tenemos un isomorfismo
$E/(\gamma_1 E + \gamma_2 E + ... + \gamma_s E) \approx \bar{E}/(\gamma_2 \bar{E} + ... + \gamma_s \bar{E})$
de ello resulta que

$$\begin{aligned} e_R(\gamma_2, ..., \gamma_s|\bar{E}) \qquad &= e_R(\gamma_1, \gamma_2, ..., \gamma_s|E) \\ &= L_R\{E/(\gamma_1 E + \gamma_2 E + ... + \gamma_s E)\} \\ &= L_R\left\{\bar{E}/(\gamma_2 \bar{E} + ... + \gamma_s \bar{E})\right\} \end{aligned}$$

es ahora posible aplicar la hipótesis inductiva. Esto prueba que

$$(\gamma_2\bar{E}, ..., \gamma_i\bar{E}) :_{\bar{E}} \gamma_{i+1} = \gamma_2\bar{E} + ... + \gamma_i\bar{E}$$

para $1 \leq i \leq s$. Pero $\gamma_2\bar{E} + ... + \gamma_i\bar{E} = (\gamma_1 E + \gamma_2 E + ... + \gamma_i E)/\gamma_1 E$.
Por consiguiente, por (3.1.4),

$$(\gamma_1 E + \gamma_2 E + ... + \gamma_i E) :_E \gamma_{i+1} = \gamma_1 E + \gamma_2 E + ... + \gamma_i E$$

no sólo para $i = 0$ sino también para $1 \leq i < s$. Se completa la prueba. ||

3.5. La fórmula límite de Lech

Históricamente la teoría moderna de multiplicidad empieza con el estudio del comportamiento asintótico de potencias de ideales.
Esta parte de la teoría vuelve a centrarse en dos expresiónes para $e_R(\gamma_1, ..., \gamma_s|E)$ como un límite. Uno de estos límites fórmulados es debido a P. Samuel y C. Lech.
Consideremos primero el caso en que tenemos un R-módulo Noetheriano E y un elemento central γ que, por si mismo forma un sistema de multiplicidad sobre E.
Entonces, porque

$$0_E\gamma \subseteq 0 :_E \gamma^2 \subseteq 0 :_E \gamma^3 \subseteq ...$$

es una sucesión ascendente de submódulos de E, existe un entero m tal que $0 :_E \gamma^n = 0 :_E \gamma^m$ para todo $n \geq m$.
Por consiguiente cuando $m \leq n$

$$e_R(\gamma^n|E) = L_R(E/\gamma^n E) - L_R(0 :_E \gamma^n) = L_R(E/\gamma^n E) - L_R(0 :_E \gamma^m)$$

ahora, por el Teorema 39, $e_R(\gamma^n)E = ne_R(\gamma|E)$. De ello resulta que

$$L_R(E/\gamma^n E) = ne_R(\gamma|E) + C$$

para todo $n \geq m$, donde C es independiente de n. En particular vemos que

$$\lim_{n\to\infty} \frac{L_R(E/\gamma^n E)}{n} = e_R(\gamma|E) \tag{3.5.22}$$

este es el caso simple de la fórmula de Lech. El resultado general está contenido en el siguiente teorema.

Teorema 42. *Sea E un R-módulo Noetheriano y $\gamma_1, \gamma_2, ..., \gamma_s$ un sistema de multiplicidad sobre E. Entonces*

$$\lim_{min(n_i)\to\infty} \frac{L_R\left\{E/(\gamma_1^{n_1}E + ... + \gamma_s^{n_s}E)\right\}}{n_1 n_2 ... n_s} = e_R(\gamma_1, ..., \gamma_s|E) \tag{3.5.23}$$

Prueba. Usaremos inducción sobre s y empezaremos observando el caso $s = 1$ dado en (3.5.22). Suponemos que $s > 1$ y la fórmula correspondiente a (3.5.23) establecida para el caso de sistema de multiplicidad posee $s-1$ miembros. El objetivo de la primera parte de la prueba es para verificar que, sin la pérdida de generalidad, se imponen condiciones extras que $0 :_E \gamma_1$ es el submódulo cero de E. Una vez hecho esto se procede al argumento y su conclusión.
Sea $F = E(0 :_E \gamma_1^p)$, donde p se escoge suficientemente grande para asegurar que $0 :_F \gamma_1 = 0$. Esto es posible por el Lema 20. Se sigue, de la sucesión exacta

$$0 \to 0 :_E \gamma_1^p \to E \to F \to 0$$

y de la proposición 22, que

$$e_R(\gamma_1, \gamma_2, ..., \gamma_s)|E = e_R(\gamma_1, \gamma_2, ..., \gamma_s|F) \tag{3.5.24}$$

luego, del isomorfismo

$$F/(\gamma_1^{n_1}F + ... + \gamma_s^{n_s}F) \approx E/((0 :_E \gamma_1^p)) + \gamma_1^{n_1}E + ... + \gamma_s^{n_s}E$$

deducimos que

$$\begin{aligned} 0 \quad &\leq L_R\left\{E/(\gamma_1^{n_1}E + ... + \gamma_s^{n_s}E)\right\} - L_R\left\{F/(\gamma_1^{n_1}F + ... + \gamma_s^{n_s}F)\right\} \\ &= L_R\left\{((0 :_E \gamma_1^p) + \gamma_1^{n_1}E + ... + \gamma_s^{n_s}E)/(\gamma_1^{n_1}E + ... + \gamma_s^{n_s}E)\right\} \\ &= L_R\left\{(0 :_E \gamma_1^p)/((0 :_E \gamma_1^p) \cap (\gamma_1^{n_1}E + ... + \gamma_s^{n_s}E))\right\} \end{aligned}$$

por uno de nuestros teorema de isomorfismo normal. Nuevamente

$$(0 :_E \gamma_1^p) \cap (\gamma_1^{n_1}E + ... + \gamma_s^{n_s}E) \supseteq \gamma_2^{n_2}(0 :_E \gamma_1^p) + ... + \gamma_s^{n_s}(0 :_E \gamma_1^p)$$

y así, por la proposición 19,
$L_R\left\{(0 :_E \gamma_1^p)/((0 :_E \gamma_1^p) \cap (\gamma_1^{n_1}E + ... + \gamma_s^{n_s}E))\right\}$

$$\begin{aligned} &\leq n_2 n_3 ... n_s L_R\left\{(0 :_E \gamma_1^p)/(\gamma_2(0 :_E \gamma_1^p) + ... + \gamma_s(0 :_E \gamma_1^p))\right\} \\ &= n_2 n_3 ... n_s C \end{aligned}$$

ahora C es finito. Para ver esto es suficiente probar que $\gamma_2, \gamma_3, ..., \gamma_s$ es un sistema de multiplicidad sobre $0 :_E \gamma_1^p$. Sin embargo es claro porque $\gamma_1^p, \gamma_2, ..., \gamma_s$ es seguro un sistema de multiplicidad sobre el módulo en cuestión y $\gamma_1^p(0 :_E \gamma_1^p) = 0$.
Estas observaciones varias prueban que tenemos la desigualdad

$$0 \leq \frac{L_R\left\{E/(\gamma_1^{n_1}E + ... + \gamma_s^{n_s}E)\right\} - L_R\left\{F/(\gamma_1^{n_1}F + ... + \gamma_s^{n_s}F)\right\}}{n_1 n_2 ... n_s} \leq \frac{C}{n_1}$$

y así, por (3.5.24), es suficiente probar que

$$\lim_{min(n_i)\to\infty} \frac{L_R\left\{F/(\gamma_1^{n_1}F + ... + \gamma_s^{n_s}F)\right\}}{n_1 n_2 ... n_s} = e_R(\gamma_1, ..., \gamma_s|F)$$

en vista de esto es permisible asumir, para el resto de la prueba, que la condición adicional $0 :_E \gamma_1 = 0$ se satisface. Sea $\bar{E} = E/\gamma_1 E$. Entonces, por el Cor. 21 del Teorema 39 y la Proposición 19,

$$\begin{aligned} 0 \quad & \leq n_1 n_2 ... n_s e_R(\gamma_1, \gamma_2, ..., \gamma_s|E) \\ & \leq L_R\left\{E/(\gamma_1^{n_1}E + ... + \gamma_s^{n_s}E)\right\} \\ & \leq n_1 L_R\left\{E/(\gamma_1 E + \gamma_2^{n_2}E + ... + \gamma_s^{n_s}E)\right\} \\ & = n_1 L_R\left\{\bar{E}/\gamma_1\bar{E} + \gamma_2^{n_2}\bar{E} + ... + \gamma_s^{n_s}\bar{E}\right\} \end{aligned}$$

porque $E/(\gamma_1 E + \gamma_2^{n_2}E + ... + \gamma_s^{n_s}E)$ y $\bar{E}/(\gamma_2^{n_2}\bar{E} + ... + \gamma_s^{n_s}\bar{E})$ son isomorfismos. Por consiguiente

$$\frac{L_R\left\{E/(\gamma_1^{n_1}E + ... + \gamma_s^{n_s}E)\right\}}{n_1 n_2 ... n_s}$$

situación entre $e_R(\gamma_1, ..., \gamma_s|E)$ y

$$\frac{L_R\left\{\bar{E}/(\gamma_2^{n_2}\bar{E} + ... + \gamma_s^{n_s}\bar{E})\right\}}{n_2 n_3 ... n_s}$$

sin embargo nuestra hipótesis inductiva nos permite concluir que esta última expresión tiende a $e_R(\gamma_2, ..., \gamma_s|\bar{E})$ y esto es igual a $e_R(\gamma_1, \gamma_2, ..., \gamma_s|E)$ porque ahora tenemos $0 :_E \gamma_1 = 0$. El teorema resulta.||

3.6. La función de Hilbert

Se establecieron anteriormente dos expresiones para $e_R(\gamma_1, \gamma_2, ..., \gamma_s|E)$ como un límite que juegan roles importantes en el desarrollo histórico de nuestra materia. Uno de estos límites fórmulados ahora se deriva.
El segundo tiene asociatividad cercana con la teoría aritmética de grado de módulos. En esta sección se estableceran algunos de los hechos básicos de esta teoría en orden para aplicar los últimos.
Además tenemos un anillo de grado (pero no necesariamente conmutativo), es posible definir la noción de un *módulo de grado* sobre el anillo exacto como antes.
El anillo de grado que tratamos son anillos polinomiales. Para ser completamente explicito, sea R un anillo no nulo y formamos el anillo polinomial

$R[X_1, X_2, ..., X_s]$ en los indeterminates $X_1, X_2, ..., X_s$, donde $s \geq 0$. Es implícito que los X_i son conmutativos con los otros así que, con una misma notación explicativa,

$$(rX_1^{\mu_1}X_2^{\mu_2}..., X_s^{\mu_s})(\rho X_1^{v_1}X_2^{v_2}..., X_s^{v_s}) = (r\rho)X_1^{\mu_1+v_1}X_2^{\mu_2+v_2}..., X_s^{\mu_s+v_s}$$

de esta manera $X_1, X_2, ..., X_s$ todos pertenecen al *centro* de $R[X_1, X_2, ..., X_s]$. Consideraremos $R[X_1, X_2, ..., X_s]$ como grado, el camino usual, por los enteros no negativos. Por consiguiente si $m \geq 0$ es un entero, entonces un polinomio es *homogéneo de grado* m si puede ser expresado en la forma

$$\sum_{\mu_1+...+\mu_s=m} r_{\mu_1\mu_2...\mu_s}X_1^{\mu_1}X_2^{\mu_2}..., X_s^{\mu_s}$$

a menudo es conveniente usar $R[X]$ como una abreviación para $R[X_1, X_2, ..., X_s]$. Cuando $s = 0$, $R[X]$ es justamente R mismo y el grado sobre R es el único trivial, i.e. todos los elementos no cero son homogéneos de grado cero. Considerando que M es un grado $R[X]$-módulo. Entonces, para cada $n \geq 0$, el elemento homogéneo de M de grado n forma un subgrupo M_n del grupo aditivo de M y tenemos

$$M = M_0 \oplus M_1 \oplus ... \oplus M_n \oplus ...$$

además, si un elemento de M_n es multiplicado por un polinomio homogéneo de grado m, entonces el resultado pertenece a M_{m+n}. Ahora el polinomio homogéneo de grado cero forma un subanillo de $R[X]$ que naturalmente identificamos con R.
Sobre esto implícito, cada M_N es un R-módulo. Sea

$$H(n, M) = L_R(M_n) \tag{3.6.25}$$

entonces $H(n, M)$ es una función de grado n, para $n = 0, 1, 2, ...$ y su valor es algún entero no negativo o “más infinito”.

Definición 35. *La función aritmética $H(n, M)$ es llamada la “función Hilbert” del grado $R[X]$-módulo M.*

Desde el punto de vista de la teoría de multiplicidad, no es $H(n, M)$ que nos interese más sino la función relación

$$H^*(n, M) = H(0, M) + H(1, M) + ... + H(n, M) \tag{3.6.26}$$

nos remitimos a $H^*(n, M)$ como la *función de Hilbert acumulativa de* M. Antes empezaremos el estudio de esta función.

Para este fin sea M un grado $R[X]$-módulo y N un $R[X]$-submódulo de M. Recordaremos que N es llamado un *submódulo homogéneo* si puede ser generado por elementos homogéneos. (Una definicion equivalente: se dice en cualquier u que pertenece a N entonces todos los componentes homogéneos de u también pertenecen a N.) Suponiendo que se tiene dicha situación. Entonces el grado en M induce un grado en N, y M/N puede también ser considerado como un grado $R[X]$-módulos en un camino natural.
Estos grados son tal que en la sucesión exacta usual

$$0 \to N \to M \to M/N \to 0 \tag{3.6.27}$$

el mapeo preserva el grado, que se dice un elemento homogéneo es algún mapeo en un elemento homogéneo, de el *mismo grado*. De ello resuta para cada entero $n \geq 0$, (3.6.27) dado aumentado a una sucesión exacta

$$0 \to N_n \to M_n \to (M/N)_n \to 0$$

de R-módulos. Por consiguiente $L_R(M_n) = L_R(N_n) + L_R((M/N)_n)$, que se dirá

$$H(n, M) = H(n, N) + H(n, M/N). \tag{3.6.28}$$

Más general, si

$$0 \to N \to M \to K \to 0$$

es una sucesión exacta de grado $R[X]$-módulo en que el mapeo preserva el grado, entonces

$$H(n, M) = H(n, N) + H(n, K) \tag{3.6.29}$$

para todo $n \geq 0$ y por ello

$$H^*(n, M) = H^*(n, N) + H^*(n, K) \tag{3.6.30}$$

para todo $n \geq 0$, donde los módulos son ambos finitamente generados y tienen una función de Hilbert que nunca es infinita.

Definición 36. *Un grado $R[X]$-módulo M será llamado “$R[X]$-módulo de Hilbert” si M es finitamente generado y $H(n, M) < \infty$ para todo $n \geq 0$.*

Sea M una $R[X]$-módulo de Hilbert y supongamos que u es un elemento de M que es homogéneo de grado p. Entonces $Ru \subseteq M_p$ y por ello

$$L_R(Ru) \leq L_R(M_p) = H(p, M) < \infty.$$

Sea I el núcleo del R-epimorfismo $R \to Ru$ en que $r \to ru$.
Entonces R/I es isomorfo a Ru y por ello $L_R(R/I) < \infty$.

En particular vemos que R/I es un R-módulo Notheriano. El $R[X]$-módulo $(R/I)[X]$, que consiste de todo polinomio en $X_1, X_2, ..., X_s$ con coeficientes en el módulo R/I, es también Noetheriano.
Si $\phi(X)$ pertenece a $R[X]$, sea $\bar{\phi}(X)$ denota el elemento de $(R/I)[X]$ obtenido por aplicar el mapeo natural $R \to R/I$ para los coeficientes de $\phi(X)$.
Fácilmente se comprueba que existe un $R[X]$-epimorfismo bien definido

$$(R/I)[X] \to R[X]u$$

en que $\bar{\phi}(X) \to \phi(X)u$.
Puesto que $(R/I)[X]$ es un $R[X]$-módulo Noetheriano, resulta que $R[X]u$ es un $R[X]$-módulo Noetheriano como bien.
Sea $U = R[X]u$. Entonces

$$U = U_p \oplus U_{p+1} \oplus U_{p+2} \oplus ...,$$

donde $U_p = Ru$, y

$$X_1U + X_2U + ... + X_sU = U_{p+1} \oplus U_{P+2} \oplus ...$$

esto prueba que $L_R\{U/(X_1U + ... + X_sU)\} = L_R\{U_p\} = L_R\{Ru\} < \infty$ y así $X_1, X_2, ..., X_s$ *es un sistema de multiplicidad sobre* $R[X]u$. Ahora estamos listos para probar:

Proposición 23. *Sea M un $R[X]$-módulo de Hilbert. Entonces M es $R[X]$-módulo Noetheriano y $X_1, X_2, ..., X_s$ es un sistema de multiplicidad sobre M.*

Prueba. Puesto que M es un $R[X]$-módulo de Hilbert, es finitamente generado. Sea $M = R[X]u_1 + R[X]u_2 + ... + R[X]u_q$
entonces es claro que podemos ordenar para que cada u_i sea homogéneo. De la observación hecha arriba, ahora resulta que, para $1 \leq i \leq q$, $R[X]u_i$ es un $R[X]$-módulo Noetheriano. Por consiguiente M es un $R[X]$-módulo Noetheriano. También sabemos, de la discusión previa, que $X_1, X_2, ..., X_s$ es un sistema de multiplicidad sobre cada submódulo $R[X]u_1, R[X]u_2, ...R[X]u_q$. Por ello resulta, que $X_1, X_2..., X_s$ es un sistema de multiplicidad sobre M. Esto establece la Proposición. ||

Corolario 27. *Sea N un submódulo homogéneo de un $R[X]$-módulo de Hilbert M. Entonces N y M/N, cuando dota con el grado usual, son también un $R[X]$-módulo de Hilbert.*

Prueba. La descomposición prueba que M es un $R[X]$-módulo Noetheriano. Por consiguiente ambos N y M/N son finitamente generados. Luego, puesto que $H(n, M) < \infty$, se sigue, de (3.6.28), que $H(n, M)$ y $H(n, M/N)$ son también finitos para todo n. Esto completa la prueba. ||

El siguiente lema trata acerca de la función de Hilbert de un módulo en el caso donde el número de variables es cero.

Lema 21. *Sea M un $R[X]$-módulo de Hilbert y supongamos que $s = 0$. Entonces $H(n, M) = 0$ para todo valor grande de n. Además $L_R(M)$ es finito y*
$H^*(n, M) = L_R(M)$ para todo valor grande de n.

Prueba. Puesto que M es finitamente generado y $s = 0$, existen elementos homogéneos $u_1, u_2, ..., u_q$ tal que $M = Ru_1 + Ru_2 + ... + Ru_q$.
Sea de grado de u_i n_i.. Entonces

$$Ru_i \subseteq M_{n_i}$$

y

$$L_R(Ru_i) \leq H(n_i, M)$$

que es finito. De ello resulta que $L_R(M) < \infty$. Pero

$$M = M_0 \oplus M_1 \oplus M_2 \oplus ...$$

es una suma directa de R-módulos. Consecuentemente, puesto que M tiene longitud finita, $L_R(M_n) = 0$ donde n es suficientemente grande, digamos cuando $n > p$. Por consiguiente $M_n = 0$ cuando $n > p$ y así

$$M = M_0 \oplus M_1 \oplus ... \oplus M_p.$$

de ello resulta que

$$\begin{aligned} H^*(n, M) \quad &= L_R(M_0) + L_R(M_1) + ... + L_R(M_n) \\ &= L_R(M_0) + L_R(M_1) + ... + L_R(M_p) \\ &= L_R(M) \end{aligned}$$

Simpre que $n > p$. Esto completa la prueba. ||

Teorema 43. *Sea M un $R[X_1, X_2, ..., X_s]$-módulo de Hilbert. Entonces para todo valor grande de n, $H(n, M)$ es dado por una relación de la forma*

$$H(n, M) = \sum_{v=0}^{s-1} C_v \binom{n+v}{v} \tag{3.6.31}$$

donde $c_0, c_1, ..., c_{s-1}$ son enteros que son independientes de n.

Observación 7. *Este es el resultado clave con respecto a la función de Hilbert. Antes de proceder a la prueba hacemos una observación un poco general.*
Primero $\binom{n+v}{v}$ *denota el binomio usual de coeficiente. Es dado explícitamente por* $\binom{n+v}{v} = \dfrac{(n+v)(n+v-1)...(n+1)}{1 \cdot 2 \cdot 3...v}$ *así, para un valor fijo* v $(v \geq 0)$, $\binom{n+v}{v}$ *es un polinomio en* n *de grado* v *del cual el primer término es* $n^v/v!$. *El teorema por tanto prueba que, para valores grandes de* n,

$$H(n, M) = c_{s-1}\frac{n^{s-1}}{(s-1)!} + ...$$

donde, en esta ecuación, el término indicado por $+...$ *constituye un polinomio en* n, *del cual el grado es menor que* $s-1$. *El siguiente punto que requiere atención es que la representación (3.6.31) es necesariamente única. Para ver esto primero observamos que si* $f(t)$ *es un polinomio (con coeficientes complejos) en una indeterminante* t *y* $f(n) = 0$ *cuando* n *es un entero positivo suficientemente grande entonces* $f(t)$ *es un polinomio nulo.*
Es porque un polinomio no nulo tiene en la mayoría un número finito de base.
Ahora supongamos que

$$c_0^{'}, c_1^{'}, ..., c_q^{'} \text{ y } c_0^{''}, c_1^{''}, ..., c_q^{''}$$

son dos sucesiones y cada una consiste de $q+1$ *términos complejos, y además supongamos que*

$$\sum_{v=0}^{q} c_v^{'}\binom{n+v}{v} = \sum_{v=0}^{q} c_v^{''}\binom{n+v}{v} \tag{3.6.32}$$

para todo entero positivo suficientemente grande n. *Podemos reescibir entonces cada lado como un polinomio en* n. *Sin embargo, hacemos esto, entonces la observación justamente hecha prueba que los dos polinomios así obtenidos tienen idénticos coeficientes. Esto a su vez implica que*

$$c_i^{'} = c_i^{''} \text{ para } i = 0, 1, 2..., q.$$

De ésta manera (3.6.32) se puede sólo tener para todo n *grande si la sucesión*

$$c_0^{'}, c_1^{'}, ..., c_q^{'} \text{ y } c_0^{''}, c_1^{''}, ..., c_q^{''}$$

son idénticas. Esto prueba que, siempre que una representación de la forma (3.6.31) es posible, debe ser unica.

De la prueba del Teorema 43, requerimos dos propiedades muy conocidas de coeficientes binomial. La primera de estas es la relación

$$\binom{n+v}{v} - \binom{n+v-1}{v-1} = \binom{n-1+v}{v} \tag{3.6.33}$$

que es valida siempre que $n \geq 1$ y $v \geq 1$. La segunda es

$$\sum_{k=0}^{n} \binom{k+v}{v} = \binom{n+v+1}{v+1} \tag{3.6.34}$$

esta dado para $n \geq 0$ y $v \geq 0$ y puede ser establecido aplicando el teorema binomial para la identidad

$$\frac{t}{1-t} + \frac{t}{(1-t)^2} + ... + \frac{t}{(1-t)^{n+1}} \equiv \frac{t}{(1-t)^{n+1}} - 1$$

Prueba del teorema 43. El argumento requiere inducción sobre el número s de indeterminantes y empezaremos por observar que el Lema 21 prueba que el teorema es verdadero cuando $s = 0$, siempre que hacemos el convenio natural con respecto a sumas vacías. Por consiguiente ahora en esto asumimos que $s \geq 1$ y que el resultado en cuestión es establecido para módulos Hilbert sobre anillos polinomiales en $s - 1$ indefinidos. Consideremos la sucesión exacta

$$0 \to 0 :_M X_s \to M \to M \to M/X_sM \to 0 \tag{3.6.35}$$

donde el mapeo $M \to M$ consiste en multiplicar los elementos de M por X_s. Es claro que $0 :_M X_s$ y X_sM, son submódulos homogéneos de M y por ello $0 :_M X_s$ y M/X_sM tienen grado natural derivado de el grado dado sobre M. Son comprensivos ambos

$$(0 :_M X_s) \to M \text{ y } M \to M/X_sM$$

preserva el grado cuando se aplican elementos homogéneos por unidad porque debemos multiplicar por X_s. Por contraste, el mapeo $M \to M$ aumenta el grado de un elemento homogéneo. De aquí para cada $n \geq 0$ tenemos una sucesión exacta

$$0 \to (0 :_M X_s)_{n-1} \to M_{n-1} \to M_n \to (M/X_sM)_n \to 0$$

de R-módulos siempre que interpretemos $(0 :_M X_s)_{n-1}$ y M_{n-1} como módulos cuando $n = 0$. Ahora todos estos R-módulos tienen longuitud finita. Por consiguiente

$$L_R\{(M/X_sM)_n\} - L_R\{(0 :_M X_s)_{n-1}\} = H(n, M) - H(n-1, M) \tag{3.6.36}$$

es comprensivo que $H(n-1,M)$ se toma como cero cuando $n=0$. Por la proposición 23. Ambos M/X_sM y $0:_M X_s$ son $R[X_1,X_2,...,X_s]$-módulos de Hilbert. Sin embargo ambos son aniquilados por X_s. De ello resulta que los considerados como $R[X_1,X_2,...,X_{s-1}]$-módulos y mantiene el grado igual, entonces serán ambos módulos de Hilbert sobre los anillos pequeños que, notamos, es un anillo polinomial en sólo $s-1$ variables. Por consiguiente, por nuestra suposición, temenos

$$L_R\left\{(M/X_SM)_n\right\} = \sum_{v=0}^{s-2} a_v \binom{n+v}{v} \qquad (n \text{ grande})$$

y

$$L_R\left\{(0:_M /X_S)_n\right\} = \sum_{v=0}^{s-2} b_v \binom{n+v}{v} \qquad (n \text{ grande})$$

donde los a_v y b_v son enteros que son independientes de n. Luego, usando (3.6.33), obtenenos

$$L_R\left\{(0:_M /X_s)_{n-1}\right\} = b_0 + \sum_{v=1}^{s-2} b_v \left[\binom{n+v}{v} - \binom{n+v-1}{v-1}\right]$$

para valores grandes de n. Si ahora sustituimos por $L_R\left\{(M/X_sM)_n\right\}$ y $L_R\left\{(0:_M /X_S)_n\right\}$ en (3.6.36), encontramos que

$$H(n,M) - H(n-1,M) = \sum_{v=0}^{s-2} d_v \binom{n+v}{v} \qquad \text{n grande}$$

donde $d_0, d_1, ..., d_{s-2}$ son ciertos enteros que no dependen en n.
Por consiguiente podemos escribir, para todo valor de k $(k \geq 0)$,

$$H(k,M) - H(k-1,M) = \sum_{v=0}^{s-2} d_v \binom{k+v}{v} + w_k \tag{3.6.37}$$

donde los w_k $(k=0,1,2,...)$ son enteros que son cero en algún punto hacia adelante, digamos $w_k = 0$ cuando $k \geq p$. Finalmente supongamos que $n \geq p$ y la suma (3.6.37) sobre el rango $k = 0,1,2,...,n$. Esto produce

$$H(n,M) = \sum_{v=0}^{s-2} d_v \sum_{k=0}^{n} \binom{k+v}{v} + \sum_{k=0}^{\infty} w_k = \sum_{v=0}^{s-2} d_v \binom{n+v+1}{v+1} + \sum_{k=0}^{\infty} w_k$$

por (3.6.34). La prueba se completa. ||

Nos permite analizar este resultado. Diremos que si M es un $R[X_1, X_2, ..., X_s]$ -módulo de Hilbert, entonces existe un único entero

$$h_0(M), h_1(M), ..., h_{s-1}(M)$$

tal que

$$H(n, M) = \sum_{v=0}^{s-1} h_v(M) \binom{n+v}{v} \tag{3.6.38}$$

para todo valor grande de n. Llamaremos el entero $h_v(M)$ el *coeficiente Hilbert de* M. Luego se demuestra que

$$H(k, M) = \sum_{v=0}^{s-1} h_v(M) \binom{k+v}{v} + \mu_k \tag{3.6.39}$$

para todo $k \geq 0$, donde $\mu_0, \mu_1, \mu_2, ...$ es una sucesión de enteros con la propiedad que $\mu_k = 0$ una vez K es suficientemente grande.
Supongamos que $\mu_k = 0$ cuando $k > q$. Si ahora $n > q$ y sumamos (3.6.39) para $K = 0, 1, ..., n$, entonces encontramos que

$$H^*(n, M) = \sum_{v=0}^{s-2} h_v(M) \sum_{k=0}^{n} \binom{k+v}{v} + \sum_{k=0}^{\infty} \mu_k = \sum_{v=0}^{\infty} \mu_k + \sum_{v=0}^{s-2} h_v(M) \binom{n+v+1}{v+1}$$

por virtud de (3.6.34). De ello resulta que existe un único entero $h_0^*(M), h_1^*(M), ..., h_s^*(M)$ tal que

$$H^*(n, M) = \sum_{v=0}^{s} h_v^*(M) \binom{n+v}{v} \tag{3.6.40}$$

siempre que n es suficionesmente grande. Además $h_0(M), h_1(M), ..., h_{s-1}(M)$ son los mismos como $h_1^*(M), h_2^*(M), ..., h_s^*(M)$. En particular, cuando $s \geq 1$ tenemos

$$h_s^*(M) = h_{s-1}(M) \tag{3.6.41}$$

nos permite asumir que $s \geq 1$. Entonces (3.6.36) demuestrá que

$$H(m, M/X_sM) - H(m-1, 0 :_M X_s) = H(m, M) - H(m-1, M)$$

es verdadero para todo $m \geq 0$. Ahora asumamos sobre el rango $m = 0, 1, ..., n$ encontramos que

$$H^*(n, M/X_sM) - H^*(n-1, 0 :_M X_s) = H(n, M) \tag{3.6.42}$$

para todo n. Pero cuando n es grande cada una de estas funciones es expresada como un polinomio en n. En hecho de todo n grande

$$H^*(n, M/X_sM) = h^*_{s-1}(M/X_sM)\frac{n^{s-1}}{(s-1)!} + ... \tag{3.6.43}$$

$$H^*(n, 0 :_m X_s) = h^*_{s-1}(0 :_M X_s)\frac{n^{s-1}}{(s-1)!} + ... \tag{3.6.44}$$

$$\text{y} \qquad H(n, M) = h_{s-1}(M)\frac{n^{s-1}}{(s-1)!} + ... \tag{3.6.45}$$

donde en cada caso $+...$ denota un polinomio en n, del cual el grado es más pequeño que $s-1$. De (3.6.44) obtenemos

$$H^*(n-1, 0 :_M X_S) = h^*_{s-1}(0 :_M X_s)\frac{n^{s-1}}{(s-1)!} + ... \tag{3.6.46}$$

y (4.6.45) podemos reescribirlo como

$$H(n, M) = h^*_s(M)\frac{n^{s-1}}{(s-1)!} + ... \tag{3.6.47}$$

porque $h_{s-1}(M) = h^*_s(M)$ Nos permite usar (3.6.43), (3.6.46) y (3.6.47) para sustituir en (3.6.42). Entonces, comparando términos de grado $s-1$, obtenemos

$$h^*_s(M) = h^*_{s-1}(M/X_sM) - h^*_{s-1}(0 :_M X_s) \tag{3.6.48}$$

esto se tiene siempre que $s \geq 1$

Teorema 44. *Sea M un $R[X_1, X_2, ..., X_s]$-módulo de Hilbert. Entonces*

$$h^*_s(M) = e_{R[X]}(X_1, ..., X_s|M)$$

Prueba. Usaremos inducción sobre s. Si $s = 0$, entonces $R[X] = R$ y $e_{R[X]}(X_1, ..., X_s|M)$ es justamente $L_R(M)$. El lema 21 demuestra que $h^*_s(M)$ es también igual a $L_R(M)$ es este caso particular. Ahora asumamos que $s \geq 1$ y que también el resultado en cuestión será probado sólo cuando $s-1$ indetermintes son concernientes.
Por la proposición 23, $e_{R[X]}(X_1, ..., X_s|M)$ es definido. Ahora

$$e_{R[X]}(X_1, ..., X_{s-1}, X_s|M) = e_{R[X]}(X_1, ..., X_{s-1}|M/X_sM) - e_{R[X]}(X_1, ..., X_{s-1}|0 :_M X_s)$$

además, la clase residual del anillo $R[X]/(X_s)$ es naturalmente isomorfo al anillo polinomial $R[X_1, ..., X_s] = \Lambda$ y el isomorfismo es tal que, para $1 \leq i \leq s-1$, la imagen de X_i en $R[X]/(X_s)$ corresponde a X_i considerado como un elemento de Λ. En adiccion, el ideal (X_s) aniquila M/X_sM. Podemos por ello aplicar (3.4.8) que prueba que

$$e_{R[X]}(X_1, ..., X_{s-1}|M/X_sM) = e_\Lambda(X_1, ..., X_{s-1}|M/X_sM)$$

pero M/X_sM es un módulo de Hilbert con respecto a $R[X_1, ..., X_{s-1}] = \Lambda$ por consiguiente, por la suposición inductiva,

$$e_\Lambda(X_1, ..., X_{s-1}|M/X_sM) = h^*_{s-1}(M/X_sM)$$

y por ello $e_{R[X]}(X_1, ..., X_{s-1}|M/X_sM) = h^*_{s-1}(M/X_sM)$

similarmente podemos probar que

$$e_{R[X]}(X_1, ..., X_{s-1}|0 :_M /X_s) = h^*_{s-1}(0 :_M X_s).$$

de esta manera

$$e_{R[X]}(X_1, ..., X_{s-1}|M) = h^*_{s-1}(M/X_sM) - h^*_{s-1}(0 :_M X_s) = h^*_{s-1}(M)$$

por (3.6.48) la prueba se tiene.||

Capítulo 4

La Fórmula Límite de Samuel

Sea E un R-módulo Noetheriano y $\gamma_1, \gamma_2, ..., \gamma_s$ un sistema de multiplicidad sobre E. Sea

$$A = \gamma_1 R + \gamma_2 R + ... + \gamma_s R$$

así que A es un ideal central finitamente generado, y usamos $X_1, X_2, ..., X_s$ para denotar indeterminantes. Con un indeterminante para cada elemento del sistema de multiplicidad.
Si $n \geq 0$ es un entero, entonces $\gamma_1^n E, \gamma_2^n E, ..., \gamma_s^n E$ está contenido en $A^n E$.
Por consiguiente $L_R(E/A^n E) < \infty$ para todo n.
Sea

$$M = (E/AE) \oplus (AE/A^2E) \oplus (A^2E/A^3E) \oplus ... \tag{4.0.1}$$

afirmemos que M(ideal maximal de R) es una estructura de grado $R[X_1, ..., X_s]$-módulo en que el grupo de elementos homogéneos de grado n, es justamente $A^nE/A^{n+1}E$. Si M cumple con la $+$ (suma) y $\cdot$ (producto) de las leyes de composición interna definidas sobre un conjunto A.
Para explicar esta estructura, damos un elemento η de $A^nE/A^{n+1}E$ representado por el elemento y de A^nE y sea

$$\phi(X) = \sum_{\mu_1+...+\mu_s=m} r_{\mu_1,\mu_2,...,\mu_s} X_1^{\mu_1} X_2^{\mu_2} ... X_s^{\mu_s}$$

un elemento homogéneo de $R[X_1, ..., X_s]$ de grado m. Entonces $\phi(X)\eta$ dicho elemento de $A^{m+1}E/A^{m+n+1}E$ que es representado por

$$\sum_{\mu_1+...,\mu_s=m} r_{\mu_1,\mu_2,...,\mu_s} \gamma_1^{\mu_1} \gamma_2^{\mu_2} ... \gamma_s^{\mu_s} y$$

donde M es un grado $R[X]$-módulo, que ordena elementos homogéneos, por ser E un R-módulo Noetheriano y A un ideal de R tal que $AE \neq E$.
Puesto que E es un R-módulo Noetheriano, es finitamente generado.

Sea $E = Re_1 + Re_2 + ..., +Re_q$ y denotado por $\bar{e}_i$ la imagen natural de e_i en E/AE así que $\bar{e}_i$ es un elemento homogéneo de M de grado cero.
Entonces

$$M = R[X]\bar{e}_1 + R[X]\bar{e}_2 + ... + R[X]\bar{e}_q$$

donde, usualmente, $R[X]$ es usado como una abreviación para $R[X_1, ..., X_2]$.
Ahora

$$L_R(M_n) = L_R(A^n E/A^{n+1}E) \tag{4.0.2}$$

que es finito. Por consiguiente *cuando M es considerado como un grado $R[X]$-módulo,será llamado $R[X]$-módulo de Hilbert.* Además, por (4.0.2), $L_R(E/A^nE) = L_R(M_0) + L_R(M_2) + ... + L_R(M_{n-1})$ eso se dira

$$L_R(E/A^nE) = H^*(n-1, M) \tag{4.0.3}$$

de aquí que, por [

Fórmula 1. $H^*(n, M) = \sum_{v=0}^{s} h_v^*(M)\binom{n+v}{v}$],

una vez n puede volverse suficientemente grande, $L_R(E/A^nE)$ es igual a un polinomio en n de grado no excediendo s.
Efectivamente [

Fórmula 2. $H^*(n, M) = \sum_{v=0}^{s} h_v^*(M)\binom{n+v}{v}$]

prueba que, para n grande,

$$L_R(E/A^nE) = h_s^*(M)\frac{n^s}{s!} + ..., \tag{4.0.4}$$

donde este calculo +... denota un polinomio de grado n, el cual es menor que s. Sea

$$e(s, A, E) = \lim_{n\to\infty} \frac{L_R(E/A^nE)}{n^s/s!} = h_s^*(M) \tag{4.0.5}$$

donde $e(s, A, E)$ es realmente igual a $e_R(\gamma_1, ..., \gamma_s|E)$.
Y cuando $s = 0$ obtenemos

$$e(0, (0), E) = L_R(E) \tag{4.0.6}$$

ahora supongamos que $s \geq 1$ y sea

$$\bar{E} = E/\gamma_1 E, \bar{A} = \gamma_2 R + ... + \gamma_s R.$$

entonces $\bar{E}$ es un R-módulo Noetheriano y este admite $\gamma_2, \gamma_3, ..., \gamma_s$ como un sistema de multiplicidad.
También, porque γ_1 aniquila $\bar{E}$, $\bar{A}^n\bar{E} = A^n\bar{E}$ y por ello $\bar{E}/(\bar{A})^n\bar{E}$ es isomorfo

a $E/(\gamma_1 E + A^n E)$.
Por lo consiguiente

$$\begin{aligned} L_R\left\{\bar{E}/(\bar{A})^n\bar{E}\right\} &= L_R\left\{E/A^nE\right\} - L_R\left\{(\gamma_1 E + A^n E)/A^nE\right\} \\ &= L_R\left\{E/A^nE\right\} - L_R\left\{\gamma_1 E/(\gamma_1 E \cap A^n E)\right\} \\ &= L_R\left\{E/A^nE\right\} - L_R\left\{\gamma_1 E/\gamma_1(A^nE :_E \gamma_1)\right\} \end{aligned}$$

por [

Fórmula 3. $\gamma E \cap K = \gamma(K :_E \gamma)$].
Sin embargo, el epimorfismo $E \to \gamma_1 E$ producido por multiplicar por γ_1 es tal que la imagen inversa de $\gamma_1(A^nE :_E \gamma_1)$ es justamente $A^nE :_E \gamma_1$.
De esta manera $\gamma_1 E/\gamma_1(A^nE :_E \gamma_1)$ es isomorfo a $E/(A^nE :_E \gamma_1)$ y así

$$\begin{aligned} L_R\left\{\bar{E}/(\bar{A})^n\bar{E}\right\} &= L_R\left\{E/A^nE\right\} - L_R\left\{E/(A^nE :_E \gamma_1)\right\} \\ &\geq L_R\left\{E/A^nE\right\} - L_R\left\{E/A^{n-1}E\right\} \end{aligned}$$

porque $A^{n-1}E \subseteq (A^nE :_E \gamma_1)$. Luego, por (4.0.4) y (4.0.5),

$$L_R\left\{E/A^nE\right\} = e(s,A,E)\frac{n^s}{s!} + ... \tag{4.0.7}$$

para n grande, donde $+...$ tiene su significado usual. De ello resulta que, cuando n es grande,

$$L_R\left\{E/A^nE\right\} - L_R\left\{E/A^{n-1}E\right\} = e(s,A,E)\frac{n^{s-1}}{(s-1)!} + ...$$

y por ello

$$L_R\left\{\bar{E}/(\bar{A})^n\bar{E}\right\} \geq e(s,A,E)\frac{n^{s-1}}{(s-1)!} + ...$$

Nos permite dividir directamente por $n^{s-1}/(s-1)!$ y despues n tiende a infinito. Esto produce $e(s-1,\bar{A},\bar{E}) \geq e(s,A,E)$.
Si ocurre que $s \geq 2$, entonces el argumento anterior puede ser repetido.
En este camino obtenemos $e(s-2,\bar{\bar{A}},\bar{\bar{E}}) \geq e(s-1,\bar{A},\bar{E})$
donde $\bar{\bar{A}} = \gamma_3 R + ... + \gamma_s R$ y $\bar{\bar{E}} = \bar{E}/\gamma_2\bar{E}$. Pero, por [

Fórmula 4. $E/(K{+}\gamma E) \approx (E/K)/\gamma(E/K)$],
$\bar{\bar{E}}$ es isomorfo a $E/(\gamma_1 E + \gamma_2 E)$ y así se establece que
$e(s,A,E) \leq e(s-1,\bar{A},E/\gamma_1 E) \leq e(c-2,\bar{\bar{A}},E/(\gamma_1 E + \gamma_2 E))$.
Por lo que obtenemos

$e(s,A,E) \leq e(0(0),E/(\gamma_1 E+...+\gamma_s E)) = L_R(E/(\gamma_1 E+...+\gamma_s E))$ por (4.0.6), o , cambiando la notación,

$$\lim_{n\to\infty} \frac{L_R(E/A^nE)}{n^s/s!} \leq L_R(E/(\gamma_1 E+...+\gamma_s E))$$

en esta relación ahora reemplazamos $\gamma_1,\gamma_2,...\gamma_s$ por $\gamma_1^p,\gamma_2^p,...\gamma_s^p$, donde p es un entero positivo arbitrario, y observamos, al mismo tiempo, que

$$(\gamma_1^p R,...\gamma_s^p R)^n E \subseteq (\gamma_1 R,...\gamma_s R)^{np} E$$

esto prueba que

$$\begin{aligned} \lim_{n\to\infty} \frac{L_R\left\{E/(\gamma_1 R+...+\gamma_s R)^{np}E\right\}}{(np)^s/s!} &\leq \lim_{n\to\infty} \frac{L_R\left\{E/(\gamma_1^p R+...+\gamma_s^p R)^{n}E\right\}}{(np)^s/s!} \\ &\leq \frac{L_R\left\{E/(\gamma_1^p E+...+\gamma_s^p E)\right\}}{p^s} \end{aligned}$$

pero el primero de estos límites es $e(s,A,E)$. De donde

$$e(s,A,E) \leq \frac{L_R\left\{E/(\gamma_1^p E+...+\gamma_s^p E)\right\}}{p^s}$$

ahora si p tiende a infinito y aplicando el Teorema:[

Teorema 45. *Sea E un R-módulo Noetheriano y $\gamma_1,\gamma_2,...,\gamma_s$ un sistema de multiplicidad sobre E. Entonces*

$$\lim_{min(n_i)\to\infty} \frac{L_R\left\{E/(\gamma_1^{n_1}E+...+\gamma_s^{n_s}E)\right\}}{n_1 n_2 ... n_s} = e_R(\gamma_1,...,\gamma_s|E) \tag{4.0.8}$$

]. Esto produce

$$e(s,A,E) \leq e_R(\gamma_1,...,\gamma_s|E) \tag{4.0.9}$$

el resto nos establece la desigualdad opuesta. Para este fin sea $n_1,n_2,...,n_s$ enteros positivos y sea

$$U = \oplus_{n=0}^{\infty}\left\{(A^nE\cap(A^{n+1}E+\gamma_1^{n_1}E+...+\gamma_s^{n_s}E))/A^{n+1}E\right\}$$

es fácil comprobar que U es un $R[X]$-submódulo homogéneo de M por(4.0.1) y que $X_1^{n_1}M+X_2^{n_2}M+...+X_s^{n_s}M\subseteq U$. Por lo consiguiente

$$L_R\left\{M/(X_1^{n_1}M+X_2^{n_2}M+...+X_s^{n_s}M)\right\} \geq L_R\left\{M/U\right\} \tag{4.0.10}$$

Sea $F=\gamma_1^{n_1}E+\gamma_2^{n_2}E+...+\gamma_s^{n_s}E$. Entonces tenemos un isomorfismo

$$M/U \approx \oplus_{n=0}^{\infty}\left\{A^nE/(A^nE\cap(A^{n+1}E+F))\right\}$$

de R-módulos. Pero

$$\begin{aligned} A^nE/(A^nE \cap (A^{n+1}E+F)) \qquad &\approx (A^nE + A^{n+1}E+F)/(A^{n+1}E+F) \\ &\approx (A^nE+F)/(A^{n+1}E+F) \end{aligned}$$

y así $M/U \approx \oplus_{n=0}^{\infty} \{(A^nE+F)/(A^{n+1}E+F)\}$.
Sin embargo, cuando $n \geq n_1+n_2+...+n_s$ tenemos $A^nE \subseteq F$ y por ello $A^nE+F=F$.
De ello resulta que:

$$L_R\{M/U\} = \sum_{n\geq 0} L_R\left\{(A^nE+F)/(A^{n+1}E+F)\right\} = L_R\{E/F\}$$

y así, por (4.0.9), $L_R\{E/(\gamma_1^{n_1}E+...+\gamma_s^{n_s}E)\} \leq L_R\{M/(X_1^{n_1}M+...+X_s^{n_s}M)\}$

El siguiente paso prueba que

$$L_R\{M/(X_1^{n_1}M+...+X_s^{n_s}M)\} = L_{R[X]}\{M/(X_1^{n_1}M+...+X_s^{n_s}M)\} \tag{4.0.11}$$

ahora

tenemos $\dfrac{L_R\{E/(\gamma_1^{n_1}E+...+\gamma_s^{n_s}E)\}}{n_1n_2...n_s} \leq \dfrac{L_{R[X]}\{M/(X_1^{n_1}M+...+X_s^{n_s}M)\}}{n_1n_2...n_s}$

se sigue, el Teorema:[

Teorema 46. *Sea E un R-módulo Noetheriano y $\gamma_1,\gamma_2,...,\gamma_s$ un sistema de multiplicidad sobre E. Entonces*

$$\lim_{min(n_i)\to\infty} \frac{L_R\{E/(\gamma_1^{n_1}E+...+\gamma_s^{n_s}E)\}}{n_1n_2...n_s} = e_R(\gamma_1,...,\gamma_s|E) \tag{4.0.12}$$

],
que $e_R(\gamma_1,...,\gamma_s|E) \leq e_{R[X]}(X_1,...,X_s|M)$.
Pero, por el Teorema:[

Teorema 47. *Sea M un $R[X_1,X_2,...,X_s]$-módulo de Hilbert. Entonces*

$$h_s^*(M) = e_{R[X]}(X_1,...,X_s|M)$$

]
y (4.0.5), $e_{R[X]}(X_1,...,X_s|M) = h_s^*(M) = e(s,A,E)$
de esta manera $e_R(\gamma_1,...,\gamma_s|E) \leq e(s,A,E)$ que, en vista de (4.0.8), conduce a:

Teorema 48. *Sea E un R-módulo Noetheriano $\gamma_1, \gamma_2, ..., \gamma_s$ un sistema de multiplicidad sobre E. Si ahora $A = \gamma_1 R + \gamma_2 R + ... + \gamma_s R$ entonces*

$$\lim_{n\to\infty} \frac{L_R\{E/A^n E\}}{n^s/s!} = e_R(\gamma_1, \gamma_2, ..., \gamma_s|E) \tag{4.0.13}$$

Además $e_R(\gamma_1, \gamma_2, ..., \gamma_s|E) = e_{R[X]}(X_1, ..., X_s|M)$ donde M es el $R[X_1, ..., X_s]$-módulo dado por (4.0.1).

Observación 8. *La expresión para $e_R(\gamma_1, \gamma_2, ..., \gamma_s|E)$ provisto por (4.0.11) es la fórmula límite de P. Samuel*

Prueba. Posteriormente sólo es necesario probar (4.0.10).
Con este fin sea I el $R[X]$-ideal generado por $X_1, X_2, ..., X_s$ y sea n un entero que satisface

$$n \geq n_1 + n_2 + ... + n_s.$$

entonces

$$I^n M \subseteq X_1^{n_1} M + ... + X_s^{n_s} M.$$

ahora
$L_R\{M/(X_1^{n_1} M + ... + X_s^{n_s} M)\} \geq L_{R[X]}\{M/(X_1^{n_1} M + ... + X_s^{n_s} M)\}$

y $L_R\{(X_1^{n_1} M + ... + X_s^{n_s} M)/I^n M\} \geq L_{R[X]}\{(X_1^{n_1} M + ... + X_s^{n_s} M)I^n M\}$

porque todo $R[X]$-módulo es también un R-módulo.
De donde el resultado deseado resulta si podemos probar que:
$L_R\{M/I^n M\} = L_{R[X]}\{M/I^n M\} < \infty$. Pero

$$L_R\{M/I^n M\} = \sum_{v=0}^{n-1} L_R\left\{I^v M/I^{v+1} M\right\}$$

$$L_{R[X]}\{M/I^n M\} = \sum_{v=0}^{n-1} L_{R[X]}\left\{I^v M/I^{v+1} M\right\}$$

y cada $X_1, X_2, ..., X_s$ aniquila $I^v M/I^{v+1} M$.
De esta manera el $R[X]$-submódulo de $I^v M/I^{v+1} M$ son los mismos como sus R-submódulos y así

$$L_R\left\{I^v M/I^{v+1} M\right\} = L_{R[X]}\left\{I^v M/I^{v+1} M\right\}$$

por consiguiente

$$L_R\{M/I^n M\} = L_{R[X]}\{M/I^n M\}$$

además la segunda expresión es finita porque, por Proposición:[

Proposición 24. *Sea M un $R[X]$-módulo de Hilbert. Entonces M es $R[X]$-módulo Noetheriano y $X_1, X_2, ..., X_s$ es un sistema de multiplicidad sobre M.*

],
$X_1, X_2, ..., X_s$ es un sistema de multiplicidad sobre M. La prueba es ahora completa.||

Como una aplicación de la fórmula límite de Samuel's probaremos

Teorema 49. *Sea E un R-módulo Noetheriano y $\gamma_1, \gamma_2, ..., \gamma_s$ y $\gamma_1', \gamma_2', ..., \gamma_s'$ sistema de multiplicidad sobre E. Supongamos que*

$$\gamma_1 E + \gamma_2 E + ... + \gamma_s E \subseteq \gamma_1' E, \gamma_2' E, ..., \gamma_s' E$$

entonces

$$e_R(\gamma_1, ..., \gamma_s | K) \geq e_R(\gamma_1^{'}, ..., \gamma_s^{'} K)$$

donde K es algún submódulo o factor módulo de E.

Prueba. Podemos asumir que $s > 0$.
Sea $\gamma_1 R, ..., \gamma_s R = A$ y $\gamma_1' R, ..., \gamma_s' R = A'$.
Entonces daremos que $AE \subseteq A'E$. De donde $A^2 E \subseteq AA'E = A'AE \subseteq A'^2 E$ y, en general, $A^n E \subseteq A'^n E$.
Por lo consiguiente

$$L_R \{E/A^n E\} \geq L_R \left\{E/A'^n E\right\}$$

y así

$$e_R(\gamma_1, ..., \gamma_s | E) \geq e_R(\gamma_1', ..., \gamma_s' | E)$$

por virtud de (4.0.11).
Ahora sea K un módulo factor de E.
Entonces de

$$\gamma_1 E + ... + \gamma_s E \subseteq \gamma_1' E + ... + \gamma_s' E$$

resulta

$$\gamma_1 K + ... + \gamma_s K \subseteq \gamma_1' K + ... + \gamma_s' K,$$

y así obtenemos

$$e_R(\gamma_1, ..., \gamma_s | K) \geq e_R(\gamma_1', ..., \gamma_s' | K)$$

por razón completemente similar a estas ya dadas.
Finalmente, supongamos que K es un submódulo de E.
Entonces, por el Teorema:[

Teorema 50. *Sea K un submódulo de un R-módulo Noetheriano E y sea A un ideal central. Entonces existe un entero $q \geq 0$ tal que:*

$$A^n E \cap K = A^{n-q}(A^q E \cap K)$$

para todo $n \geq q$],
existe un entero $q \geq 0$ tal que $A'(A'^q E \cap K) = A'^{q+1} E \cap K$.
Ahora $\gamma_1^{'q}(K/(A'^q E \cap K)) = 0$.
También $\gamma_1^q(K/(A'^q E \cap K)) = 0$ porque $\gamma_1^q K \subseteq A^q E \cap K \subseteq A'^q E \cap K$.
Por lo tanto se sigue, la Proposición:[

Proposición 25. *Sea E un R-módulo Noetheriano y $\gamma_1, \gamma_2, ..., \gamma_s$ un sistema de multiplicidad sobre E.*
Asumamos que para algún valor en particular de i tenemos $\gamma_i^m E = 0$, donde m es un entero positivo.
Entonces $e_R(\gamma_1, \gamma_2, ..., \gamma_s | E) = 0$

],
que

$$e_R(\gamma_1^{'}, ..., \gamma_s^{'} | K) = e_R(\gamma_1^{'}, ..., \gamma_s^{'} | A'^q E \cap K) \tag{4.0.14}$$

y

$$e_R(\gamma_1, ..., \gamma_s | K) = e_R(\gamma_1, ..., \gamma_s | A'^q E \cap K) \tag{4.0.15}$$

luego

$$A(A'^q E \cap K) \subseteq AA'^q E \cap K = A'^q AE \cap K \subseteq A'^{q+1} E \cap K = A'(A'^q E \cap K)$$

y por ello

$$\gamma_1(A'^q E \cap K) + ... + \gamma_s(A'^q E \cap K) \subseteq \gamma_1^{'}(A'^q E \cap K) + ... + \gamma_s^{'}(A'^q E \cap K).$$

Por lo consiguiente

$$e_R(\gamma_1, ..., \gamma_s | A'^q E \cap K) \geq e_R(\gamma_1^{'}, ..., \gamma_s^{'} | A'^q E \cap K)$$

por el caso ya considerado. Finalmente

$$e_R(\gamma_1, ..., \gamma_s | K) \geq e_R(\gamma_1^{'}, ..., \gamma_s^{'} | K)$$

por (4.0.12) y (4.0.13). Se completa la prueba. ||

Parte II

Bibliografía

Bibliografía

[1] Introductión Commutative Algebra M.F.ATIYAH,FRS/ university of oxford.

[2] Historía de las Ideas Modernas en Matemática, Programa Regional de Desarrollo Científico y Tecnológico Departamento de Asuntos Científicos Secretaria General de la Organización de los Estados Americanos Washington, D.C.

[3] Estructuras Algebraicas, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, Argentina.

[4] Estructuras Algebraicas I, Por Artibano Micali Institut de Mathématiques Universite de Montpellier II, FRANCIA.

[5] Estructuras Algebraicas II, Por Artibano Micali Institut de Mathématiques Universite de Montpellier II, FRANCIA.

[6] Estructuras Algebraicas III, Por Artibano Micali Institut de Mathématiques Universite de Montpellier II, FRANCIA.

[7] Estructuras Algebraicas IV, Por Artibano Micali Institut de Mathématiques Universite de Montpellier II, FRANCIA.

[8] Estructuras Algebraicas V, Por Artibano Micali Institut de Mathématiques Universite de Montpellier II, FRANCIA.

[9] Estructuras Algebraicas VI, Por Artibano Micali Institut de Mathématiques Universite de Montpellier II, FRANCIA.

[10] Estructuras Algebraicas VII, Por Artibano Micali Institut de Mathématiques Universite de Montpellier II, FRANCIA.

[11] Álgebra Homológica y Álgebra Conmutativa, Carlos Ivorra Castillo.

[12] Multiplicidades Algebraicas y Teoría de Bifurcación, Memoria Presentada Para Optar al Grado de Doctor Por: Carlos Mora Corral, Madrid, 2004.

[13] Algebra Commutativa , Northcot.

[14] Northcott, D. G., An Introduction to Homological Algebra, Cambridge University Press, Londres, 1960.

[15] Northcott, D. G., Lessons on Rings, Modules and Multiplicities, Cambridge University Press, Londres, 1968.

[16] Obtenido"http://es.wikipedia.org/wiki/HomologCategoría: Topología algebraica.

[17] Hilton, P. J., y S. Wylie, Homology Theory, Cambridge University Press, Londres, 1960.

[18] Jans, J. P., Rings and Homology, Holt, Rinehart, y Winston, Nueva York, 1964.

[19] MacLane, S., Homology, Academic Press, Nueva York, 1963.

[20] Spanier, E.H., Algebra Topology, McGraw-Hill, Nueva York, 1966.

[21] Sze-Tsen Hu .Introduction to Homological Algebra. Holden-Day, San Francisco California,1974.

[22] BOURBAKI, N. Algébre Commutative, Chap. X: profondeur, dualité, Masson, 1998.

[23] EISENBUD, D. Commutative Algebra with a view toward Algebraic Geometry. Springer,1995.

[24] GIRAL, J. M. Anillos locales regulares, teoría del grado, anillos de Cohen-Macaulay. UB, 1995.

[25] ZARISKI, O., SAMUEL, P., Commutative Algebra, vol. I, II, Van Nostrand, 1960: Springer, 1975.