Departamento de Matemáticas, Facultad de Ciencias
Universidad Autónoma de Madrid

Descomposición primaria de ideales monomiales en anillos noetherianos

Trabajo de fin de grado

Grado en Matemáticas

Autor: Alejandro Arias Gómez

Tutor: María de la Paz Tirado Hernández

Curso 2024-2025

Resumen

El objetivo principal de este trabajo es estudiar la descomposición primaria en el caso particular de los ideales monomiales, obteniendo descomposiciones explícitas y analizando su estructura, estudiando sus descomposiciones m-irreducibles. Este tipo de ideales, generados por monomios, permiten un tratamiento más accesible, lo que los convierte en un recurso idóneo para explorar una variedad de conceptos del álgebra conmutativa.

Tras una primera parte dedicada a introducir las nociones básicas necesarias —como los ideales primos, maximales, radicales y primarios—, se desarrolla la teoría general de la descomposición primaria, incluyendo resultados esenciales como el primer teorema de unicidad y el teorema de Lasker-Noether. Posteriormente, se analiza el caso específico de los ideales monomiales, donde propiedades como la m-irreducibilidad y la relación entre los exponentes de los monomios permiten obtener descomposiciones constructivas de manera explícita. A lo largo del trabajo se presentan ejemplos ilustrativos que permiten comprender con mayor claridad el funcionamiento de la descomposición primaria.

Abstract

The main objective of this thesis is to study primary decomposition in the particular case of monomial ideals, by obtaining explicit decompositions and analyzing their structure through their m-irreducible decompositions. These ideals, generated by monomials, allow for a more accessible treatment, making them an ideal tool for exploring a variety of concepts in commutative algebra.

After a first section introducing the basic notions—such as prime, maximal, radical, and primary ideals—the general theory of primary decomposition is developed, including fundamental results like the first uniqueness theorem and the Lasker–Noether theorem. The focus then shifts to the specific case of monomial ideals, where properties such as m-irreducibility and the relationship between the exponents of the monomials allow for the explicit construction of primary decompositions. Throughout the thesis, illustrative examples are provided to aid in understanding the workings of primary decomposition.

Índice general

Introducción

Uno de los temas recurrentes en matemáticas es el estudio de descomposiciones: representar un objeto como combinación o intersección de otros más simples, pero con ciertas propiedades especiales. Un ejemplo es el teorema fundamental de la aritmética, que afirma que todo número entero positivo se puede escribir de manera única (salvo reordenación) como producto de potencias de números primos. Encontramos un fenómeno análogo en geometría algebraica, ya que, si K es un cuerpo algebraicamente cerrado, entonces cualquier conjunto algebraico $V(\mathfrak{a}) \subset K^d$, es decir, el conjunto de ceros comunes de un ideal $\mathfrak{a} \subset K[x_1, ..., x_d]$, puede descomponerse como unión finita de variedades afines irreducibles:

$$V(\mathfrak{a}) = V(\mathfrak{p}_1) \cup ... \cup V(\mathfrak{p}_m)$$

donde cada $\mathfrak{p}_i$ es un ideal primo. Además, en este caso, el teorema de los ceros de Hilbert dice que el ideal formado por todos los polinomios que se anulan en todos los puntos de $V(\mathfrak{a})$, $I(V(\mathfrak{a}))$, coincide con su radical $r(\mathfrak{a})$. Por otro lado, dado que $I(V(\mathfrak{p}_i)) = r(\mathfrak{p}_i) = \mathfrak{p}_i$, se concluye que

$$r(\mathfrak{a}) = \mathfrak{p}_1 \cap ... \cap \mathfrak{p}_m$$

por lo que todo ideal radical de $K[x_1, ..., x_d]$, es decir, todo ideal que coincide con su radical, se puede expresar como una intersección de ideales primos. Esta correspondencia entre conjuntos algebraicos e ideales radicales permite entender la estructura de $V(\mathfrak{a})$ a través del ideal $\mathfrak{a}$ (ver [2, Ch. 1]).

En álgebra conmutativa, podemos plantearnos una pregunta análoga: ¿es posible descomponer todo ideal en un anillo conmutativo en términos de otros ideales 'con buenas propiedades'? A la luz del ejemplo geométrico anterior, una respuesta natural sería considerar a los ideales primos como esos bloques fundamentales, pues hemos visto que todo ideal radical de $K[x_1, ..., x_d]$ se puede expresar como intersección de ideales primos. Sin embargo, este razonamiento encuentra rápidamente una limitación. Por ejemplo, en el anillo $K[x]$, donde K es un cuerpo, el ideal $\langle x^n \rangle$, con $n > 1$, no puede escribirse como intersección de ideales primos, ya que el único ideal primo que lo contiene es $\langle x \rangle$, pero claramente $\langle x^n \rangle \neq \langle x \rangle$. Este tipo de situaciones muestra que la descomposición en primos resulta insuficiente para describir la estructura de todos los ideales. Para superar esta limitación, se introduce el concepto de ideal primario, que generaliza al de ideal primo y permite establecer una teoría de descomposición más completa.

El concepto de ideal primario fue introducido por Emanuel Lasker en 1905 (ver [8]), con el objetivo de generalizar la factorización de los enteros al contexto de los ideales en anillos conmutativos. En particular, Lasker demostró que todo ideal en un anillo de polinomios sobre un cuerpo puede expresarse como una intersección finita de ideales primarios, estableciendo así una analogía con la descomposición única en potencias de primos de los números enteros. Este resultado fue generalizado por Emmy Noether en 1921 (ver [13]), quien extendió la descomposición primaria a todos los anillos noetherianos, estableciendo el conocido teorema de Lasker–Noether

(teorema 2.3.4). Este teorema puede considerarse una generalización del teorema fundamental de la aritmética, pero es de carácter meramente existencial, puesto que obtener efectivamente dicha descomposición constituye, en general, una tarea computacionalmente compleja. Este hecho motiva un interés tanto teórico como algorítmico por el estudio de descomposiciones primarias.

En este contexto, resulta especialmente interesante identificar clases de ideales en las que la descomposición primaria no solo exista, sino que pueda obtenerse de forma constructiva y eficiente. Una de las más destacadas es la de los ideales monomiales, cuyo comportamiento presenta una notable diferencia con respecto al caso general. En efecto, en el caso especial de los ideales monomiales en un dominio noetheriano $R[x_1, ..., x_d]$ la situación es mucho más accesible. Es posible calcular explícitamente su descomposición primaria mediante algoritmos constructivos, como se detalla en el algoritmo 3, utilizando únicamente los exponentes de sus generadores (ver teorema 3.4.14). Además, los ideales monomiales presentan otras ventajas significativas. Entre otras, permiten calcular de forma efectiva diversos invariantes algebraicos, como la dimensión y codimensión de un ideal (ver [4, Ch. 13]) o la resolución de Taylor (ver [10, Ch. 4]), y muchas operaciones resultan más sencillas que en el caso general. Esta simplicidad ha motivado también el desarrollo de técnicas que permiten reducir ciertos problemas sobre ideales arbitrarios al estudio de sus partes monomiales, como ocurre en el contexto de las bases de Gröbner y los ideales iniciales (ver [9]).

Más allá de su papel en el álgebra, los ideales monomiales aparecen en múltiples áreas, con diversas aplicaciones. Por ejemplo, en combinatoria algebraica, la correspondencia de Stanley–Reisner asocia a cada complejo simplicial un ideal monomial cuadrático sin cuadrados, de forma que ciertos invariantes combinatorios del complejo se reflejan en propiedades algebraicas del ideal (ver [7]). También en teoría de códigos, algunos parámetros de códigos lineales —como los pesos generalizados— pueden estudiarse a través de invariantes homológicos de ideales monomiales asociados (ver [5]). Además, en teoría de invariantes, las bases SAGBI y otros métodos constructivos recurren con frecuencia a ideales monomiales para describir subálgebras invariantes bajo acciones de grupos (ver [3]). Estas conexiones ilustran la riqueza estructural de los ideales monomiales y refuerzan la motivación para estudiar sus propiedades internas, como sus descomposiciones primarias, de manera más sistemática y constructiva.

Para concluir esta introducción, describimos brevemente la estructura del documento. El capítulo 1 presenta los conceptos básicos sobre ideales en anillos conmutativos con unidad, sentando las bases para el trabajo. En particular, se repasan las nociones de ideal primo, ideal maximal y radical de un ideal, y se establecen algunos resultados básicos. El capítulo 2 se adentra en la teoría de la descomposición primaria, primero se introduce la definición de ideal primario y se estudian las propiedades de la descomposición de un ideal en ideales primarios. Aquí se demuestra rigurosamente el teorema de Lasker–Noether, que garantiza la existencia de descomposición primaria irredundante para todo ideal en un anillo noetheriano, así como la unicidad de los primos asociados a dicha descomposición. En el capítulo 3, el último y principal de este trabajo, nos enfocamos en los ideales monomiales en anillos de polinomios. Se prueban resultados específicos que muestran cómo estos ideales pueden descomponerse y, en particular, se desarrolla un algoritmo constructivo para obtener la descomposición primaria de cualquier ideal monomial a partir de sus generadores monomiales, cuando el anillo de polinomios es un dominio noetheriano.

CAPÍTULO 1
Ideales

Uno de los principales objetos que podemos estudiar relacionados con un anillo son sus ideales. Recordamos que, dado un anillo conmutativo con elemento unidad R, un **ideal** $\mathfrak{a}$ de R es un subconjunto que, además de ser un subgrupo aditivo de $(R, +)$, satisface la propiedad de absorción: para todo $r \in R$ y $a \in \mathfrak{a}$, se tiene $ra \in \mathfrak{a}$.

En este capítulo introduciremos las nociones básicas sobre ideales en anillos conmutativos con unidad junto con algunas propiedades que serán de utilidad en los siguientes capítulos. En concreto, en la sección 1.1 veremos los ideales primos y maximales, y en la sección 1.2 abordaremos el concepto de radical de un ideal. Los resultados que aparecen en este capítulo pueden ser encontrados en [1, Ch. 1], [11, Ch. 1] y [14, Ch. 1].

A lo largo de este documento, denotaremos por R a un anillo conmutativo con elemento unidad. Además, si C es un subconjunto de R, escribiremos como $\langle C \rangle$ al ideal más pequeño que contiene a C. Este ideal coincide con la intersección de todos los ideales de R que contienen a C, y sus elementos son combinaciones lineales finitas de elementos de C con coeficientes en R. Si además $C = \{f_1, ..., f_m\}$ es un conjunto finito, entonces escribiremos directamente $\langle f_1, ..., f_m \rangle$ en vez de $\langle \{f_1, ..., f_m\} \rangle$. Por último, recordamos que la proyección canónica de R en el anillo cociente $R/\mathfrak{a}$, que denotaremos por $\pi : R \to R/\mathfrak{a}$ y lleva $a \in R$ a su clase de equivalencia $\overline{a} \in R/\mathfrak{a}$, induce una correspondencia biyectiva entre los ideales de R que contienen a $\mathfrak{a}$ y los ideales del anillo cociente. En concreto:

$$\begin{array}{ccc} \{\text{Ideales de } R \text{ que contienen a } \mathfrak{a}\} & \longleftrightarrow & \{\text{Ideales de } R/\mathfrak{a}\} \\ \mathfrak{b} & \longmapsto & \mathfrak{b}/\mathfrak{a} := \pi(\mathfrak{b}) = \{b + \mathfrak{a} \mid b \in \mathfrak{b}\} \end{array} \tag{1.1}$$

Esta correspondencia será utilizada de forma recurrente en los resultados posteriores.

1.1. Ideales Primos e Ideales Maximales

En esta sección se introducen los ideales primos y maximales en un anillo conmutativo, así como algunas de sus propiedades básicas, que se utilizarán en secciones posteriores. Comenzamos estableciendo las definiciones de estos conceptos:

Definición 1.1.1. Un ideal $\mathfrak{p} \subset R$ es **primo** si $\mathfrak{p} \neq \langle 1 \rangle$ y para todo $ab \in \mathfrak{p}$ entonces $a \in \mathfrak{p}$ o $b \in \mathfrak{p}$.

Notación 1.1.2. Al conjunto de ideales primos de un anillo R lo denominaremos como $\mathrm{Spec}(R)$.

Definición 1.1.3. Un ideal $\mathfrak{m} \subset R$ es **maximal** si $\mathfrak{m} \neq \langle 1 \rangle$ y no existe un ideal $\mathfrak{a} \subset R$ tal que $\mathfrak{m} \subsetneq \mathfrak{a} \subsetneq R$, donde las inclusiones son estrictas.

Para profundizar en la relación entre un ideal y su anillo cociente asociado, presentamos a continuación dos resultados relevantes. La primera proposición proporciona una caracterización de los ideales primos y maximales mediante propiedades algebraicas del anillo cociente de dicho ideal, mientras que la segunda proposición establece que la primalidad o maximalidad de un ideal se refleja —y se preserva— al pasar al cociente por un ideal contenido en él.

Proposición 1.1.4. *Sea R un anillo. Se tienen las siguientes propiedades:*

i) Un ideal $\mathfrak{p}$ es primo si y solo si el anillo $R/\mathfrak{p}$ es un dominio de integridad.

ii) Un ideal $\mathfrak{m}$ es maximal si y solo si el anillo $R/\mathfrak{m}$ es un cuerpo.

Demostración. Ver Apéndice (A.1). □

Proposición 1.1.5. *Sea $\mathfrak{a} \subseteq R$ un ideal. Entonces:*

i) Un ideal $\mathfrak{p} \subseteq R$ tal que $\mathfrak{a} \subseteq \mathfrak{p}$ es primo si y solo si $\mathfrak{p}/\mathfrak{a}$ es un ideal primo en $R/\mathfrak{a}$.

ii) Un ideal $\mathfrak{m} \subseteq R$ tal que $\mathfrak{a} \subseteq \mathfrak{m}$ es maximal si y solo si $\mathfrak{m}/\mathfrak{a}$ es un ideal maximal en $R/\mathfrak{a}$.

Demostración. Ver Apéndice (A.2). □

Ejemplo 1.1.6. Los ideales primos de $\mathbb{Z}$ son el ideal generado por el 0 y los ideales generados por los números primos en $\mathbb{Z}$. Es decir, $\mathrm{Spec}(\mathbb{Z}) = \{\langle 0\rangle\} \cup \{\langle 2\rangle, \langle 3\rangle, \langle 5\rangle, \langle 7\rangle, ...\}$.

Ejemplo 1.1.7. Sea K un cuerpo. Sabemos que $K[x]$ es un dominio de ideales principales (DIP), por lo que cualquier ideal generado por un polinomio irreducible es primo. De hecho, los ideales primos de $K[x]$ son $\langle 0\rangle$ (por ser un dominio) y los ideales generados por elementos irreducibles de K.

Además, dado que $K[x]$ es un DIP, los ideales primos generados por elementos irreducibles son también maximales y se concluye que los ideales maximales de $K[x]$ son exactamente los ideales de la forma $\langle f\rangle$, con f irreducible.

Ejemplo 1.1.8. En el anillo de polinomios $K[x, y]$, con K cuerpo, los ideales $\langle 0\rangle \subset \langle x\rangle \subset \langle x, y\rangle$ son todos ideales primos, pero sólo el último es maximal. De hecho, para cualquier $(a, b) \in K^2$ se cumple que $\langle x - a, y - b\rangle$ es un ideal maximal. Esto se debe a que los anillos $K[x, y]/\langle x - a, y - b\rangle$ y K son isomorfos, mediante la evaluación de un polinomio $f(x, y)$ en el punto (a, b): $f(x, y) \mapsto f(a, b)$.

Para finalizar esta sección, daremos dos resultados que serán utilizados en las siguientes secciones. El primero de ellos afirma que la proyección canónica, además de preservar la primalidad y maximalidad de los ideales, respeta las intersecciones. El segundo establece que, si una intersección de ideales está contenida en un ideal primo, entonces uno de los ideales de la intersección también está contenido en él.

Proposición 1.1.9. *Sean $\mathfrak{a}$ un ideal en un anillo R y $\pi : R \to R/\mathfrak{a}$ su proyección canónica. Si $\mathfrak{b}_i \subseteq R$ son ideales tales que $\mathfrak{a} \subseteq \mathfrak{b}_i$, donde i recorre los elementos de un conjunto S de índices, entonces:*

$$\pi\Big(\bigcap_{i\in S} \mathfrak{b}_i\Big) = \bigcap_{i\in S} \pi(\mathfrak{b}_i)$$

Además, si $\mathfrak{b}_i$ es primo, entonces $\pi(\mathfrak{b}_i)$ también lo es, y π lleva intersecciones de primos a intersecciones de primos.

Demostración.

En primer lugar, veamos la inclusión $\subseteq$. Sea $a \in \bigcap_i \mathfrak{b}_i$. Entonces, $\overline{a} \in \pi(\mathfrak{b}_i)$ para todo i, por lo que $\overline{a} \in \bigcap_i \pi(\mathfrak{b}_i)$.

Para ver la inclusión $\supseteq$, seleccionamos un $\overline{a} \in \bigcap_i \pi(\mathfrak{b}_i)$, es decir, $\overline{a} \in \pi(\mathfrak{b}_i)$ para cada i. Por tanto, en cada $\mathfrak{b}_i$, existe al menos un $a_i \in \mathfrak{b}_i$ tal que $\pi(a_i) = \overline{a}$. Fijando i, podemos ver que se cumple que, para todo j, $\pi(a_i) - \pi(a_j) = 0$. Es decir, $a_i - a_j \in \mathfrak{a}$. Esto implica que $a_i - a_j \in \mathfrak{b}_j$ y, como $a_j \in \mathfrak{b}_j$, deducimos que $a_i \in \mathfrak{b}_j$ para todo $j \in S$. Concluimos, por tanto, que $a_i \in \cap_j \mathfrak{b}_j$. Pasándolo al anillo cociente, tenemos que $\overline{a} \in \pi(\cap_j \mathfrak{b}_j)$.

La afirmación acerca de que, si $\mathfrak{b}_i$ es primo, entonces $\pi(\mathfrak{b}_i)$ también lo es, viene dada por la proposición 1.1.5. □

Proposición 1.1.10. *Sean $\mathfrak{a}_1, ..., \mathfrak{a}_n, \mathfrak{p}$ ideales de R y supongamos que $\mathfrak{p}$ es primo tal que $\cap_{i=1}^n \mathfrak{a}_i \subseteq \mathfrak{p}$. Entonces, $\mathfrak{a}_i \subseteq \mathfrak{p}$ para algún i. Además, si $\cap_{i=1}^n \mathfrak{a}_i = \mathfrak{p}$, entonces $\mathfrak{p} = \mathfrak{a}_i$ para algún i.*

Demostración.

Procedemos por reducción al absurdo. Asumimos que $\mathfrak{a}_i \nsubseteq \mathfrak{p}$ para todo i. Entonces, para cada $i \in \{1, ..., n\}$, existe un $x_i \in \mathfrak{a}_i$ que no pertenece a $\mathfrak{p}$. Luego, $\prod_i x_i \in \prod_i \mathfrak{a}_i \subseteq \cap_i \mathfrak{a}_i$; pero $\prod_i x_i \notin \mathfrak{p}$ por definición de ideal primo. Esto implica que $\cap_i \mathfrak{a}_i \nsubseteq \mathfrak{p}$, lo que nos lleva a una contradicción. Por último, si $\mathfrak{p} = \cap_i \mathfrak{a}_i$, entonces $\mathfrak{p} \subseteq \mathfrak{a}_i$ para todo i y, por la afirmación anterior, podemos concluir que $\mathfrak{p} = \mathfrak{a}_j$ para algún $j \in \{1, ..., n\}$. □

1.2. Radicales

En esta sección nos adentramos en el estudio del radical de un ideal, una noción que permite identificar aquellos elementos que, al elevarse a potencias, terminan por pertenecer al ideal.

Antes de introducir formalmente la noción de radical de un ideal, comenzamos estudiando un caso particular, el radical del ideal cero, cuyos elementos llamaremos nilpotentes. Además, veremos que este ideal coincide con la intersección de todos los ideales primos del anillo, es decir, todos los ideales primos que contienen al cero. Este primer paso, nos permitirá demostrar un resultado general que nos dice todo radical de un ideal $\mathfrak{a}$ es la intersección de todos los ideales primos que contienen a $\mathfrak{a}$.

Definición 1.2.1. Un elemento $x \in R$ es **nilpotente** si $x^n = 0$ para algún n.

Proposición 1.2.2. *El conjunto de elementos nilpotentes es un ideal y se conoce como **nilradical de** R. Lo denotamos como* $\text{nilrad}(R)$.

Demostración.

Queremos demostrar que el conjunto $C = \{a \in R \mid a^m = 0 \text{ para algún } m > 0\}$ es un ideal. Para ello, tenemos que demostrar que C es un subgrupo aditivo, y que se cumple la propiedad de absorción. Sean $x, y \in R$ tales que $x^n = 0, y^m = 0$. Queremos ver que $x + y$ es nilpotente. Para ello, definimos $N = n + m$, y desarrollamos el binomio de Newton de grado N:

$$(x+y)^N = \sum_{j=0}^{N} \binom{N}{j} x^j y^{N-j}$$

En cada término del sumatorio, o bien $j \geq n$, lo que implica que $x^j = 0$, o bien $j < n$, de lo que deducimos que $N - j \geq m$, por lo que $y^{N-j} = 0$. Por lo tanto, todos los términos de la suma serán cero, lo que implica que $(x + y)^N = 0$. Luego, $x + y$ es nilpotente.

Es fácil comprobar la propiedad de absorción en el conjunto de elementos nilpotentes, ya que si $x \in C, r \in R$, se tiene que, si $x^n = 0$, entonces $(rx)^n = r^n x^n = r^n 0 = 0$. □

Presentamos la caracterización de este ideal por medio de ideales primos, tal y como hemos mencionado anteriormente:

Proposición 1.2.3. *El nilradical de R es la intersección de todos los ideales primos de R.*

Para demostrar la proposición que acabamos de enunciar, recordaremos brevemente el Lema de Zorn, uno de los resultados fundamentales de la teoría de conjuntos. Para ello, a su vez es necesario definir previamente los siguientes conceptos que actúan en el lema:

Definición 1.2.4. Sea $(P, \leq)$ un conjunto parcialmente ordenado:

1. Un subconjunto $C \subseteq P$ es una **cadena** si para todo $x, y \in C$, se tiene $x \leq y$ o $y \leq x$ (es decir, los elementos son comparables).
2. Sea $C \subseteq P$ una cadena. Un elemento $u \in P$ es una **cota superior** de C si $x \leq u$ para todo $x \in C$.
3. Un elemento $m \in P$ es **maximal** si no existe un elemento $x \in P$ tal que $m < x$.

Lema 1.2.5. [6, Ch. 16] (Lema de Zorn) *Sea $(P, \leq)$ un conjunto parcialmente ordenado no vacío tal que toda cadena en P tiene una cota superior en P. Entonces, P contiene al menos un elemento maximal.*

Una vez enunciado el lema, procedemos a demostrar la proposición 1.2.3:

Demostración.

Sea R un anillo y sea $\Theta = \bigcap \mathfrak{p}$ la intersección de todos los ideales primos de R. Queremos ver que:

$$\operatorname{nilrad}(R) = \Theta$$

Comenzamos viendo la contención $\operatorname{nilrad}(R) \subseteq \Theta$. Si $f \in R$ es nilpotente y $\mathfrak{p}$ es un ideal primo, entonces $f^n = 0 \in \mathfrak{p}$ para algún $n > 0$, lo que implica que $f \in \mathfrak{p}$ y, por tanto, $f \in \Theta$. Es decir, todo elemento nilpotente pertenece a la intersección de ideales primos.

Para demostrar que $\operatorname{nilrad}(R) \supseteq \Theta$, queremos ver que todos los elementos que pertenecen a Θ son nilpotentes. Procederemos demostrando la afirmación contrarrecíproca. Es decir, demostraremos que si un elemento no pertenece al nilradical, entonces no pertenece a la intersección de los ideales primos. Para ello, dado un elemento no nilpotente, construiremos un ideal al que este elemento no pertenezca, para luego demostrar que este ideal es primo.

Consideremos un elemento no nilpotente $f \in R$. Sea Σ el conjunto de ideales $\mathfrak{a}$ que cumplen que, para todo $n > 0$, $f^n \notin \mathfrak{a}$. Observar que Σ es un conjunto no vacío, pues claramente, $\langle 0 \rangle \in \Sigma$. Además, es un conjunto parcialmente ordenado con la inclusión de ideales como orden parcial y, dada cualquier cadena C, existe una cota superior, que es la unión de todos los elementos de la cadena $\mathfrak{a}^* = \cup_{\mathfrak{a} \in C} \mathfrak{a}$, ya que para todo $\mathfrak{a}$, se cumple que $\mathfrak{a} \subseteq \mathfrak{a}^*$. Este elemento es un ideal porque surge de una cadena de ideales, cada uno contenido en el anterior. Por tanto, podemos aplicar el Lema de Zorn a Σ para afirmar que existe un elemento maximal en Σ, al que llamaremos $\mathfrak{q}$.

Veamos que $\mathfrak{q}$ es primo. Sean $x, y \in R$. Si $x, y \notin \mathfrak{q}$, por la maximalidad de $\mathfrak{q}$ en Σ, los ideales $\mathfrak{q} + \langle x \rangle, \mathfrak{q} + \langle y \rangle \notin \Sigma$. Por tanto, $f^n \in \mathfrak{q} + \langle x \rangle$, $f^m \in \mathfrak{q} + \langle y \rangle$ para algunos $m, n > 0$. Se sigue que $f^{n+m} \in \mathfrak{q} + \langle xy \rangle$. Observamos también que xy no puede pertenecer a $\mathfrak{q}$ porque, si no, f^{m+n} pertenecería a $\mathfrak{q}$ y esto contradeciría su condición de elemento maximal de Σ, ya que causaría que $\mathfrak{q} \notin \Sigma$. Esto, a su vez, implica que $\mathfrak{q}$ es primo. Finalmente, como $f \notin \mathfrak{q}$, se cumple que $f \notin \Theta$, por lo que no existe ningún elemento no nilpotente en Θ. □

Como hemos mencionado anteriormente, el nilradical es un caso particular de una construcción más general, el radical de un ideal. A continuación lo definiremos y daremos su caracterización.

Definición 1.2.6. Sea $\mathfrak{a} \subseteq R$ un ideal. El **radical** de $\mathfrak{a}$ es el conjunto:

$$r(\mathfrak{a}) = \sqrt{\mathfrak{a}} = \{f \in R \mid f^m \in \mathfrak{a} \text{ para algún } m > 0\}$$

Este conjunto es a su vez un ideal, pues la suma es cerrada por el desarrollo del binomio de Newton y la propiedad de absorción es directa.

Una consecuencia trivial de la definición es que $\mathfrak{a} \subseteq r(\mathfrak{a})$, pero no siempre se da la igualdad.

Definición 1.2.7. Un ideal $\mathfrak{a}$ es **radical** si y solo si $\mathfrak{a} = r(\mathfrak{a})$. Es decir, para todo f tal que $f^m \in \mathfrak{a}$ para algún $m > 0$, entonces $f \in \mathfrak{a}$.

Gracias a la proposición 1.2.3, podemos escribir el siguiente corolario, que permite caracterizar al radical de un ideal por medio de ideales primos, relacionando el concepto de radical de un ideal con el concepto de nilradical a través del anillo cociente:

Corolario 1.2.8. *Sea $\mathfrak{a}$ un ideal propio de R. Entonces, $r(\mathfrak{a})$ es la intersección de todos los ideales primos que contienen a $\mathfrak{a}$. Es decir:*

$$r(\mathfrak{a}) = \bigcap_{\substack{\mathfrak{p} \in \operatorname{Spec}(R) \\ \mathfrak{a} \subseteq \mathfrak{p}}} \mathfrak{p}$$

Demostración.

Definimos

$$P := \bigcap_{\substack{\mathfrak{p} \in \operatorname{Spec}(R) \\ \mathfrak{a} \subseteq \mathfrak{p}}} \mathfrak{p}$$

Para demostrar esta proposición, consideraremos el anillo cociente $R/\mathfrak{a}$, cuyos ideales se encuentran en correspondencia biyectiva con los ideales de R que contienen a $\mathfrak{a}$ por medio de la proyección canónica π. Por tanto, nuestro objetivo será demostrar lo siguiente:

$$\pi(r(\mathfrak{a})) = \pi(P)$$

En primer lugar, observamos que el nilradical de $R/\mathfrak{a}$ es:

$$\operatorname{nilrad}(R/\mathfrak{a}) = \bigcap_{\mathfrak{q} \in \operatorname{Spec}(R/\mathfrak{a})} \mathfrak{q} = \bigcap_{\substack{\mathfrak{p} \in \operatorname{Spec}(R) \\ \mathfrak{a} \subseteq \mathfrak{p}}} \pi(\mathfrak{p}) = \pi(P)$$

donde segunda igualdad viene dada por la proposición 1.1.5, y la última igualdad viene dada por la proposición 1.1.9, donde $\pi(\mathfrak{p})$ es primo. Por lo tanto, nos basta con demostrar que $\operatorname{nilrad}(R/\mathfrak{a}) = \pi(r(\mathfrak{a}))$.

Demostraremos, en primer lugar, la inclusión $\pi(r(\mathfrak{a})) \subseteq \operatorname{nilrad}(R/\mathfrak{a})$. Supongamos que $a \in r(\mathfrak{a})$. Entonces $a^m \in \mathfrak{a}$ para algún $m > 0$. Por tanto, $\overline{a}^m = 0$. Es decir, $\overline{a}$ es nilpotente y, por tanto, pertenece al nilradical de $R/\mathfrak{a}$. Tenemos entonces que $\pi(r(\mathfrak{a})) \subseteq \operatorname{nilrad}(R/\mathfrak{a})$.

Ahora probamos la inclusión $\supseteq$. Sea $\overline{a} \in \operatorname{nilrad}(R/\mathfrak{a})$. Queremos probar que $\overline{a} \in \pi(r(\mathfrak{a}))$. Como $\overline{a}^m = 0$ para algún $m > 0$, tenemos que, para todo elemento a del conjunto $\pi^{-1}(\overline{a})$, $a^m \in \mathfrak{a}$. Por definición de radical, $a \in r(\mathfrak{a})$ y se cumple la inclusión deseada, por lo que el resultado queda demostrado. □

Ejemplo 1.2.9. Todo ideal primo es radical, por lo que $\langle x+1\rangle \in \mathbb{Q}[x]$ lo es. Sin embargo, no todo ideal es radical, en particular el ideal $\langle x^2+2x+1\rangle$ no lo es, ya que $(x+1)^2 \in \langle x^2+2x+1\rangle$ pero $x+1 \notin \langle x^2+2x+1\rangle$. El radical de este ideal es $\langle x+1\rangle$.

Ejemplo 1.2.10. Consideremos $m \in \mathbb{Z}$ y sea $m = p_1^{e_1}\dots p_l^{e_l}$ su factorización en primos, con p_i primos distintos y $e_i > 0$ para todo i. Veamos que el radical de $\langle m\rangle$ es $\langle r\rangle$, donde $r := p_1\dots p_l$. Para ver que $\langle r\rangle \subseteq r(\langle m\rangle)$, tomamos $x \in \langle r\rangle$, es decir, $x = ry$ para algún $y \in \mathbb{Z}$. Entonces, $x^k = r^k y^k = (p_1...p_l)^k y^k \in \langle m\rangle$ para algún $k \geq 1$, donde basta elegir $k \geq \max\{e_1, ..., e_l\}$ para asegurar que todos los primos que dividen a m aparecen con exponente suficiente, por lo que $\langle r\rangle \subseteq r(\langle m\rangle)$. Por otro lado, si $x \in r(\langle m\rangle)$, es decir, si $x^n \in \langle m\rangle \subseteq \langle p_i\rangle$ para todo i, entonces $x \in \langle p_i\rangle$ para todo i, y por tanto $x \in \bigcap_i \langle p_i\rangle = \langle r\rangle$.

Concluimos que los únicos ideales con un radical primo son los ideales generados por un elemento que sea una potencia de un número primo, pues su radical es uno de los ideales vistos en el ejemplo 1.1.6.

Terminamos la sección con dos proposiciones auxiliares. La primera nos ayudará a demostrar que si el radical de un ideal es maximal, entonces el ideal será primario, mientras que la segunda indica que las operaciones de la intersección y tomar radicales son conmutables.

Proposición 1.2.11. *Si un anillo R tiene un único ideal primo $\mathfrak{p}$, entonces todo divisor de cero en R es nilpotente.*

Demostración.

Veamos que todo divisor de cero pertenece a $\mathfrak{p}$. Como $\mathfrak{p}$ es el único ideal primo del anillo, debe ser maximal y cualquier divisor de cero está en $\mathfrak{p}$. Por la proposición 1.2.3, se sigue que $\operatorname{nilrad}(R) = \mathfrak{p}$. Luego x es nilpotente. □

Proposición 1.2.12. *Sea $\mathfrak{a}_1, ..., \mathfrak{a}_n \subseteq R$ una colección de ideales. Entonces, $r(\bigcap_{i=1}^n \mathfrak{a}_i) = \bigcap_{i=1}^n r(\mathfrak{a}_i)$.*

Demostración.

Comenzaremos demostrando que $r(\bigcap_{i=1}^n \mathfrak{a}_i) \subseteq \bigcap_{i=1}^n r(\mathfrak{a}_i)$. Sea $x \in r\left(\bigcap_{i=1}^n \mathfrak{a}_i\right)$, entonces, por definición de radical, existe un entero positivo m tal que $x^m \in \bigcap_{i=1}^n \mathfrak{a}_i$. Esto implica que $x^m \in \mathfrak{a}_i$ para todo i. Por la definición de radical, esto significa que $x \in r(\mathfrak{a}_i)$ para cada i. Por lo tanto, $x \in \bigcap_{i=1}^n r(\mathfrak{a}_i)$.

Para demostrar la inclusión inversa tomamos $x \in \bigcap_{i=1}^n r(\mathfrak{a}_i)$, entonces $x \in r(\mathfrak{a}_i)$ para todo i. Por la definición de radical, esto significa que, para cada i, existe un entero positivo m_i tal que $x^{m_i} \in \mathfrak{a}_i$. Sea $m = \prod_{i=1}^n m_i$, entonces, para cada i, $x^m \in \mathfrak{a}_i$. Por lo tanto, $x^m \in \bigcap_{i=1}^n \mathfrak{a}_i$, lo que implica que $x \in r\left(\bigcap_{i=1}^n \mathfrak{a}_i\right)$. □

CAPÍTULO 2
Descomposición Primaria de Ideales

La descomposición primaria de un ideal puede interpretarse como una generalización de la factorización de un número entero en potencias de números primos. Esta idea surge con el objetivo de simplificar el estudio de un ideal $\mathfrak{a}$ en un anillo R, reduciendo su estudio al estudio de ideales asociados a $\mathfrak{a}$ con unas propiedades conocidas (los ideales primos y primarios), y la idea del proceso de descomposición es análoga a cómo en $\mathbb{Z}$ descomponemos un número cualquiera n como:

$$n = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$$

donde p_i son números primos distintos y $\alpha_i > 0$. Reescribiendo la ecuación con los ideales generados por cada elemento, obtenemos $\langle n \rangle = \langle p_1^{\alpha_1} \rangle \cap \ldots \cap \langle p_r^{\alpha_r} \rangle$. De igual forma, veremos que, bajo ciertas condiciones, cualquier ideal de un anillo R se puede escribir como intersección de los ideales que veremos a continuación, los ideales primarios.

En este capítulo abordamos el estudio de la descomposición primaria de ideales en anillos conmutativos con unidad, basándonos en las referencias [1, Ch. 4], [2, Ch. 4] y [14, Ch. 7]. Comenzaremos introduciendo la definición y propiedades básicas de los ideales primarios, explorando su relación con los ideales primos mediante el concepto de radical en la sección 2.1. En la sección 2.2, formalizaremos la idea de descomposición primaria y discutiremos la existencia y unicidad de las descomposiciones minimales. Finalmente, demostraremos en la sección 2.3 que todo ideal en un anillo noetheriano admite una descomposición primaria, lo que justifica el estudio de esta teoría en el marco de los anillos noetherianos.

2.1. Ideales Primarios

En esta sección introducimos la definición de ideal primario y estudiamos sus propiedades fundamentales, con el objetivo de preparar el camino hacia la formulación de la descomposición primaria de ideales.

Definición 2.1.1. Un ideal $\mathfrak{q} \subset R$ es **primario** si $\mathfrak{q} \neq R$ y se cumple que si $xy \in \mathfrak{q}$, entonces $x \in \mathfrak{q}$ ó $y^m \in \mathfrak{q}$ para algún $m > 0$.

En particular, si un ideal $\mathfrak{q} \subseteq R$ es primario, y denotamos su radical como $r(\mathfrak{q}) = \mathfrak{p}$, entonces diremos que $\mathfrak{q}$ es un ideal **$\mathfrak{p}$-primario**.

Una vez definida esta clase de ideales, se estudia su relación con los ideales primos a través del radical. En particular, se demuestra que el radical de un ideal primario es un ideal primo, lo que permite clasificar los ideales primarios en función de los ideales primos que los contienen mínimamente. Esto justifica la introducción de la terminología 'ideal $\mathfrak{p}$-primario'.

Proposición 2.1.2. *Sea $\mathfrak{q} \subseteq R$ un ideal primario. Entonces $r(\mathfrak{q})$ es el ideal primo más pequeño que contiene a $\mathfrak{q}$.*

Demostración.

Sabemos que $r(\mathfrak{q})$ es un ideal, y por el corolario 1.2.8, sabemos que $r(\mathfrak{q})$ es la intersección de ideales primos de R que contienen a $\mathfrak{q}$:

$$r(\mathfrak{q}) = \bigcap_{\substack{\mathfrak{p} \in \operatorname{Spec}(R) \\ \mathfrak{q} \subseteq \mathfrak{p}}} \mathfrak{p}$$

Queremos ver que esta intersección es, además, un ideal primo y que es el ideal primo más pequeño que contiene a $\mathfrak{q}$.

Para ver que este ideal es primo, tomamos dos elementos $x, y \in R$ tales que $xy \in r(\mathfrak{q})$. Por tanto, sabemos que $(xy)^m \in \mathfrak{q}$ para algún $m > 0$. A su vez, como $\mathfrak{q}$ es primario, tenemos que $x^m \in \mathfrak{q}$ o $y^{mn} \in \mathfrak{q}$ para algún $n > 0$. En cualquier caso, se cumple que $x \in r(\mathfrak{q})$ o $y \in r(\mathfrak{q})$, y concluimos que $r(\mathfrak{q})$ es un ideal primo.

Por último, como $r(\mathfrak{q})$ está contenido en cualquier ideal primo que contenga a $\mathfrak{q}$, y hemos visto que es primo, es el mínimo ideal primo que contiene a $\mathfrak{q}$. □

Al igual que en el caso de ideales primos y maximales, el paso al anillo cociente permite caracterizar los ideales primarios mediante el comportamiento de los elementos en dicho cociente.

Proposición 2.1.3. *Sean R un anillo y $\mathfrak{q}$ un ideal propio de R. Entonces, $\mathfrak{q}$ es primario si y solo si, en $R/\mathfrak{q}$, todo divisor de cero es nilpotente.*

Demostración.

Veamos la implicación a la derecha: sea $\overline{a} \in R/\mathfrak{q}$ un divisor de cero tal que $\overline{a}\overline{b} = 0$ con $\overline{b} \neq 0$. Entonces, si a, b son representantes de $\overline{a}$ y $\overline{b}$ en R, respectivamente, tenemos que $ab \in \mathfrak{q}$, pero sabemos que $b \notin \mathfrak{q}$. Como $\mathfrak{q}$ es primario, se cumple que $a^m \in \mathfrak{q}$ para algún $m > 0$. Es decir, $\overline{a}$ es nilpotente.

Para la otra implicación, observar que, si $a \in R$ cumple que $\overline{a} \in R/\mathfrak{q}$ es un divisor de cero, entonces se tiene que $\overline{a}^m = 0$ para algún $m > 0$, y se concluye que $a^m \in \mathfrak{q}$. Esta hipótesis es cierta para todo par de elementos de R cuya multiplicación esté en $\mathfrak{q}$ (es decir, son divisores de cero en $R/\mathfrak{q}$). Luego $\mathfrak{q}$ es un ideal primario. □

A través de ejemplos concretos, se ilustra cómo identificar ideales primarios en casos particulares, mostrando que la condición de ser primario no coincide necesariamente con ser una potencia de un ideal primo.

Ejemplo 2.1.4. Los ideales primarios en $\mathbb{Z}$ son $\langle 0 \rangle$ y $\langle p^n \rangle$, para $n \geq 1$ y con p primo. Veámoslo: sean $x, y \in \mathbb{Z}$, con $xy \in \mathfrak{q} = \langle p^n \rangle$ y supongamos que $x \notin \mathfrak{q}$. Entonces $p^n \nmid x$, es decir, la potencia de p máxima que divide a x es menor que n. Sea $x = p^k x'$ con $k < n$ y $p \nmid x'$. Como $p^n \mid xy = p^k x' y$ y $p \nmid x'$, se deduce que $p^{n-k} \mid y$. En particular, $y \in \langle p \rangle = r(\mathfrak{q})$, por lo que existe $m > 0$ tal que $y^m \in \mathfrak{q}$, y se concluye que $\mathfrak{q}$ es primario.

Por otro lado, si $\langle d \rangle$ es un ideal primario y d no es una potencia de un primo, entonces su radical no es un ideal primo, como hemos visto en el ejemplo 1.2.10, y estaría contradiciendo la proposición 2.1.2.

Ejemplo 2.1.5. Sea $\mathfrak{q} = \langle x, y^2 \rangle \in K[x, y]$, con K cuerpo. Entonces $R/\mathfrak{q} \cong K[y]/\langle y^2 \rangle$. En este anillo, los divisores de cero son elementos $a_0 + a_1 y$ tales que $(a_0 + a_1 y)(b_0 + b_1 y) = 0$

con algún $b_i, i \in \{1,2\}$ distinto de cero. Expandiendo la ecuación obtenemos $a_0b_0 + (a_1b_0 + a_0b_1)y = 0$, donde la única solución de igualar ambos coeficientes a cero es que $a_0 = 0$, es decir, todos los divisores de cero son múltiplos de y, por lo que son nilpotentes. Por la proposición 2.1.3, esto implica que $\mathfrak{q}$ es primario.

Observar que $r(\mathfrak{q}) = \langle x, y\rangle = \mathfrak{p}$ y, como tenemos $\mathfrak{p}^2 \subsetneq \mathfrak{q} \subsetneq \mathfrak{p}$, y como no puede haber otro ideal primo candidato, debido a que el radical de una potencia de un primo es el propio primo, vemos que un ideal primario no es necesariamente la potencia de un ideal primo.

Se profundiza a continuación en el estudio de la relación entre el radical de un ideal primario y la propiedad de maximalidad, mostrando que si el radical es maximal, entonces el ideal es necesariamente primario.

Proposición 2.1.6. *Sea $\mathfrak{q}$ un ideal de R. Si $r(\mathfrak{q})$ es maximal, entonces $\mathfrak{q}$ es primario. En particular, las potencias de un ideal maximal $\mathfrak{m}$ son $\mathfrak{m}$-primarias.*

Demostración.

Supongamos que $r(\mathfrak{q}) = \mathfrak{m}$ es un ideal maximal. Entonces, por el corolario 1.2.8, podemos afirmar que $\mathfrak{m}$ es el único ideal primo que contiene a $\mathfrak{q}$. Aplicando la correspondencia biyectiva (1.1) y la proposición 1.1.5 a $\mathfrak{m}$, tenemos que $\pi(\mathfrak{m}) = \mathfrak{m}/\mathfrak{q}$ es el único ideal primo en $R/\mathfrak{q}$. Podemos entonces aplicar en $R/\mathfrak{q}$ la proposición 1.2.11 para concluir que en $R/\mathfrak{q}$ todo divisor de cero es nilpotente y, por la proposición 2.1.3, concluimos que $\mathfrak{q}$ es primario

Finalmente, si $\mathfrak{m}$ es un ideal maximal, entonces $r(\mathfrak{m}^n) = \mathfrak{m}$, pues $\mathfrak{m}$ está contenido en $r(\mathfrak{m}^n)$ y, como es un ideal maximal, se tiene la igualdad. Afirmamos entonces que las potencias de un ideal maximal son $\mathfrak{m}$-primarias. □

Ejemplo 2.1.7. Vemos que una potencia de un ideal primo $\mathfrak{p}$ no es necesariamente primaria. Por ejemplo, consideremos el anillo $R = K[x,y,z]/\langle xy - z^2\rangle$ y sea $\mathfrak{p} = \langle \overline{x}, \overline{z}\rangle$ un ideal de R. Este ideal es primo, ya que $R/\mathfrak{p} \cong K[y]$. En R, tenemos que $\mathfrak{p}^2 = \langle \overline{x}^2, \overline{xz}, \overline{z}^2\rangle = \langle \overline{x}^2, \overline{xz}, \overline{xy}\rangle$, con radical $r(\mathfrak{p}^2) = \mathfrak{p}$. Por tanto, $\overline{xy} \in \mathfrak{p}^2$ pero $\overline{x} \notin \mathfrak{p}^2$ e $\overline{y} \notin \mathfrak{p}$, luego $\mathfrak{p}^2$ no es primario.

Se demuestra también que la intersección de ideales $\mathfrak{p}$-primarios sigue siendo $\mathfrak{p}$-primaria.

Proposición 2.1.8. *Sea $\mathfrak{q} = \bigcap_{i=1}^n \mathfrak{q}_i$ con $\mathfrak{q}_i$ ideal $\mathfrak{p}$-primario para todo $i \in \{1,...,n\}$. Entonces $\mathfrak{q}$ es $\mathfrak{p}$-primario.*

Demostración.

Tenemos $r(\mathfrak{q}) = r(\bigcap_{i=1}^n \mathfrak{q}_i) = \bigcap_{i=1}^n r(\mathfrak{q}_i) = \mathfrak{p}$ por la proposición 1.2.12. Para ver que es primario tomamos $x, y \in R$, con $xy \in \mathfrak{q}$, e $y \notin \mathfrak{q}$. Entonces, para algún i se cumple que $y \notin \mathfrak{q}_i$, luego $x^m \in \mathfrak{q}_i$ para algún $m > 0$, porque $\mathfrak{q}_i$ es $\mathfrak{p}$-primario, y tenemos que $x \in \mathfrak{p} = r(\mathfrak{q})$. □

Se introduce seguidamente el concepto de cociente de ideales, una herramienta central para trabajar con descomposiciones y operaciones entre ideales. Su compatibilidad con operaciones como la intersección, junto con su comportamiento particular cuando se aplica a ideales primarios, permite analizar las interacciones entre los ideales primarios de manera más precisa.

Definición 2.1.9. Si $\mathfrak{a}, \mathfrak{b} \subseteq R$ son ideales, el **cociente de ideales** es el ideal:

$$(\mathfrak{a} : \mathfrak{b}) = \{x \in R \mid x \cdot \mathfrak{b} \subseteq \mathfrak{a}\}$$

Notación 2.1.10. Si $\mathfrak{b} = \langle f\rangle$ es un ideal principal entonces escribimos $(\mathfrak{a} : f)$ en vez de $(\mathfrak{a} : \langle f\rangle)$.

Proposición 2.1.11. *Sean $\mathfrak{a}_1, ..., \mathfrak{a}_n \subseteq R$ una colección de ideales y f un elemento cualquiera de R. Entonces:*

$$(\bigcap_{i=1}^{n} \mathfrak{a}_i : f) = \bigcap_{i=1}^{n} (\mathfrak{a}_i : f)$$

Demostración.

Observamos que $r \in (\bigcap_{i=1}^{n} \mathfrak{a}_i : f)$ si y solo si $fr \in \bigcap_{i=1}^{n} \mathfrak{a}_i$, es decir, $fr \in \mathfrak{a}_i$ para todo i. Por definición, esto es equivalente a que $r \in \bigcap_{i=1}^{n} (\mathfrak{a}_i : f)$. □

El siguiente lema caracteriza los cocientes de ideales de los ideales primarios, y nos será útil a lo largo de este capítulo, hasta terminar con el Primer Teorema de Unicidad:

Lema 2.1.12. *Sean $\mathfrak{q}$ un ideal $\mathfrak{p}$-primario de R y $x \in R$. Entonces:*

i) Si $x \in \mathfrak{q}$ entonces $(\mathfrak{q} : x) = \langle 1 \rangle$

ii) Si $x \in \mathfrak{p} \backslash \mathfrak{q}$, entonces $(\mathfrak{q} : x)$ es $\mathfrak{p}$-primario y, por consiguiente, $r((\mathfrak{q} : x)) = \mathfrak{p}$.

iii) Si $x \notin \mathfrak{p}$ entonces $(\mathfrak{q} : x) = \mathfrak{q}$, y $r((\mathfrak{q} : x)) = \mathfrak{p}$.

Demostración.

i) Por definición de ideal, si $x \in \mathfrak{q}$ entonces $xr \in \mathfrak{q}$ para todo $r \in R$. Eso quiere decir que $r \in (\mathfrak{q} : x)$ para todo r.

ii) Queremos probar que si $a, b \in R$, tales que $ab \in (\mathfrak{q} : x)$ y $a \notin (\mathfrak{q} : x)$, entonces $b^m \in (\mathfrak{q} : x)$ para algún $m > 0$. Dado que $ab \in (\mathfrak{q} : x)$, por definición, tenemos que $(ab)x \in \mathfrak{q}$, pero como $ax \notin \mathfrak{q}$ y $\mathfrak{q}$ es $\mathfrak{p}$-primario, se sigue que $b^m \in \mathfrak{q}$ para algún $m > 0$, lo que implica que $b^m x \in \mathfrak{q}$, es decir, $b^m \in (\mathfrak{q} : x)$, y concluimos que $(\mathfrak{q} : x)$ es un ideal primario.

Continuamos tratando de demostrar que el radical de $(\mathfrak{q} : x)$ es igual a $\mathfrak{p}$, y comenzamos viendo la inclusión $r((\mathfrak{q} : x)) \subseteq \mathfrak{p}$. Tomamos $y \in r((\mathfrak{q} : x))$, lo que significa que existe $m > 0$ tal que $y^m \in (\mathfrak{q} : x)$, es decir, $y^m x \in \mathfrak{q}$. Como $\mathfrak{q}$ es $\mathfrak{p}$-primario y $x \notin \mathfrak{q}$ por hipótesis, tenemos que para algún $n > 0$, $y^{nm} \in \mathfrak{q}$. Por tanto, $y \in r(\mathfrak{q}) = \mathfrak{p}$.

Para la inclusión $\mathfrak{p} \subseteq r((\mathfrak{q} : x))$, queremos probar que cualquier $y \in \mathfrak{p}$ cumple que $y^m \in (\mathfrak{q} : x)$ para algún $m > 0$. Sabemos que $y^m \in \mathfrak{q}$ porque $\mathfrak{p} = r(\mathfrak{q})$, lo que quiere decir que $y^m x \in \mathfrak{q}$. Podemos afirmar entonces que $y^m \in (\mathfrak{q} : x)$.

iii) Para cualquier ideal $\mathfrak{q}$ y elemento x de R, se tiene trivialmente que $\mathfrak{q} \subseteq (\mathfrak{q} : x)$. Veamos que $(\mathfrak{q} : x) \subseteq \mathfrak{q}$ en este caso. Para ello, tomamos $y \in (\mathfrak{q} : x)$, es decir, $yx \in \mathfrak{q}$, pero como $x \notin \mathfrak{p}$, esto quiere decir que $x^n \notin \mathfrak{q}$ para ningún $n > 0$. Concluimos que $y \in \mathfrak{q}$ porque $\mathfrak{q}$ es un ideal $\mathfrak{p}$-primario. □

2.2. Descomposición Primaria

En esta sección se introduce formalmente el concepto de descomposición primaria. Se define qué significa que un ideal sea descomponible, y se establecen las condiciones para que una descomposición sea minimal, esto es, sin componentes redundantes y cada ideal primario con un radical distinto.

Definición 2.2.1. Sea $\mathfrak{a} \subseteq R$ un ideal. Una **descomposición primaria** de $\mathfrak{a}$ es una expresión de $\mathfrak{a}$ como intersección finita de ideales primarios, es decir:

$$\mathfrak{a} = \mathfrak{q}_1 \cap ... \cap \mathfrak{q}_k$$

con todos los $\mathfrak{q}_i$ ideales primarios. Si además se cumple que:

i) Para cada j, se tiene que $\mathfrak{a} \subsetneq \cap_{i \neq j} \mathfrak{q}_i$, es decir, no hay ningún término redundante.

ii) $\mathfrak{q}_i$ es $\mathfrak{p}_i$-primario con $\mathfrak{p}_i \neq \mathfrak{p}_j$ si $i \neq j$.

entonces $\mathfrak{q}_1 \cap ... \cap \mathfrak{q}_k$ es una **descomposición primaria minimal** de $\mathfrak{a}$.

De una descomposición primaria de un ideal, es posible obtener una descomposición minimal, sustituyendo ideales primarios con el mismo radical por su intersección, gracias a la proposición 2.1.8, y omitiendo términos superfluos (aquellos ideales que contienen a la intersección del resto de ideales de la descomposición).

Observar que no todo ideal puede escribirse como intersección de ideales primarios. Esto pone de manifiesto la necesidad de imponer condiciones adicionales sobre el anillo, como la noetherianidad, que veremos en el último capítulo, para garantizar la existencia de dichas descomposiciones. Cuando un ideal admite una descomposición primaria, diremos que es **descomponible**. Por otro lado, incluso cuando la descomposición existe, no siempre es sencillo obtenerla de forma explícita. A continuación, veremos un ejemplo de un ideal que admite varias descomposiciones primarias.

Ejemplo 2.2.2. Consideremos el ideal maximal $\mathfrak{m} = \langle x, y \rangle$ en el anillo $R = K[x, y]$, con K cuerpo, y definamos el ideal $\mathfrak{a} = \langle x^2, xy \rangle = \mathfrak{m} \cdot \langle x \rangle \subseteq R$. Observamos que $\mathfrak{m}^2 = \langle x^2, xy, y^2 \rangle$, por lo que se cumple que $\mathfrak{a} = \mathfrak{m}^2 \cap \langle x \rangle$. Como $\langle x \rangle$ es un ideal primo, entonces es un ideal primario. Por otro lado, dado que $\mathfrak{m}$ es maximal, la proposición 2.1.6 garantiza que $\mathfrak{m}^2$ sea un ideal $\mathfrak{m}$-primario. En consecuencia, la igualdad anterior representa una descomposición primaria de $\mathfrak{a}$. Además, esta descomposición es minimal, ya que los radicales de los ideales primarios involucrados son distintos.

Cabe destacar que esta descomposición primaria no es única, ya que también se puede escribir como $\mathfrak{a} = \langle x \rangle \cap \langle x^2, y \rangle$. En esta segunda descomposición, $\langle x^2, y \rangle$ sigue siendo $\mathfrak{m}$-primario, pues su radical es $\mathfrak{m}$, y se puede verificar que cumple la definición de ideal primario.

Continuamos formulando y demostrando el Primer Teorema de Unicidad, un resultado clave que establece que el conjunto de radicales de los ideales primarios asociados a una descomposición primaria minimal es independiente de la descomposición elegida.

Teorema 2.2.3. (Primer Teorema de Unicidad) *Sea $\mathfrak{a} \subseteq R$ un ideal descomponible y sea $\mathfrak{a} = \cap_{i=1}^{n} \mathfrak{q}_i$ una descomposición primaria minimal de $\mathfrak{a}$. Entonces el conjunto $\{r(\mathfrak{q}_i) \mid i \in \{1, ..., n\}\}$ es independiente de la descomposición elegida de $\mathfrak{a}$. Al conjunto anterior se le conoce como* $\mathrm{Ass}(\mathfrak{a})$*, y a cada uno de los radicales $r(\mathfrak{q}_i)$ se le denomina primo asociado de $\mathfrak{a}$.*

Demostración.

Sea $\mathrm{Ass}(\mathfrak{a}) := \{r(\mathfrak{q}_i) \mid i \in \{1, ..., n\}\}$. Nuestro objetivo será demostrar la siguiente igualdad:

$$\mathrm{Ass}(\mathfrak{a}) = \{r((\mathfrak{a} : x)) \in \mathrm{Spec}(R) \mid x \in R\}$$

donde el segundo conjunto no depende de la descomposición elegida. Sabemos, por el corolario 1.2.8, que los elementos $r((\mathfrak{a} : x))$ son intersecciones de ideales primos, por lo que primero nos centraremos en demostrar que dichos primos son elementos de $\mathrm{Ass}(\mathfrak{a})$:

Para todo $x \in R$ se cumple que $(\mathfrak{a} : x) = (\cap \mathfrak{q}_i : x) = \cap (\mathfrak{q}_i : x)$ por la proposición 2.1.11, y tenemos que $r((\mathfrak{a} : x)) = r((\cap_{i=1}^{n} \mathfrak{q}_i : x)) = \cap_{i=1}^{n} r((\mathfrak{q}_i : x))$ por la proposición 1.2.12. Por el lema 2.1.12 (i), si $x \in \mathfrak{q}_i$, se tiene que $(\mathfrak{q}_i : x) = \langle 1 \rangle = r((\mathfrak{q}_i : x))$ y $(\mathfrak{q}_i : x)$ no contribuye a la intersección, y en caso contrario tenemos $r((\mathfrak{q}_i : x)) = \mathfrak{p}_i$ por los apartados (ii) y (iii) del lema anterior. Por tanto, podemos expresar $r((\mathfrak{a} : x))$ como:

$$r((\mathfrak{a} : x)) = \bigcap_{i=1}^{n} r((\mathfrak{q}_i : x)) = \bigcap_{\substack{j=1,\\ x\notin\mathfrak{q}_j}}^{n} \mathfrak{p}_j$$

Supongamos ahora que, para $x \in R$, $r((\mathfrak{a} : x))$ es un ideal primo. Entonces, como $r((\mathfrak{a} : x)) = \cap_{j=1, x\notin\mathfrak{q}_j}^{n} \mathfrak{p}_j$, podemos aplicar la proposición 1.1.10, por lo que tenemos que $r((\mathfrak{a} : x)) = \mathfrak{p}_j$. Como x es arbitrario, cualquier ideal primo de la forma $r((\mathfrak{a} : x))$ debe ser uno de los $\mathfrak{p}_j$. Es decir, $r((\mathfrak{a} : x))$ pertenece a $\mathrm{Ass}(\mathfrak{a})$.

Para terminar, veamos que todo ideal primo $\mathfrak{p}_i \in \mathrm{Ass}(\mathfrak{a})$ tiene la forma $r((\mathfrak{a} : x))$ para algún $x \in R$. Como hemos supuesto que la descomposición primaria es minimal, para todo i, sabemos que $\mathfrak{a} \neq \cap_{j\neq i}\mathfrak{q}_j$. Es decir, existe algún elemento $x \in \cap_{j\neq i}\mathfrak{q}_j$ tal que $x \notin \mathfrak{q}_i$. Entonces, la intersección $\cap_{j=1}^{n} r((\mathfrak{q}_j : x))$ se reduce a $r((\mathfrak{a} : x)) = r((\mathfrak{q}_i : x)) = \mathfrak{p}_i$, puesto que $r((\mathfrak{q}_j : x)) = \langle 1\rangle$ para $j \neq i$. □

2.3. Existencia de Descomposición Primaria

En las secciones anteriores hemos estudiado en profundidad las descomposiciones primarias de ideales descomponibles y la unicidad de los ideales primos asociados. Sin embargo, no todo ideal admite necesariamente una descomposición de este tipo. Existen ejemplos de ideales en ciertos anillos conmutativos que no admiten ninguna descomposición primaria. Esto plantea una pregunta natural: ¿bajo qué condiciones sobre el anillo podemos asegurar que todo ideal es descomponible? En esta sección veremos que una condición suficiente es que el anillo sea noetheriano.

Definición 2.3.1. Un anillo R es **noetheriano** si satisface alguna de las siguientes tres condiciones:

i) Todo conjunto no vacío de ideales Σ de R tiene un ideal maximal.

ii) Para toda cadena $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq ...$ de ideales en R existe un entero $N \geq 1$ tal que $\mathfrak{a}_N = \mathfrak{a}_{N+1} = \cdots$.

iii) Todo ideal de R está finitamente generado.

Comenzamos demostrando la equivalencia entre las tres caracterizaciones clásicas de la noetherianidad, lo que nos permitirá emplearlas de forma intercambiable en los resultados posteriores.

Proposición 2.3.2. *Las tres propiedades de la definición 2.3.1 son equivalentes.*

Demostración.

i) ⇒ ii): Supongamos que toda familia no vacía de ideales de R tiene un elemento maximal. Sea $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq ...$ una cadena ascendente de ideales. Consideramos el conjunto $\Sigma := \{\mathfrak{a}_n \mid n \in \mathbb{N}\}$. Por hipótesis, Σ tiene un elemento maximal respecto a la inclusión, digamos $\mathfrak{a}_N$. Pero como la cadena es ascendente, se tiene $\mathfrak{a}_N \subseteq \mathfrak{a}_{N+1} \subseteq ....$ Así, por maximalidad, $\mathfrak{a}_{N+1} = \mathfrak{a}_N$, y por inducción, $\mathfrak{a}_n = \mathfrak{a}_N$ para todo $n \geq N$. Por tanto, la cadena se estabiliza.

ii) ⇒ iii): Supongamos que toda cadena ascendente de ideales se estabiliza. Sean $\mathfrak{a} \subseteq R$ un ideal no finitamente generado, y $a_1 \in \mathfrak{a}$. Como $\langle a_1\rangle \neq \mathfrak{a}$, entonces existe $a_2 \in \mathfrak{a}\backslash\langle a_1\rangle$ y, por tanto, $\langle a_1\rangle \subsetneq \langle a_1, a_2\rangle \neq \mathfrak{a}$. Repitiendo el proceso, se obtiene una cadena ascendente de ideales finitamente generados. Por hipótesis, esta cadena se estabiliza, digamos en $\langle a_1, ..., a_N\rangle$, y se tiene que este ideal es igual a $\mathfrak{a}$, lo cual es una contradicción.

iii) $\Rightarrow$ i): Supongamos que todo ideal de R es finitamente generado y, por contradicción, que existe un conjunto Σ de ideales en R sin elemento maximal respecto a la inclusión. Entonces, podemos construir una cadena ascendente estricta de ideales $\mathfrak{a}_1 \subsetneq \mathfrak{a}_2 \subsetneq ...$ eligiendo en cada paso un ideal estrictamente mayor, ya que el conjunto no tiene máximo. Consideramos el ideal $\mathfrak{b} := \cup_i \mathfrak{a}_i$, que es un ideal de R y, por hipótesis, es finitamente generado por $a_1, ..., a_n \in \mathfrak{b}$. Pero cada a_i pertenece a algún $\mathfrak{a}_{k_i}$ de la cadena y, como son finitos, existe un N que cumple que $a_i \in \mathfrak{a}_N$ para todo i. Entonces, $\mathfrak{b} \subseteq \mathfrak{a}_N \subseteq \mathfrak{b}$ y esto contradice que la cadena sea estrictamente creciente, por lo que el conjunto Σ tiene un elemento maximal. □

A continuación, presentaremos el resultado principal de la sección, precedido de un lema necesario para su demostración. Éste muestra que, en anillos noetherianos, todo ideal irreducible es primario. El teorema de Lasker-Noether afirma que cualquier ideal puede escribirse como intersección finita de ideales irreducibles, concluyendo que todo ideal admite una descomposición primaria.

Lema 2.3.3. *Sea R un anillo noetheriano. Entonces, todo ideal irreducible es un ideal primario.*

Demostración.

Sean $\mathfrak{a} \subseteq R$ un ideal irreducible, y $a, b \in R$ tales que $ab \in \mathfrak{a}$, pero $b^m \notin \mathfrak{a}$ para todo entero positivo m. Queremos ver que $a \in \mathfrak{a}$. En primer lugar, observar que, para cualquier elemento $x \in R$, se tiene que $(\mathfrak{a} : x^n) \subseteq (\mathfrak{a} : x^{n+1})$, por lo que podemos construir la siguiente cadena de ideales en R: $(\mathfrak{a} : b) \subseteq (\mathfrak{a} : b^2) \subseteq (\mathfrak{a} : b^3) \subseteq ....$ Debido a que R es noetheriano, esta cadena se estabiliza en $(\mathfrak{a} : b^m)$ para algún $m > 0$. Consideramos los ideales $\mathfrak{b}_1 = (\mathfrak{a} + \langle a \rangle), \mathfrak{b}_2 = (\mathfrak{a} + \langle b^m \rangle) \supsetneq \mathfrak{a}$. Claramente, se cumple que $\mathfrak{a} \subseteq \mathfrak{b}_1 \cap \mathfrak{b}_2$, por lo que nuestro objetivo será comprobar la igualdad para poder aplicar la hipótesis de irreducibilidad de $\mathfrak{a}$.

Sea $x \in \mathfrak{b}_1 \cap \mathfrak{b}_2$, entonces podemos escribirlo de las siguientes maneras: $x = \alpha + ay = \beta + b^m z$, con $\alpha, \beta \in \mathfrak{a}$, $y, z \in R$. Multiplicando por b, obtenemos $b\alpha + bay = b\beta + b^{m+1}z$ y, despejando, $b^{m+1}z = b(\alpha - \beta) + bay \in \mathfrak{a}$, pues $ba \in \mathfrak{a}$. Esto implica que $z \in (\mathfrak{a} : b^{m+1}) = (\mathfrak{a} : b^m)$. Concluimos que $x = \beta + b^m z \in \mathfrak{a}$, por lo que se cumple la igualdad $\mathfrak{a} = \mathfrak{b}_1 \cap \mathfrak{b}_2$ y, debido a que $b \notin \mathfrak{a}$, se da la igualdad de ideales $\mathfrak{a} = \mathfrak{b}_1$, que implica que $a \in \mathfrak{a}$, y concluimos que $\mathfrak{a}$ es un ideal primario. □

Teorema 2.3.4. (Teorema de Lasker-Noether). *Sea R un anillo noetheriano. Entonces, todo ideal $\mathfrak{a} \subseteq R$ se puede escribir como $\mathfrak{a} = \cap_{i=1}^n \mathfrak{a}_i$, donde $\mathfrak{a}_i$ es un ideal irreducible para todo i. En consecuencia, todo ideal de R admite una descomposición primaria.*

Demostración.

La consecuencia se obtiene del lema anterior (2.3.3) de forma trivial. Probaremos la primera afirmación por reducción al absurdo, es decir, supongamos que el conjunto de ideales Σ para los que no se cumple el lema es no vacío. Como R es noetheriano, Σ tiene un elemento maximal $\mathfrak{b}$ que, como es reducible, podemos escribir como $\mathfrak{b} = \mathfrak{b}_1 \cap \mathfrak{b}_2$, donde $\mathfrak{b} \subsetneq \mathfrak{b}_1, \mathfrak{b}_2$. Por la maximalidad de $\mathfrak{b}$ en Σ, $\mathfrak{b}_1$ y $\mathfrak{b}_2$ no están en el conjunto, y podemos escribirlos como una intersección finita de ideales irreducibles, lo que implica que también podemos escribir $\mathfrak{b}$ de dicha manera, haciendo la intersección de ambas intersecciones. Hemos llegado a una contradicción, y concluimos que Σ es vacío. □

CAPÍTULO 3
Ideales Monomiales en Anillos de Polinomios

Los ideales monomiales constituyen una clase de ideales especialmente útil en álgebra conmutativa. Su importancia radica en que, al estar generados por monomios, permiten abordar problemas algebraicos complejos de manera más directa, como el cálculo de intersecciones, sumas o descomposiciones primarias. Además, muchos algoritmos en álgebra computacional se basan en la manipulación de este tipo de ideales.

A lo largo de este capítulo, trabajaremos en el anillo de polinomios con coeficientes en un anillo R, que denotamos por $A = R[x_1, ..., x_d]$. Recordamos que un **monomio** de A en las variables $x_1, ..., x_d \in A$ es una expresión de la forma $\underline{x}^{\underline{n}} = x_1^{n_1}...x_d^{n_d}$, donde a la tupla $\underline{n} = (n_1, ..., n_d) \in \mathbb{N}^d$ la llamamos **vector exponente** de $\underline{x}^{\underline{n}} \in A$.

Observar que el conjunto de monomios del anillo A, que escribiremos como $[[A]]$, es linealmente independientes sobre R. Es decir, una combinación lineal finita de monomios con coeficientes en R sólo puede anularse si todos los coeficientes son nulos. Esto implica que los monomios forman una base de A como R-módulo, lo cual permite expresar de forma única cualquier polinomio como combinación lineal de monomios. Gracias a esta propiedad, podremos estudiar muchas de las propiedades de los ideales monomiales, es decir, aquellos que estás generados por monomios.

En este capítulo abordaremos el estudio de los ideales monomiales. Comenzaremos introduciendo su definición formal, junto con los conceptos fundamentales que permiten caracterizarlos y operar con ellos en la sección 3.1. En la sección 3.2, profundizaremos en el estudio de sus intersecciones, mientras que en la sección 3.3 presentamos el concepto de m-irreducibilidad, para profundizar en las descomposiciones m-irreducibles en la sección 3.4. Finalmente, veremos cómo estas propiedades permiten obtener descomposiciones primarias explícitas en el contexto de dominios noetherianos en la sección 3.5. La referencia principal de este capítulo será [12].

3.1. Ideales Monomiales

Comenzamos dando la definición formal de ideal monomial:

Definición 3.1.1. Sea $A = R[x_1, ..., x_d]$. Un **ideal monomial** en A es un ideal en A que está generado por monomios en los elementos $x_1, ..., x_d$.

Conviene señalar que, aunque un ideal sea monomial, puede tener un conjunto generador no formado estrictamente por monomios, como veremos en este ejemplo:

Ejemplo 3.1.2. Consideremos el ideal $\mathfrak{a} = \langle x^2, y^3 \rangle \subseteq R[x, y]$. Este ideal es claramente monomial, ya que está generado por monomios. No obstante, no todos los elementos de $\mathfrak{a}$ son monomios; por ejemplo, $x^2 - y^3 \in \mathfrak{a}$. Esto implica que es posible encontrar un sistema de generadores para $\mathfrak{a}$ que no esté formado por monomios. De hecho, se tiene: $\langle x^2, y^3 \rangle = \langle x^2 - y^3, y^3 \rangle$. Así, $\{x^2 - y^3, y^3\}$ constituye un sistema de generadores no monomial de $\mathfrak{a}$.

Definimos también el conjunto de monomios contenidos en un ideal $\mathfrak{a} \subseteq A$ como el conjunto $[[\mathfrak{a}]] := \mathfrak{a} \cap [[A]]$. Nótese que, en general, $[[\mathfrak{a}]]$ no es un ideal: por ejemplo, si $\mathfrak{a} = \langle x^2 \rangle \in A$, entonces, $x^2, x^3 \in [[\mathfrak{a}]]$ pero $x^2 + x^3 \notin [[\mathfrak{a}]]$, ya que no es un monomio. A pesar de esto, si $\mathfrak{a}$ es un ideal monomial, el conjunto $[[\mathfrak{a}]]$ constituye un sistema de generadores (por monomios) del ideal monomial $\mathfrak{a}$. Formalizamos esta idea con el siguiente lema:

Lema 3.1.3. *Si $\mathfrak{a} \subseteq A = R[x_1, ..., x_d]$ es un ideal monomial, entonces $\mathfrak{a} = \langle [[\mathfrak{a}]] \rangle$.*

Demostración.

Como $\mathfrak{a}$ es un ideal monomial, existe un conjunto de monomios que generan $\mathfrak{a}$, que denotamos por S. Es directo que $S \subseteq [[\mathfrak{a}]] \subseteq \mathfrak{a}$, luego tenemos que $\mathfrak{a} = \langle S \rangle \subseteq \langle [[\mathfrak{a}]] \rangle \subseteq \mathfrak{a}$. Concluimos entonces que $\mathfrak{a} = \langle [[\mathfrak{a}]] \rangle$. □

Con la siguiente proposición, obtenemos condiciones para la igualdad o inclusión entre ideales monomiales, simplemente comparando sus respectivos conjuntos de monomios.

Proposición 3.1.4. *Sean $\mathfrak{a}, \mathfrak{b} \subseteq A = R[x_1, ..., x_d]$ dos ideales monomiales. Entonces:*

i) $\mathfrak{a} \subseteq \mathfrak{b}$ *si y solo si* $[[\mathfrak{a}]] \subseteq [[\mathfrak{b}]]$.

ii) $\mathfrak{a} = \mathfrak{b}$ *si y solo si* $[[\mathfrak{a}]] = [[\mathfrak{b}]]$.

Demostración.

Para i), tenemos que, si $\mathfrak{a}$ está contenido en $\mathfrak{b}$, entonces $[[\mathfrak{a}]] = \mathfrak{a} \cap [[A]] \subseteq \mathfrak{b} \cap [[A]] = [[\mathfrak{b}]]$. En la otra dirección, por el lema 3.1.3 se deduce que, si $[[\mathfrak{a}]] \subseteq [[\mathfrak{b}]]$, entonces $\mathfrak{a} = \langle [[\mathfrak{a}]] \rangle \subseteq \langle [[\mathfrak{b}]] \rangle = \mathfrak{b}$.

La parte ii) es consecuencia trivial del apartado i). □

Una vez afianzada la relación entre monomios y los ideales que generan, nos detenemos a introducir la noción de múltiplo monomial:

Definición 3.1.5. Sea $A = R[x_1, ..., x_d]$, y consideremos $f, g \in [[A]]$. Diremos que f es un **múltiplo monomial** de g si existe un monomio h tal que $f = gh$.

Con estos elementos, nos preparamos para establecer un orden parcial sobre los monomios basado en sus exponentes, lo que permitirá caracterizar la divisibilidad entre ellos de forma combinatoria.

Definición 3.1.6. Definimos una relación $\succcurlyeq$ en $\mathbb{N}^d$, para $d \geq 1$, de la siguiente manera:

$$(a_1, ..., a_d) \succcurlyeq (b_1, ..., b_d)$$

si, para todo $i \in \{1, ..., d\}$, se cumple que $a_i \geq b_i$, donde $\geq$ es el orden natural en $\mathbb{N}$.

A continuación, formalizamos el vínculo entre esta relación y la noción algebraica de ser múltiplo monomial:

Lema 3.1.7. *Sea $A = R[x_1, ..., x_d]$, y consideremos los monomios $f = \underline{x^n}, g = \underline{x^m} \in A$. Si existe un polinomio h en R tal que $f = gh$, entonces se cumple que $\underline{n} \succcurlyeq \underline{m}$ y h es un monomio de la forma $h = \underline{x^p}$, donde $p_i = n_i - m_i$ para todo i.*

Demostración.

Supongamos que $f = \underline{x}^{\underline{n}} = \underline{x}^{\underline{m}}h = gh$, donde $h = \sum_{\underline{r}\in S} a_{\underline{r}}\underline{x}^{\underline{r}} \in A$, con S subconjunto finito de $\mathbb{N}^d$. Como los monomios son linealmente independientes, la única manera de tener $f = gh = \sum_{\underline{r}\in S} a_{\underline{r}}\underline{x}^{\underline{m}}\underline{x}^{\underline{r}}$ es si $a_{\underline{r}} = 1$ cuando $\underline{n} = \underline{m} + \underline{r}$, y $a_{\underline{r}} = 0$ en caso contrario. Llamemos $\underline{p}$ al único elemento de S que cumple que $\underline{n} = \underline{m} + \underline{p}$. Como todos los $p_i \in \mathbb{N}$, se cumple que $\underline{n} \succcurlyeq \underline{m}$, y h es un monomio de la forma $\underline{x}^{\underline{p}}$ con $p_i = n_i - m_i$. □

Con este resultado, estamos en condiciones de caracterizar completamente cuándo un monomio pertenece al ideal generado por otro, un criterio que emplearemos repetidamente en lo que sigue.

Lema 3.1.8. *Sea $A = R[x_1, ..., x_d]$, y consideremos los monomios $f = \underline{x}^{\underline{n}}, g = \underline{x}^{\underline{m}} \in A$. Las siguientes afirmaciones son equivalentes:*

i) $f \in \langle g \rangle$.

ii) El elemento f es un múltiplo de g.

iii) El elemento f es un múltiplo monomial de g.

iv) $\underline{n} \succcurlyeq \underline{m}$.

Demostración.

Para empezar, se cumple trivialmente que iii) ⇒ ii). Por el lema 3.1.7 sabemos que ii) ⇒ iii) y ii) ⇒ iv). Veamos que i) y ii) también son equivalentes: como $\langle g \rangle = \{ga \in A \mid a \in A\}$, decir que $f \in \langle g \rangle$ es equivalente a decir que $f = gh$ para algún $h \in A$, es decir, f es un múltiplo de g. Nos quedaría ver iv) ⇒ iii): como $\underline{n} \succcurlyeq \underline{m}$, llamamos $p_i = n_i - m_i \geq 0$ para cada i, con $p_i \in \mathbb{N}$. Se sigue que $f = g\underline{x}^{\underline{p}}$. Por tanto, f es un múltiplo monomial de g. □

Este criterio se generaliza de forma natural a ideales generados por varios monomios, obteniendo una condición necesaria y suficiente para la pertenencia de un monomio a dicha clase de ideales.

Teorema 3.1.9. *Sea $A = R[x_1, ..., x_d]$, y consideremos los monomios $f, f_1, ..., f_m \in A$. Entonces, $f \in \langle f_1, ..., f_m \rangle$ si y solo si $f \in \langle f_i \rangle$ para algún i.*

Demostración.

La implicación hacia la izquierda es directa, pues $\langle f_i \rangle \subseteq \langle f_1, ..., f_m \rangle$. Para ver la implicación contraria, tomamos $f \in \langle f_1, ..., f_m \rangle$ y lo escribimos como combinación lineal de los elementos del conjunto generador, $f = \sum_{i=1}^{m} g_i f_i$ con $g_i \in A$. Como f, f_i son monomios por hipótesis, escribimos $f = \underline{x}^{\underline{n}}, f_i = \underline{x}^{\underline{n}_i}$ para algunos $\underline{n}, \underline{n}_i \in \mathbb{N}^d$, y podemos desarrollar cada polinomio g_i como $g_i = \sum_{\underline{k}\in S_i} a_{i,\underline{k}}\underline{x}^{\underline{k}}$, con $S_i \subseteq \mathbb{N}^d$ subconjuntos finitos, donde cada $a_{i,\underline{k}} \in R$. Tomando $S = \cup_i S_i$, y definiendo $a_{i,\underline{k}} = 0$ si $\underline{k} \notin S_i$, podemos reescribir f de la siguiente manera:

$$f = \underline{x}^{\underline{n}} = \sum_{i=1}^{m} g_i f_i = \sum_{i=1}^{m} \underline{x}^{\underline{n}_i} \left(\sum_{\underline{k}\in S} a_{i,\underline{k}}\underline{x}^{\underline{k}} \right) = \sum_{i=1}^{m} \sum_{\underline{k}\in S} a_{i,\underline{k}}\underline{x}^{\underline{n}_i + \underline{k}}$$

y, como los monomios son linealmente independientes sobre R, el monomio $\underline{x}^{\underline{n}}$ debe aparecer en algún término de la suma de la derecha, es decir, $\underline{x}^{\underline{n}} = \underline{x}^{\underline{n}_i + \underline{k}}$ para algunos i y $\underline{k}$. Como f es un múltiplo monomial de f_i, por el lema 3.1.8 concluimos que $f \in \langle f_i \rangle$. □

Continuando con el estudio de la pertenencia a ideales monomiales, podemos formular un criterio preciso para determinar cuándo un polinomio pertenece a un ideal monomial, como se recoge en el siguiente lema:

Lema 3.1.10. *Sean $A = R[x_1, ..., x_d]$ y $\mathfrak{a} \subseteq A$ un ideal monomial, y escribimos $f \in A$ como $f = \sum_{\underline{r} \in S} a_{\underline{r}} x^{\underline{r}}$, con $a_{\underline{r}} \in R \backslash \{0\}$ y $S \subset \mathbb{N}^d$. Entonces, $f \in \mathfrak{a}$ si y solo si $x^{\underline{r}} \in \mathfrak{a}$ para todo $\underline{r} \in S$.*

Demostración.

Sea $\mathfrak{a}$ un ideal monomial y $f = \sum_{\underline{r} \in S} a_{\underline{r}} x^{\underline{r}}$ como en el enunciado. Por definición de ideal, si $x^{\underline{r}} \in \mathfrak{a}$ para todo $\underline{r} \in S$, entonces $f \in \mathfrak{a}$, por lo que podemos centrarnos en la otra implicación. Como $\mathfrak{a}$ es un ideal monomial, y $f \in \mathfrak{a}$, podemos expresar f como una combinación lineal finita de monomios $f_1, ..., f_s \in \mathfrak{a}$: $f = \sum_{i=1}^{s} g_i f_i$ con $g_i \in A$. Como los g_i son polinomios en A, los podemos escribir como $g_i = \sum_{\underline{k} \in S_i} a_{i,\underline{k}} \underline{x}^{\underline{k}}$, con $S_i \subseteq \mathbb{N}^d$ subconjuntos finitos. Tenemos por tanto:

$$f = \sum_{i=1}^{s} g_i f_i = \sum_{i=1}^{s} \sum_{\underline{k} \in S_i} a_{i,\underline{k}} \underline{x}^{\underline{k}} f_i$$

donde cada monomio $\underline{x}^{\underline{k}} f_i \in \langle f_i \rangle$ se encuentra contenido en $\mathfrak{a}$ y, como $\underline{x}^{\underline{r}}$, con $\underline{r} \in S$, debe ser algún $\underline{x}^{\underline{k}} f_i$, deducimos que $\underline{x}^{\underline{r}} \in \mathfrak{a}$ para todo $\underline{r} \in S$. □

Finalmente, concluimos esta sección con un resultado central que garantiza que el estudio de ideales monomiales puede reducirse al estudio de conjuntos finitos de monomios. Este resultado, el Lema de Dickson, nos permite trabajar bajo la hipótesis de finitud sin pérdida de generalidad, lo que será crucial en los capítulos siguientes.

Teorema 3.1.11. (Lema de Dickson) *Sea $A = R[x_1, ..., x_d]$. Todo ideal monomial de A es un ideal finitamente generado y tiene un sistema de generadores finito formado por monomios en A.*

Demostración.

Realizaremos la prueba por inducción sobre el número de variables, d. Supongamos que tenemos el ideal monomial $\mathfrak{a} \subseteq A$. Si $\mathfrak{a} = \langle 0 \rangle$, la prueba es trivial, luego vamos a suponer que $\mathfrak{a} \neq \langle 0 \rangle$.

En el caso de $d = 1$, tenemos que $A = R[x_1]$. Podemos tomar $\alpha = \min\{n \mid x_1^n \in \mathfrak{a}\}$. De manera trivial se cumple que $\langle x_1^\alpha \rangle \subseteq \mathfrak{a}$. Si vemos que $\langle x_1^\alpha \rangle \supseteq \mathfrak{a}$, tendremos el caso base. Como $\mathfrak{a}$ está generado por monomios, basta comprobar que $\langle x_1^\alpha \rangle \supseteq [[\mathfrak{a}]]$, que es un conjunto generador de $\mathfrak{a}$ por el lema 3.1.3. Sea $f \in [[\mathfrak{a}]]$, entonces f tiene la forma x_1^m con $m \geq \alpha$, por la minimalidad de α, y se cumple que $x_1^m = x_1^{m-\alpha} x_1^\alpha \in \langle x_1^\alpha \rangle$.

Supongamos que, para $d \geq 2$, todo ideal monomial de $A' = R[x_1, ..., x_{d-1}]$ está generado por un conjunto finito de monomios, y fijamos un ideal monomial $\mathfrak{a} \subseteq A$, con $\mathfrak{a} \neq 0$. Queremos encontrar un subconjunto finito de $[[\mathfrak{a}]]$ que genere $\mathfrak{a}$. En primer lugar, observamos que todo elemento de $[[\mathfrak{a}]]$ se puede expresar como un polinomio en la variable x_d con coeficientes en $[[A']]$, de forma única. Es decir, si $f \in [[A]]$, entonces existen unos únicos $g \in [[A']]$ y $m \geq 0$, tales que $f = g x_d^m$. Por tanto, si definimos el conjunto:

$$G = \{f \in [[A']] \mid f x_d^m \in \mathfrak{a} \text{ para algún } m \geq 0\}$$

se tiene que $[[\mathfrak{a}]] = \{f x_d^m \in \mathfrak{a} \mid f \in G, m \geq 0\} =: C_0$ es un sistema de generadores de $\mathfrak{a}$.

Cabe resaltar que $\mathfrak{b} := \langle G \rangle$ es un ideal monomial en A', con $G = [[\mathfrak{b}]]$ y, por la hipótesis de inducción, existe un subconjunto finito de monomios $S \subset G$ que genera $\mathfrak{b}$. Entonces, el subconjunto:

$$C_1 := \{f x_d^m \in \mathfrak{a} \mid f \in S, m \geq 0\} \subset \langle C_0 \rangle$$

es un sistema de generadores de $\mathfrak{a}$. Para comprobar esta afirmación, debido a que $\langle C_0 \rangle = \mathfrak{a}$, nos basta con ver que $C_0 \subseteq \langle C_1 \rangle$: si $f x_d^m \in C_0$, con $f \in G, m \geq 0$, entonces $f \in \langle S \rangle \subseteq A'$, es decir, f es un múltiplo de algún elemento de S, ya que f es un monomio.

Hasta ahora, tenemos que $\mathfrak{a} = \langle C_1 \rangle$, pero aún existe el problema de que C_1 no es finito, aunque S lo sea, pues las potencias de x_d son infinitas. A continuación veremos que podemos acotar el exponente de x_d en los monomios de C_1 para generar $\mathfrak{a}$.

Por construcción de S, para cada $f \in S$, existe algún $m \geq 0$ que cumple que $fx_d^m \in \mathfrak{a}$ y, como el conjunto es finito, podemos tomar el m más pequeño que cumpla que $fx_d^m \in \mathfrak{a}$ para todo $f \in S$, al que denotaremos como M. Restringimos el conjunto anterior a:

$$C_2 := \{fx_d^m \in \mathfrak{a} \mid f \in S, 0 \leq m \leq M\} \subset \langle C_1 \rangle$$

Este conjunto es finito y, de manera trivial, $C_2 \subseteq \mathfrak{a}$. Si demostramos que $\mathfrak{a} \subseteq \langle C_2 \rangle$, habremos terminado. Pero, como hemos visto antes, basta con demostrar que $C_1 \subseteq \langle C_2 \rangle$. Para ello, tomamos $h := fx_d^m \in C_1$, es decir, $fx_d^m \in \mathfrak{a}$, con $f \in S$ y $m \geq 0$. Entonces, si $m \leq M$, se tiene que $h \in C_2$. En caso contrario, si $m > M$, entonces, $fx_d^m = fx^M x^{d-M} \in \langle C_2 \rangle$, y concluimos la prueba. □

3.2. Intersecciones de Ideales Monomiales

Habiendo comprendido las propiedades básicas de los ideales monomiales, damos ahora un paso más y estudiamos cómo interactúan entre sí mediante la operación de intersección. Esta operación, al igual que la suma o el producto, es central en álgebra conmutativa, y su comportamiento en el caso de ideales monomiales presenta una estructura combinatoria particularmente accesible.

Comenzamos constatando que, si tomamos la intersección de varios ideales monomiales, el resultado sigue siendo un ideal monomial, cuyo conjunto de monomios es la intersección de los monomios de cada ideal.

Proposición 3.2.1. *Sea $A = R[x_1, ..., x_d]$ y consideremos los ideales monomiales $\mathfrak{a}_1, ..., \mathfrak{a}_r$ de A. La intersección $\mathfrak{b} = \mathfrak{a}_1 \cap ... \cap \mathfrak{a}_r$ está generada por el conjunto de monomios de $\mathfrak{b}$. Más concretamente, el ideal $\mathfrak{b}$ es un ideal monomial de A, y $[[\mathfrak{b}]] = [[\mathfrak{a}_1]] \cap ... \cap [[\mathfrak{a}_r]]$.*

Demostración.

Comenzamos la prueba demostrando que, dada una colección de ideales $\mathfrak{a}_1, ..., \mathfrak{a}_r \subseteq A$ y, definiendo $\mathfrak{b} = \cap_{i=1}^r \mathfrak{a}_i$, se cumple que $[[\mathfrak{b}]] = \cap_{i=1}^r [[\mathfrak{a}_i]]$. En efecto:

$$[[\mathfrak{b}]] = (\cap_{j=1}^r \mathfrak{a}_j) \cap [[A]] = \cap_{j=1}^r (\mathfrak{a}_j \cap [[A]]) = \cap_{j=1}^r [[\mathfrak{a}_j]]$$

A continuación, probamos que, si todos los $\mathfrak{a}_i$ son ideales monomiales, entonces $\mathfrak{b}$ también lo es. Definimos el conjunto:

$$S = \cap_{i=1}^r [[\mathfrak{a}_i]] = [[\mathfrak{b}]]$$

Queremos ver que S genera el ideal $\mathfrak{b}$. Sea $f \in \mathfrak{b}$. Como $f \in \mathfrak{a}_i$ para todo i, y cada $\mathfrak{a}_i$ es un ideal monomial, por el lema 3.1.10, se deduce que cada monomio de f pertenece a $\mathfrak{a}_i$ para todo i y, por tanto, a $\mathfrak{b}$. Luego, todos los monomios de f están en S, y se deduce que $f \in \langle S \rangle$. Así, $\mathfrak{b} \subseteq \langle S \rangle$, y la otra inclusión es trivial. Concluimos que $\mathfrak{b}$ es un ideal monomial. □

Dado que conocemos ahora cómo obtener el conjunto de monomios de una intersección de ideales monomiales, surge naturalmente el interés por encontrar un conjunto generador explícito para dicha intersección. Nos enfocamos primero en el caso más simple: la intersección de dos ideales principales generados por un monomio, que resultará estar generada por el mínimo común múltiplo de los generadores.

Definición 3.2.2. Sean $A = R[x_1, ..., x_d]$ y $f, g \in A$ dos monomios tales que $f = \underline{x}^{\underline{n}}$ y $g = \underline{x}^{\underline{m}}$ para algunos $\underline{n}, \underline{m} \in \mathbb{N}^d$. Definimos $p_i = \max\{n_i, m_i\}$ para cada $i \in \{1, ..., d\}$. El **mínimo común múltiplo** de f y g es el monomio $\text{mcm}(f, g) = \underline{x}^{\underline{p}}$.

Lema 3.2.3. *Sean $A = R[x_1, ..., x_d]$ y f, g dos monomios de A. Entonces, $\langle f \rangle \cap \langle g \rangle = \langle \text{mcm}(f, g) \rangle$.*

Demostración.

Sean $f = \underline{x}^{\underline{n}}$ y $g = \underline{x}^{\underline{m}}$ para algunos $\underline{n}, \underline{m} \in \mathbb{N}^d$, y $h = \text{mcm}(f, g)$. Aplicando el lema 3.1.8, se cumple que $h \in \langle f \rangle \cap \langle g \rangle$, pues es múltiplo de ambos elementos, y tenemos que $\langle h \rangle \subseteq \langle f \rangle \cap \langle g \rangle$. Para el otro contenido, seleccionamos un $\alpha \in \langle f \rangle \cap \langle g \rangle$. Como esta intersección es un ideal monomial, por el lema 3.1.10 sabemos que cada monomio de α (en el sentido del lema referenciado) está en la intersección, por lo que basta probar este lema en el caso de que α sea un monomio. Entonces, como α es múltiplo de f y g, se tiene que $\alpha = a\underline{x}^{\underline{n}} = b\underline{x}^{\underline{m}}$ para algunos $a, b \in [[A]]$. Escribimos $\alpha = \underline{x}^{\underline{r}}\underline{x}^{\underline{n}} = \underline{x}^{\underline{k}}\underline{x}^{\underline{m}}$, y observamos que $\underline{r} + \underline{n} \succcurlyeq \underline{m}$ y $\underline{k} + \underline{m} \succcurlyeq \underline{n}$. Luego, si escribimos $p_i = \max\{n_i, m_i\}$ para cada $i \in \{1, ..., d\}$, entonces $h = \underline{x}^{\underline{p}}$ y $\underline{r} + \underline{n} = \underline{k} + \underline{m} \succcurlyeq \underline{p}$. Concluimos, por el lema 3.1.8, que $\alpha \in \langle h \rangle$. □

A continuación, generalizamos esta idea al caso de dos ideales monomiales arbitrarios (no necesariamente principales). Esta caracterización explícita de sus intersecciones nos permitirá abordar de manera constructiva la descomposición de ideales monomiales y eliminar redundancias entre generadores, tal y como exploraremos en la siguiente sección.

Teorema 3.2.4. *Sea $A = R[x_1, ..., x_d]$. Supongamos que tenemos dos ideales $\mathfrak{a} = \langle f_1, ..., f_n \rangle, \mathfrak{b} = \langle g_1, ..., g_m \rangle$ de A, con f_i, g_j monomios. Entonces:*

$$\mathfrak{a} \cap \mathfrak{b} = \langle \{\text{mcm}(f_i, g_j) \mid 1 \leq i \leq n, 1 \leq j \leq m\} \rangle$$

Demostración.

Definimos $G = \langle \{\text{mcm}(f_i, g_j) \mid 1 \leq i \leq n, 1 \leq j \leq m\} \rangle$, que es un ideal monomial. Para demostrar que $\mathfrak{a} \cap \mathfrak{b} \subseteq G$, por la proposición 3.1.4, basta con demostrar que $[[\mathfrak{a} \cap \mathfrak{b}]]$ está contenido en $[[G]]$. Sea $h \in [[\mathfrak{a} \cap \mathfrak{b}]]$. Entonces, por el teorema 3.1.9, sabemos que $h \in \langle f_i \rangle \cap \langle g_j \rangle$ para algunos i, j. Aplicando el lema anterior (3.2.3), deducimos que $h \in \langle \text{mcm}(f_i, g_j) \rangle$. Concluimos que $[[\mathfrak{a} \cap \mathfrak{b}]] \subseteq [[G]]$ y, por tanto, $\mathfrak{a} \cap \mathfrak{b} \subseteq G$.

Continuamos con la demostración de $G \subseteq \mathfrak{a} \cap \mathfrak{b}$, donde basta con demostrar que, para cada i, j, se cumple que $\text{mcm}(f_i, g_j) \in \mathfrak{a} \cap \mathfrak{b}$. Nuevamente, aplicando el lema anterior (3.2.3), obtenemos la siguiente igualdad: $\langle f_i \rangle \cap \langle g_j \rangle = \langle \text{mcm}(f_i, g_j) \rangle$, que claramente está contenido en $\mathfrak{a} \cap \mathfrak{b}$. Podemos entonces afirmar que $\mathfrak{a} \cap \mathfrak{b} = G$. □

3.3. M-Irreducibilidad de Ideales Monomiales

Una de las nociones fundamentales para el estudio de los ideales monomiales es el concepto de m-irreducibilidad, que desempeña un papel análogo al de los ideales primarios en la descomposición primaria, pues permiten reconstruir cualquier ideal monomial a partir de intersecciones. Comenzamos esta sección definiendo los tipos de secuencias generadoras de monomios que puede tener un ideal:

Definición 3.3.1. Sean $A = R[x_1, ..., x_d]$, y $\mathfrak{a}$ un ideal monomial de A con generadores $f_1, ..., f_k \in [[A]]$. La lista $f_1, ..., f_k$ es una **secuencia generadora irredundante de monomios** (s.g.i.m.) para $\mathfrak{a}$ si, para todo $i \in \{1, ..., k\}$, se cumple que $\langle f_1, ..., f_{i-1}, f_{i+1}, ..., f_k \rangle \subsetneq \mathfrak{a}$. En caso contrario, diremos que la secuencia generadora de monomios es **redundante**.

Una vez dada esta definición, nos preguntamos si es posible garantizar siempre la existencia de una secuencia generadora irredundante y, en caso afirmativo, si estas secuencias son únicas. Para ello, comenzamos con un resultado que caracteriza cuándo una secuencia generadora de monomios es irredundante.

Proposición 3.3.2. *Sean $A = R[x_1, ..., x_d]$ y $\mathfrak{a}$ un ideal monomial de A. Sea $f_1, ..., f_k$ una secuencia generadora de monomios para $\mathfrak{a}$. Son equivalentes las siguientes condiciones:*

i) Si $i \neq j$, entonces f_i no es múltiplo de f_j.

ii) Para cada $i \in \{1, ..., k\}$, se cumple que $f_i \notin \langle f_1, ..., f_{i-1}, f_{i+1}, ..., f_k \rangle$.

iii) La secuencia generadora $f_1, ..., f_k$ es irredundante.

Demostración.

i) $\Rightarrow$ ii): Si $f_i \in \langle f_1, ..., f_{i-1}, f_{i+1}, ..., f_k \rangle$, entonces el teorema 3.1.9 asegura que $f_i \in \langle f_j \rangle$ para algún $j \neq i$, lo que contradice nuestra hipótesis.

ii) $\Rightarrow$ iii): Fijando un i, tenemos que $f_i \in \mathfrak{a} \backslash \langle f_1, ..., f_{i-1}, f_{i+1}, ..., f_k \rangle$, por lo que el ideal $\langle f_1, ..., f_{i-1}, f_{i+1}, ..., f_k \rangle \subsetneq \mathfrak{a}$ y, por definición, tenemos una secuencia irredundante.

iii) $\Rightarrow$ i): Supongamos que existen índices i, j tales que $i \neq j$, y f_i es múltiplo de f_j, es decir, $f_i \in \langle f_j \rangle$. Entonces, $\mathfrak{a} = \langle f_1, ..., f_{i-1}, f_{i+1}, ..., f_k \rangle$, por lo que la secuencia no es irredundante, llegando a una contradicción. □

La proposición anterior permite simplificar la descripción de los ideales y facilita el trabajo con sus sistemas de generadores. En particular, nos proporciona un procedimiento efectivo para eliminar redundancias en un conjunto generador, como vemos a continuación:

1. Obtención s.g.i.m. de un ideal monomial

Sean $A = R[x_1, ..., x_d]$ y $\mathfrak{a}$ un ideal monomial de A. Establecemos una secuencia de monomios $f_1, ..., f_k$, con $k \geq 1$, que generan el ideal $\mathfrak{a}$.

1. Utilizando la proposición 3.3.2, comprobar si la secuencia $f_1, ..., f_k$ es irredundante.
   - *a*) Comprobar si, para cada índice i, se cumple que para cada índice $j \neq i$, entonces $f_i \notin \langle f_j \rangle$. En el caso de que sea así, el algoritmo ha terminado.
   - *b*) En el caso de que para algún par i, j no se cumpla el paso anterior, avanzar al paso 2.
2. Sean i, j unos índices con $i \neq j$, tal que $f_i \in \langle f_j \rangle$. Eliminar f_i de la secuencia y volver a ejecutar el paso 1 con $f_1, ..., f_{i-1}, f_{i+1}, ..., f_k$.

El algoritmo tiene a lo sumo $k - 1$ iteraciones, asumiendo, en el peor caso, que todos los monomios sean múltiplos de uno de los elementos de la secuencia. Se presenta a continuación un ejemplo del algoritmo:

Ejemplo 3.3.3. Sea $A = R[x, y, z]$ un anillo. Definimos el ideal $\mathfrak{a} \subseteq A$ como:

$$\mathfrak{a} = \langle x^4, y^2z^2, y^3, x^2y^2, x^2y, z \rangle$$

Ejecutando el algoritmo, observamos que $y^2z^2 \in \langle z \rangle$, por lo que lo eliminamos y reevaluamos la secuencia:

$$\{x^4, y^3, x^2y^2, x^2y, z\}$$

Nuevamente, encontramos dos monomios que cumplen la condición 1b): $x^2y^2 \in \langle x^2y \rangle$. Eliminamos el primero y volvemos a ejecutar el algoritmo con:

$$\{x^4, y^3, x^2y, z\}$$

En este caso, la secuencia no es redundante, por lo que hemos terminado.

Procedemos a demostrar la existencia de una s.g.i.m. única:

Teorema 3.3.4. *Sean $A = R[x_1, ..., x_d]$ y $\mathfrak{a}$ un ideal monomial de A. Entonces, se cumplen las tres siguientes condiciones:*

i) Toda secuencia generadora de monomios S para el ideal $\mathfrak{a}$ contiene una s.g.i.m. para $\mathfrak{a}$.

ii) El ideal $\mathfrak{a}$ tiene una secuencia generadora irredundante de monomios.

iii) Las s.g.i.m. son únicas, salvo reordenamiento.

Demostración.

i): Como $\mathfrak{a}$ es un ideal monomial, por el Lema de Dickson (3.1.11), existe un conjunto finito de monomios $\{a_1, ..., a_k\} \subseteq \mathfrak{a}$ que lo genera. Sea S una secuencia de monomios que genera $\mathfrak{a}$. Entonces, para cada $i = 1, ..., k$, se tiene que:

$$a_i = \sum_{j=1}^{n_i} g_{ij} f_{ij}$$

donde $g_{ij} \in A$, $f_{ij} \in S$ y $n_i \in \mathbb{N}$. Es decir, cada a_i pertenece al ideal generado por un subconjunto finito de S. En particular, $\mathfrak{a} = \langle a_1, ..., a_k \rangle \subseteq \langle \{f_{ij} \mid 1 \leq i \leq k,\ 1 \leq j \leq n_i\} \rangle \subseteq \mathfrak{a}$, por lo que se obtiene la igualdad y, por tanto, el conjunto $\{f_{ij}\}$ es una secuencia generadora finita de $\mathfrak{a}$ contenida en S, de la cual obtenemos una s.g.i.m. mediante el algoritmo 1.

ii): Como el Lema de Dickson (3.1.11) asegura la existencia de una secuencia generadora de monomios S, el resultado se deriva del apartado anterior.

iii): Consideremos dos s.g.i.m. de $\mathfrak{a}$, $F = \{f_1, ..., f_m\}$ y $G = \{g_1, ..., g_n\}$. Veamos que $m = n$, y que $F = G$.

Estudiemos los monomios de F en función de la secuencia G. Como $\langle g_1, ..., g_n \rangle = \mathfrak{a}$, si fijamos $i \in \{1, ..., m\}$, el teorema 3.1.9 nos dice que existe un j para el que $f_i \in \langle g_j \rangle$, porque $f_i \in \mathfrak{a}$. Realizando el mismo proceso con el $g_j \in \langle f_1, ..., f_m \rangle$ obtenido, tenemos que $g_j \in \langle f_k \rangle$ para algún k. Esto implica que f_k es divisor de f_i. Debido a que F es irredundante, se deduce que $i = k$ por la proposición 3.3.2. Esto quiere decir que $f_i \in \langle g_j \rangle \subseteq \langle f_k \rangle = \langle f_i \rangle$. Como se cumple que $\langle f_i \rangle = \langle g_j \rangle$, entonces tenemos que $f_i \mid g_j$ y $g_j \mid f_i$ y, como ambos son monomios, se sigue que $f_i = g_j$, ya que, si $f_i = \underline{x}^{\underline{i}}$, $g_j = \underline{x}^{\underline{j}}$, entonces se cumple que $\underline{j} \succcurlyeq \underline{i}$ e $\underline{i} \succcurlyeq \underline{j}$, de donde se deduce que $\underline{i} = \underline{j}$.

Como todos los f_i son distintos (por irredundancia), se sigue que los g_j correspondientes también son distintos. Esto implica que $m \leq n$ y que $F \subseteq G$. De forma simétrica, para cada g_j, existe i tal que $g_j = f_i$, y tenemos que $n \leq m$ y $G \subseteq F$. Luego, $m = n$, y se tiene la igualdad entre F y G. Concluimos que las s.g.i.m. son únicas, salvo reordenación de sus monomios. □

Comenzamos a estudiar ahora el concepto de m-irreducibilidad:

Definición 3.3.5. Sea $A = R[x_1, ..., x_d]$. Un ideal monomial $\mathfrak{a} \subsetneq A$ es **m-reducible** si existen ideales monomiales $\mathfrak{a}_1, \mathfrak{a}_2 \neq \mathfrak{a}$ tales que $\mathfrak{a} = \mathfrak{a}_1 \cap \mathfrak{a}_2$, y es **m-irreducible** si no es m-reducible.

Dicho de otra manera, un ideal monomial $\mathfrak{a} \neq A$ es m-irreducible si, cuando existen ideales monomiales $\mathfrak{a}_1, \mathfrak{a}_2$ de A tales que $\mathfrak{a} = \mathfrak{a}_1 \cap \mathfrak{a}_2$, entonces $\mathfrak{a} = \mathfrak{a}_1$ o $\mathfrak{a} = \mathfrak{a}_2$. La definición se mantiene

en el caso de que $\mathfrak{a}$ sea igual a una intersección finita: si $\mathfrak{a}$ es m-irreducible y $\mathfrak{a}_1, ..., \mathfrak{a}_d$ son ideales monomiales tales que $\mathfrak{a} = \cap_{j=1}^{d} \mathfrak{a}_j$, entonces uno de esos ideales debe ser igual a $\mathfrak{a}$, es decir, $\mathfrak{a} = \mathfrak{a}_j$ para algún j.

A continuación, daremos una descripción explícita de los ideales monomiales m-irreducibles en cuya demostración usaremos el siguiente lema, que nos da un criterio suficiente para que un ideal monomial sea m-reducible.

Lema 3.3.6. *Sea $A = R[x_1, ..., x_d]$ y consideremos un ideal monomial $\mathfrak{a} \subseteq A$ generado por una secuencia de monomios irredundante $f_1, ..., f_k$. Asumiendo que $f_k = x_1^m g$, con $m \geq 1$, $g \neq 1$, y $x_1 \nmid g$, definimos los ideales de A: $\mathfrak{b}_1 = \langle f_1, ..., f_{k-1}, x_1^m \rangle$ y $\mathfrak{b}_2 = \langle f_1, ..., f_{k-1}, g \rangle$. Entonces, $\mathfrak{a} = \mathfrak{b}_1 \cap \mathfrak{b}_2$, con $\mathfrak{a} \subsetneq \mathfrak{b}_1$, $\mathfrak{a} \subsetneq \mathfrak{b}_2$. Luego $\mathfrak{a}$ es un ideal m-reducible.*

Demostración.

Para demostrar que $\mathfrak{a} = \mathfrak{b}_1 \cap \mathfrak{b}_2$, basta con aplicar el teorema 3.2.4 para obtener la siguiente secuencia de monomios generadores de $\mathfrak{b}_1 \cap \mathfrak{b}_2$:

$$f_1, ..., f_{k-1}, \text{mcm}(f_1, x_1^m), \text{mcm}(f_1, g), ..., \text{mcm}(f_{k-1}, x_1^m), \text{mcm}(f_{k-1}, g), \text{mcm}(x_1^m, g)$$

y vemos que, para cualquier $r \in \{1, ..., k-1\}$, se tiene que $\text{mcm}(f_r, x_1^m), \text{mcm}(f_r, g) \in \langle f_r \rangle$ y $\text{mcm}(x_1^m, g) = f_k$ y, claramente, esta secuencia también genera $\mathfrak{a}$.

Para ver que $\mathfrak{a} \neq \mathfrak{b}_1$, basta con demostrar que $x_1^m \notin \mathfrak{a}$. Si asumimos que $x_1^m \in \mathfrak{a}$, por el teorema 3.1.9, se tiene que cumplir que $f_r \mid x_1^m$ para algún r. Pero, como $x_1^m \mid f_k$, esto implica que $f_r \mid f_k$. Como la secuencia de monomios es irredundante, se tiene que $r = k$. Aplicando que $f_r \mid x_1^m$, se obtiene que $g = 1$, lo cual es una contradicción. Siguiendo un razonamiento análogo para $\mathfrak{b}_2$, obtenemos la conclusión final deseada. □

Teorema 3.3.7. *Sean $A = R[x_1, ..., x_d]$ y $\mathfrak{a} \neq 0$ un ideal monomial de A. El ideal $\mathfrak{a}$ es m-irreducible si y solo si existen enteros positivos $k, t_1, ..., t_k, m_1, ..., m_k$ tales que $\mathfrak{a} = \langle x_{t_1}^{m_1}, ..., x_{t_k}^{m_k} \rangle$ y $1 \leq t_1 \leq ... \leq t_k \leq d$.*

Demostración.

Primero, probaremos que si un ideal monomial $\mathfrak{a}$ es m-irreducible, entonces está necesariamente generado por potencias de variables (es decir, sus generadores son monomios de la forma $x_i^{m_i}$). Lo haremos por reducción al absurdo.

Sea $f_1, ..., f_k$ una s.g.i.m. del ideal $\mathfrak{a}$. Como $\mathfrak{a} \neq 0$, esto asegura que $k \geq 1$. Sin pérdida de generalidad, asumimos que f_k no es potencia de alguna de las variables. De nuevo, sin pérdida de generalidad asumimos que $f_k = x_1^m g$, con $g \neq 1$, $m \geq 1$ y $x_1 \nmid g$. Por el lema anterior (3.3.6), tenemos que $\mathfrak{a}$ es m-reducible, llegando a una contradicción.

Continuamos con la implicación en el otro sentido. Sea $\mathfrak{a}$ un ideal monomial generado por potencias de las variables y, reordenando si es necesario, podemos considerar que $\mathfrak{a} = \langle x_1^{m_1}, ..., x_k^{m_k} \rangle$, con $k \leq d$. Probaremos, de nuevo por reducción al absurdo, que $\mathfrak{a}$ es m-irreducible.

Sean $\mathfrak{b}_1, \mathfrak{b}_2$ dos ideales monomiales tales que $\mathfrak{a} = \mathfrak{b}_1 \cap \mathfrak{b}_2$, y $\mathfrak{a} \subsetneq \mathfrak{b}_1$, $\mathfrak{a} \subsetneq \mathfrak{b}_2$. Se tiene que existen monomios $f_1 \in [[\mathfrak{b}_1]] \backslash [[\mathfrak{a}]]$, $f_2 \in [[\mathfrak{b}_2]] \backslash [[\mathfrak{a}]]$, que escribiremos como $f_1 = \underline{x}^{\underline{n}}$, $f_2 = \underline{x}^{\underline{r}}$ con $\underline{n}, \underline{r} \in \mathbb{N}^d$. Sea ahora $h := \text{mcm}(f_1, f_2) = \underline{x}^{\underline{p}}$, donde $p_i := \text{máx}\{n_i, r_i\}$ para todo $i = 1, \ldots, d$. Por el lema 3.2.3, se cumple que

$$h \in \langle f_1 \rangle \cap \langle f_2 \rangle \subseteq \mathfrak{b}_1 \cap \mathfrak{b}_2 = \mathfrak{a}$$

Vamos a ver que h no puede pertenecer a $\mathfrak{a}$. Como $f_1 \notin \mathfrak{a}$, entonces, por el teorema 3.1.9, $f_1 \notin \langle x_i^{m_i} \rangle$ para ningún $i \in \{1, ..., k\}$, lo que implica que $n_i < m_i$. Análogamente para f_2, se cumple que $r_i < m_i$ para todo $i = 1, ..., k$. De ello se deduce que, para cada $i = 1, ..., k$, se

tiene que $p_i = \max\{n_i, r_i\} < m_i$. Esto implica que $h = \underline{x^p} \notin \mathfrak{a}$, por el lema 3.1.8. Por tanto, hemos llegado a una contradicción, y $\mathfrak{a}$ es m-irreducible. □

3.4. Descomposiciones M-Irreducibles de Ideales Monomiales

Una vez comprendida la noción de m-irreducibilidad y habiendo caracterizado los ideales que la satisfacen, estamos en disposición de abordar uno de los objetivos centrales de este capítulo, que es descomponer cualquier ideal monomial como intersección de ideales m-irreducibles. Comenzamos formalizando esta idea mediante la definición correspondiente:

Definición 3.4.1. Sean $A = R[x_1, ..., x_d]$ y $\mathfrak{a}$ un ideal monomial de A. Una **descomposición m-irreducible** de $\mathfrak{a}$ es una expresión como intersección finita de ideales m-irreducibles, es decir:

$$\mathfrak{a} = \mathfrak{a}_1 \cap ... \cap \mathfrak{a}_n$$

con $n \geq 1$ donde, además, cada $\mathfrak{a}_i$ es un ideal monomial m-irreducible.

Aunque es evidente que cualquier ideal m-irreducible tiene una descomposición trivial (el propio ideal), debemos plantearnos esta cuestión de forma más general, es decir, ¿tienen todos los ideales monomiales alguna descomposición m-irreducible? Y si es así, ¿puede garantizarse que ésta sea irredundante y única? Antes de poder responder estas preguntas, necesitamos una herramienta fundamental sobre las propiedades de las cadenas de ideales monomiales.

Teorema 3.4.2. *Sea $A = R[x_1, ..., x_d]$. Se cumplen las dos siguientes afirmaciones:*

i) Dada una cadena $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq ...$ de ideales monomiales en A, existe un entero $N \geq 1$ tal que $\mathfrak{a}_N = \mathfrak{a}_{N+1} = \cdots$.

ii) Dado un conjunto Σ de ideales monomiales no vacío en A, existe un ideal $\mathfrak{b} \in \Sigma$ tal que, para todo $\mathfrak{a} \in \Sigma$, si $\mathfrak{b} \subseteq \mathfrak{a}$, entonces se cumple que $\mathfrak{a} = \mathfrak{b}$. Es decir, $\mathfrak{b}$ es maximal en Σ. Además, para todo $\mathfrak{c} \in \Sigma$, existe un ideal $\mathfrak{b} \in \Sigma$ que cumple que $\mathfrak{c} \subseteq \mathfrak{b}$ y, para todo $\mathfrak{a} \in \Sigma$, si $\mathfrak{b} \subseteq \mathfrak{a}$, entonces se cumple que $\mathfrak{a} = \mathfrak{b}$. De otra manera, todo ideal monomial de Σ está contenido en un elemento maximal.

Demostración.

i) Sea $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq ...$ una cadena de ideales monomiales en A. Definimos la unión de todos los ideales como $\mathfrak{b} = \bigcup_{j=1}^{\infty} \mathfrak{a}_j$. Sabemos que, en este caso, es un ideal y, como cada $\mathfrak{a}_j$ es monomial, afirmamos que $\mathfrak{b}$ también es monomial, pues está generado por la unión de los conjuntos generadores de los $\mathfrak{a}_j$. Aplicando el Lema de Dickson (3.1.11), podemos afirmar que la secuencia de monomios generadores de $\mathfrak{b}$ es finita: $f_1, ..., f_m$.

Buscamos un ideal que contenga a todos los generadores, que será el elemento de la cadena a partir del cual todas las contenciones se vuelven igualdades. Dado que $\mathfrak{b} = \bigcup_{j=1}^{\infty} \mathfrak{a}_j$ y los $\mathfrak{a}_i$ forman una sucesión ascendente, para cada $f_i \in \mathfrak{b}$ existe un índice N_i tal que $f_i \in \mathfrak{a}_{N_i}$. Tomando $N = \text{máx}\{N_1, ..., N_m\}$, se tiene que $f_i \in \mathfrak{a}_N$ para todo i, y por tanto:

$$\mathfrak{b} = \langle f_1, ..., f_m \rangle \subseteq \mathfrak{a}_N \subseteq \mathfrak{a}_{N+1} \subseteq ... \subseteq \mathfrak{b}$$

Se deduce entonces, que $\mathfrak{a}_N = \mathfrak{a}_{N+1} = \mathfrak{a}_{N+2} = ...$, el resultado deseado.

ii) Sea $\mathfrak{a} \in \Sigma$ y supongamos que no es maximal, ni está contenido en ningún elemento maximal de Σ. Queremos ver que todo elemento de este conjunto es maximal, o está contenido en uno maximal: sea $\mathfrak{a}_1 \in \Sigma$ con $\mathfrak{a} \subsetneq \mathfrak{a}_1$ y, como $\mathfrak{a}_1$ tampoco es maximal, existe un ideal $\mathfrak{a}_2 \in \Sigma$ con $\mathfrak{a}_1 \subsetneq \mathfrak{a}_2$. Aplicando el argumento recursivamente, obtenemos una cadena estrictamente ascendente

de ideales, lo que contradice el apartado i) de este resultado. Por lo tanto, concluimos que Σ tiene un elemento maximal y cualquier ideal está contenido en un ideal maximal. □

Este resultado nos permite aplicar argumentos de maximalidad para construir ideales con propiedades deseadas. En particular, proporciona una herramienta para demostrar uno de los teoremas clave de esta sección:

Teorema 3.4.3. *Todo ideal monomial de cualquier anillo de polinomio con un número finito de variables tiene una descomposición m-irreducible.*

Demostración.

Sea $\mathfrak{a}$ un ideal monomial de $A = R[x_1, ..., x_d]$. Supongamos que $\mathfrak{a}$ no tiene descomposición m-irreducible con el objetivo de llegar a una contradicción. Consideremos entonces el conjunto Σ de ideales sin descomposición m-irreducible, que es no vacío, ya que $\mathfrak{a} \in \Sigma$. Por el teorema 3.4.2 ii), sabemos que existe un elemento maximal del conjunto, al que llamamos $\mathfrak{b}$.

Como $\mathfrak{b}$ no es m-irreducible, existen ideales monomiales $\mathfrak{b}_1, \mathfrak{b}_2$ de A tales que $\mathfrak{b} = \mathfrak{b}_1 \cap \mathfrak{b}_2$ y $\mathfrak{b} \subsetneq \mathfrak{b}_1, \mathfrak{b}_2$. La condición de maximalidad de $\mathfrak{b}$ obliga a la existencia de descomposiciones m-irreducibles para ambos ideales, por lo que podemos construir una descomposición m-irreducible para $\mathfrak{b}$ con la intersección de ambas descomposiciones, lo cual nos lleva a una contradicción. Concluimos que el conjunto Σ es vacío y, más concretamente, todo ideal monomial tiene una descomposición m-irreducible. □

Las descomposiciones m-irreducibles no son únicas en general, como podemos ver con el siguiente ejemplo:

Ejemplo 3.4.4. En $A = R[x, y]$, el ideal $\mathfrak{a} = \langle x^5, xy, y^2 \rangle$ tiene más de una descomposición m-irreducible:

$$\mathfrak{a} = \langle x, y^2 \rangle \cap \langle x^5, y \rangle$$

donde $\langle x, y^2 \rangle$ no contiene a y, y $\langle x^5, y \rangle$ no contiene a x. Pero también:

$$\mathfrak{a} = \langle x, y^2 \rangle \cap \langle x, y \rangle \cap \langle x^5, y \rangle$$

Vemos que los ideales de ambas descomposiciones son m-irreducibles por el teorema 3.3.7, pero la descomposición no es única.

El teorema anterior garantiza la existencia de una descomposición m-irreducible para cualquier ideal monomial, pero no proporciona un procedimiento para obtenerla. Además, como hemos visto en el ejemplo anterior, estas descomposiciones no son únicas. Sin embargo, algunas de estas expresiones pueden contener términos innecesarios, en el sentido de que un ideal de la descomposición contiene a la intersección del resto. En ese caso, podemos eliminar dicho ideal sin alterar el resultado final. Este tipo de observación nos conduce a introducir el concepto de descomposición irredundante, que daremos en esta sección. En particular, mostraremos que toda descomposición irredundante es única (salvo reordenación) y construiremos un algoritmo para obtenerla a partir de un conjunto de generadores del ideal monomial.

Definición 3.4.5. Sean $A = R[x_1, ..., x_d]$ y $\mathfrak{a}$ un ideal monomial propio de A. Una descomposición $\mathfrak{a} = \cap_{i=1}^{n} \mathfrak{a}_i$ m-irreducible de $\mathfrak{a}$ se llama **redundante** si existe algún índice j para el que $\mathfrak{a} = \cap_{i \neq j} \mathfrak{a}_i$. Una descomposición es **irredundante** si no es redundante. Es decir, $\mathfrak{a} \subsetneq \cap_{i \neq j} \mathfrak{a}_i$ estrictamente para todo j.

Estudiar la redundancia requiere analizar cómo se relacionan los ideales que participan en la descomposición. Para ello, necesitaremos un resultado que garantice que, cuando una intersección

está contenida en un ideal m-irreducible, al menos uno de sus términos también lo está. Este lema nos permitirá inmediatamente dar una caracterización útil de las descomposiciones redundantes:

Lema 3.4.6. *Sea $A = R[x_1, ..., x_d]$, y consideremos $\mathfrak{a}, \mathfrak{b}_1, ..., \mathfrak{b}_n$ ideales monomiales de A, que cumplen que $\mathfrak{a}$ es m-irreducible y $\cap_{i=1}^n \mathfrak{b}_i \subseteq \mathfrak{a}$. Entonces, existe un índice j tal que $\mathfrak{b}_j \subseteq \mathfrak{a}$.*

Demostración.

Estudiemos, en primer lugar, el caso trivial $\mathfrak{a} = \langle 0 \rangle$. Entonces, $\cap_{i=1}^n \mathfrak{b}_i \subseteq \mathfrak{a} = \langle 0 \rangle$ implica que $\cap_{i=1}^n \mathfrak{b}_i = \langle 0 \rangle$. Deducimos que, para que la intersección sea cero, debe de haber algún j tal que $\mathfrak{b}_j = \langle 0 \rangle$. Si no, sea $f_j \in [[\mathfrak{b}_j]] \backslash \{0\}$. Entonces, $h := \text{mcm}(f_1, ..., f_n) \neq 0$ y $h \in \langle f_1 \rangle \cap ... \cap \langle f_n \rangle$.

Para el caso general, supongamos que $\mathfrak{a} \neq \langle 0 \rangle$ y procedemos por inducción sobre n, el número de elementos de la intersección. El caso $n = 1$ es inmediato, por lo que estudiamos los valores $n \geq 2$.

En el caso $n = 2$, asumimos que $\mathfrak{b}_1 \cap \mathfrak{b}_2 \subseteq \mathfrak{a}$, pero $\mathfrak{b}_1, \mathfrak{b}_2 \nsubseteq \mathfrak{a}$ para llegar a una contradicción. Por la proposición 3.1.4, esto implica que $[[\mathfrak{b}_1]], [[\mathfrak{b}_2]] \nsubseteq [[\mathfrak{a}]]$. Podemos tomar monomios $f_1 = \underline{x}^r \in \mathfrak{b}_1 \backslash \mathfrak{a}$, $f_2 = \underline{x}^n \in \mathfrak{b}_2 \backslash \mathfrak{a}$. Definimos $h := \text{mcm}(f_1, f_2) = \underline{x}^p$, y observamos que se cumple que $h \in \mathfrak{b}_1 \cap \mathfrak{b}_2 \subseteq \mathfrak{a}$ por definición de mínimo común múltiplo. Ahora, debido a que $\mathfrak{a}$ es un ideal m-irreducible, podemos aplicar el teorema 3.3.7 para expresar $\mathfrak{a} = \langle x_1^{m_1}, ..., x_k^{m_k} \rangle$, con $m_i \geq 1$, $k \leq d$, por lo que existe al menos un índice $j \in \{1, ..., k\}$ que cumple que $x_j^{m_j} \mid \underline{x}^p$. Comparando los vectores exponentes de los polinomios, obtenemos que $m_j \leq p_j = \max\{r_j, n_j\}$. Sin pérdida de generalidad, supongamos que $p_j = r_j$. Esto implica que $x_j^{m_j} \mid f_1$, por lo que $f_1 \in \mathfrak{a}$, una contradicción.

Supongamos ahora que el enunciado es cierto para intersecciones de $n-1$ ideales. Es decir, si $\mathfrak{b}_1, ..., \mathfrak{b}_{n-1}$ son ideales monomiales tales que $\bigcap_{i=1}^{n-1} \mathfrak{b}_i \subseteq \mathfrak{a}$, entonces existe j tal que $\mathfrak{b}_j \subseteq \mathfrak{a}$.

Consideremos ahora n ideales $\mathfrak{b}_1, ..., \mathfrak{b}_n$ tales que $\cap_{i=1}^n \mathfrak{b}_i \subseteq \mathfrak{a}$. Definimos el ideal $\mathfrak{c} = \bigcap_{i=1}^{n-1} \mathfrak{b}_i$, que es monomial porque $\mathfrak{b}_i$ lo es para $i \in \{1, ..., n-1\}$ (ver teorema 3.2.4). Entonces, por el caso $n = 2$, tenemos que $\mathfrak{b}_n \subseteq \mathfrak{a}$ o $\mathfrak{c} \subseteq \mathfrak{a}$. En el primer caso hemos terminado y, en el segundo, por la hipótesis de inducción existe un elemento $\mathfrak{b}_j$ con $j \in \{1, ..., n-1\}$ tal que $\mathfrak{b}_j \subseteq \mathfrak{a}$. Concluimos que existe un índice $k \in \{1, ..., n\}$ tal que $\mathfrak{b}_k \subseteq \mathfrak{a}$. □

Proposición 3.4.7. *Sea $A = R[x_1, ..., x_d]$ y sea $\mathfrak{a}$ un ideal monomial de A con $\mathfrak{a} = \cap_{i=1}^n \mathfrak{a}_i$ una descomposición m-irreducible de $\mathfrak{a}$. Son equivalentes las siguientes condiciones:*

i) La descomposición $\cap_{i=1}^n \mathfrak{a}_i$ es redundante.

ii) Existen índices j, k con $j \neq k$ tales que $\mathfrak{a}_j \subseteq \mathfrak{a}_k$.

Demostración.

i) ⇒ ii): Asumiendo que la descomposición $\cap_{i=1}^n \mathfrak{a}_i$ es redundante, entonces, por definición, existe un índice k tal que $\mathfrak{a} = \cap_{i \neq k} \mathfrak{a}_i \subseteq \mathfrak{a}_k$. Bajo estas condiciones, podemos aplicar el lema 3.4.6, que nos da un índice j que cumple que $\mathfrak{a}_j \subseteq \mathfrak{a}_k$.

ii) ⇒ i): Partimos de la base de que tenemos dos índices j, k con $j \neq k$ y se cumple que $\mathfrak{a}_j \subseteq \mathfrak{a}_k$. Entonces, utilizando propiedades básicas de intersecciones sobre la descomposición de $\mathfrak{a}$, podemos escribir la siguiente igualdad:

$$\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{a}_i = \bigcap_{i \neq k} \mathfrak{a}_i \cap \mathfrak{a}_k$$

Si nos fijamos en el primer término de la intersección, podemos ver que está contenido en $\mathfrak{a}_j$, y por tanto en $\mathfrak{a}_k$. Luego, la ecuación anterior es simplemente $\mathfrak{a} = \bigcap_{i \neq k} \mathfrak{a}_i$, y concluimos que la descomposición inicial es una descomposición redundante. □

Esta caracterización nos permite eliminar sistemáticamente los términos redundantes de una descomposición m-irreducible, lo que nos lleva a definir un algoritmo:

2. Algoritmo de eliminación de redundancias de una descomposición m-irreducible

Sean $A = R[x_1, ..., x_d]$ y $\mathfrak{a}$ un ideal monomial de A con una descomposición m-irreducible $\mathfrak{a} = \cap_{i=1}^{n} \mathfrak{a}_i$, y $n \geq 1$.

1. Comprobar si la descomposición m-irreducible es redundante haciendo uso de la proposición 3.4.7.
   a) Si para todo par de índices distintos j, k, se cumple que $\mathfrak{a}_j \nsubseteq \mathfrak{a}_k$, entonces la descomposición es irredundante y el algoritmo ha finalizado.
   b) En el caso de que para algún par j, k no se cumpla el paso anterior, avanzar al paso 2.
2. Sean j, k índices distintos tal que $\mathfrak{a}_j \subseteq \mathfrak{a}_k$. Eliminar $\mathfrak{a}_k$ de la intersección y volver a ejecutar el paso 1 con $\cap_{i \neq k} \mathfrak{a}_i$.

El algoritmo tiene a lo sumo $n-1$ iteraciones, asumiendo, en el peor caso, que todos los ideales de la intersección estén contenidos en un único ideal. Se presenta a continuación un ejemplo del algoritmo:

Ejemplo 3.4.8. Sea $A = R[x, y, z]$ un anillo. Definimos el ideal $\mathfrak{a} \subseteq A$ como:

$$\mathfrak{a} = \langle x^2, xy^3 \rangle = \langle x \rangle \cap \langle x^2, y^2 \rangle \cap \langle x^2, y^3 \rangle$$

Comparando los elementos de la descomposición m-irreducible, vemos que $\langle x^2, y^3 \rangle \subseteq \langle x^2, y^2 \rangle$, por lo que eliminamos $\langle x^2, y^2 \rangle$ de la descomposición y nos queda que $\mathfrak{a} = \langle x \rangle \cap \langle x^2, y^3 \rangle$. Como ninguno de estos ideales está contenido en el otro, podemos determinar que esta descomposición m-irreducible de $\mathfrak{a}$ es irredundante.

Corolario 3.4.9. *Sea $A = R[x_1, ..., x_d]$. Todo ideal monomial propio de A tiene una descomposición m-irreducible irredundante.*

Demostración.

La existencia de una descomposición m-irreducible viene dada por el teorema 3.4.3, y el algoritmo que acabamos de definir la convierte en irredundante. □

Una vez garantizada la existencia de estas descomposiciones minimales, podemos preguntarnos por su unicidad: ¿puede un mismo ideal admitir dos descomposiciones irredundantes en m-irreducibles distintas? El siguiente resultado proporciona una respuesta definitiva.

Teorema 3.4.10. *Sean $A = R[x_1, ..., x_d]$ y $\mathfrak{a}$ un ideal monomial de A con dos descomposiciones m-irreducibles irredundantes $\mathfrak{a} = \cap_{i=1}^{m} \mathfrak{b}_i = \cap_{j=1}^{n} \mathfrak{c}_i$. Entonces, $m = n$ y existe una permutación $\sigma \in S_n$ tal que $\mathfrak{b}_k = \mathfrak{c}_{\sigma(k)}$ para $k \in \{1, ..., m\}$.*

Demostración.

Fijamos un $k \in \{1, ..., m\}$ cualquiera. Por definición de intersección, se cumple que:

$$\mathfrak{a} = \cap_{j=1}^{n} \mathfrak{c}_i = \cap_{i=1}^{m} \mathfrak{b}_i \subseteq \mathfrak{b}_k$$

y, por el lema 3.4.6 podemos encontrar un l tal que $\mathfrak{c}_l \subseteq \mathfrak{b}_k$. Realizando el mismo razonamiento con $\mathfrak{c}_l$, obtenemos la cadena de inclusiones $\mathfrak{b}_r \subseteq \mathfrak{c}_l \subseteq \mathfrak{b}_k$ para un determinado r. Como las descomposiciones son irredundantes, se deduce que es imposible que $\mathfrak{b}_r \subseteq \mathfrak{b}_k$ con $r \neq k$, por lo que $\mathfrak{b}_r = \mathfrak{b}_k$, lo que implica que $\mathfrak{c}_l = \mathfrak{b}_k$.

Como esto sucede para todo k, podemos definir una función $\sigma : \{1, ..., m\} \to \{1, ..., n\}$, con $\sigma(k) = l$ para cada par de elementos k, l. Por construcción, esta función es inyectiva, por lo que $m \leq n$. Razonando de igual manera para los elementos $\mathfrak{c}_l$ de la descomposición, obtenemos que $n \leq m$. Por tanto, se deduce que $n = m$. Concluimos que σ es biyectiva, ya que una aplicación inyectiva entre conjuntos finitos con el mismo cardinal es, automáticamente, sobreyectiva. Hemos obtenido nuestra permutación $\sigma \in S_n$. □

Habiendo asentado que cualquier ideal monomial tiene una única forma m-irreducible en términos de intersección de ideales m-irreducibles, aún nos falta una pieza importante, una forma sistemática de construir esta descomposición dada una secuencia generadora de monomios. Para llegar a ese objetivo, necesitamos algunas herramientas auxiliares. Primero, entendemos cómo se comportan las sumas e intersecciones de ideales monomiales en términos de sus monomios generadores.

Proposición 3.4.11. *Sea $A = R[x_1, ..., x_d]$ y sean $\mathfrak{a}_1, ..., \mathfrak{a}_n$ ideales monomiales de A. Entonces, la suma $\mathfrak{a}_1 + ... + \mathfrak{a}_n$ es un ideal monomial y se cumple que $[[\mathfrak{a}_1 + ... + \mathfrak{a}_n]] = [[\mathfrak{a}_1]] \cup ... \cup [[\mathfrak{a}_n]]$.*

Demostración.

Sabemos que cada ideal monomial $\mathfrak{a}_i$ tiene un sistema de generadores G_i formado por monomios, es decir, $\mathfrak{a}_i = \langle G_i \rangle$ con $G_i \subseteq [[\mathfrak{a}_i]]$. Entonces, la suma de los ideales $\mathfrak{a}_1 + \cdots + \mathfrak{a}_n$ está generada por la unión de estos conjuntos $G_1 \cup ... \cup G_n$, luego es monomial. Ahora, $[[\mathfrak{a}_1 + ... + \mathfrak{a}_n]] = [[\langle \bigcup_{i=1}^n G_i \rangle]] = \bigcup_{i=1}^n [[\mathfrak{a}_i]]$, ya que todo monomio que pertenezca a la suma lo hace por ser múltiplo monomial de algún generador en la unión de los $G_i \subseteq [[\mathfrak{a}_i]]$. Esto prueba la igualdad deseada. □

Lema 3.4.12. *Sea $A = R[x_1, \ldots, x_d]$ y sean $\mathfrak{a}_1, ..., \mathfrak{a}_n$ y $\mathfrak{b}_1, ..., \mathfrak{b}_m$ ideales monomiales de A. Entonces se cumple que:*

$$\left(\bigcap_{i=1}^{n} \mathfrak{a}_i\right) + \left(\bigcap_{j=1}^{m} \mathfrak{b}_j\right) = \bigcap_{i=1}^{n} \bigcap_{j=1}^{m} (\mathfrak{a}_i + \mathfrak{b}_j).$$

Demostración.

Como la suma e intersección de ideales monomiales es también un ideal monomial, podemos trabajar sobre los conjuntos de monomios involucrados. Comenzamos desarrollando el conjunto de monomios del lado izquierdo:

$$[[\left(\bigcap_{i=1}^{n} \mathfrak{a}_i\right) + \left(\bigcap_{j=1}^{m} \mathfrak{b}_j\right)]] = [[\bigcap_{i=1}^{n} \mathfrak{a}_i]] \cup [[\bigcap_{j=1}^{m} \mathfrak{b}_j]] = \bigcap_{i=1}^{n} [[\mathfrak{a}_i]] \cup \bigcap_{j=1}^{m} [[\mathfrak{b}_j]]$$

donde usamos primero la proposición 3.4.11, y luego la proposición 3.2.1. Aplicando las propiedades de la unión e intersección de conjuntos, obtenemos:

$$\bigcap_{i=1}^{n} [[\mathfrak{a}_i]] \cup \bigcap_{j=1}^{m} [[\mathfrak{b}_j]] = \bigcap_{i=1}^{n} \bigcap_{j=1}^{m} ([[\mathfrak{a}_i]] \cup [[\mathfrak{b}_j]])$$

Terminamos volviendo a aplicar las proposiciones 3.4.11 y 3.2.1:

$$\bigcap_{i=1}^{n} \bigcap_{j=1}^{m} ([[\mathfrak{a}_i]] \cup [[\mathfrak{b}_j]]) = \bigcap_{i=1}^{n} \bigcap_{j=1}^{m} [[\mathfrak{a}_i + \mathfrak{b}_j]] = [[\bigcap_{i=1}^{n} \bigcap_{j=1}^{m} (\mathfrak{a}_i + \mathfrak{b}_j)]]$$

y obtenemos el resultado deseado. □

Proposición 3.4.13. *Sea $A = R[x_1, ..., x_d]$, y sea $\mathfrak{a}$ un ideal de A con una secuencia generadora de monomios $f_1, ..., f_k$. Si definimos f_k como $f_k = \underline{x}^{\underline{m}}$, entonces $\mathfrak{a} = \cap_{i=1}^{d} \langle f_1, ..., f_{k-1}, x_i^{m_i} \rangle$.*

Demostración.

Reordenando las variables si es preciso, podemos suponer que $f_k = x_1^{m_1} ... x_t^{m_t}$, para un cierto $t \leq d$, con $m_i \geq 1$, y procedemos a demostrar la proposición por inducción sobre t. El caso base resulta trivial, pues si $f_k = x_1^{m_1}$, entonces $\mathfrak{a} = \langle f_1, ..., f_{k-1}, x_1^{m_1} \rangle$.

Supongamos que la hipótesis se cumple para $t-1$, y demostremos la proposición para t. Supongamos que $f_k = x_1^{m_1} ... x_t^{m_t} = g x_t^{m_t}$. Entonces, podemos aplicar el lema 3.3.6 para decir que $\mathfrak{a} = \langle f_1, ..., f_{k-1}, g \rangle \cap \langle f_1, ..., f_{k-1}, x_t^{m_t} \rangle$. Aplicando la hipótesis de inducción a $\langle f_1, ..., f_{k-1}, g \rangle$, concluimos que:

$$\mathfrak{a} = \cap_{i=1}^{t-1} \langle f_1, ..., f_{k-1}, x_i^{m_i} \rangle \cap \langle f_1, ..., f_{k-1}, x_t^{m_t} \rangle = \cap_{i=1}^{t} \langle f_1, ..., f_{k-1}, x_i^{m_i} \rangle$$

y este es el resultado deseado. □

Con estas herramientas en mano, estamos listos para enunciar y demostrar el teorema fundamental de esta sección, que tras estudiar la existencia de descomposiciones m-irreducibles, nos da una herramienta para generarlas:

Teorema 3.4.14. *Sean $A = R[x_1, ..., x_d]$ y $\mathfrak{a}$ un ideal monomial de A con una secuencia generadora de monomios $f_1, ..., f_k$, con $f_i = \underline{x}^{\underline{m}_i}$, donde $\underline{m}_i = (m_{i1}, ..., m_{id}) \in \mathbb{N}^d$. Entonces, podemos dar una descomposición m-irreducible del ideal $\mathfrak{a}$ con la siguiente fórmula:*

$$\mathfrak{a} = \bigcap_{i_1=1}^{d} ... \bigcap_{i_k=1}^{d} \langle x_{i_1}^{m_{1i_1}}, ..., x_{i_k}^{m_{ki_k}} \rangle$$

Demostración.

Demostramos el teorema por inducción sobre k, el número de monomios de la secuencia. En el caso base, la ecuación tiene la forma:

$$\mathfrak{a} = \langle f_1 \rangle = \langle \underline{x}^{\underline{m}_1} \rangle = \bigcap_{i=1}^{d} \langle x_i^{m_{1i}} \rangle$$

donde la última igualdad es consecuencia directa de la proposición anterior (3.4.13).

Asumimos que la hipótesis es cierta para $k-1$, con $k > 1$. Es decir, el resultado se verifica para cualquier ideal con una secuencia generadora de monomios con $k-1$ elementos. Sea $f_1, ..., f_k$ una secuencia generadora de $\mathfrak{a}$, y definimos $\mathfrak{b} = \langle f_1, ..., f_{k-1} \rangle$. Escribiendo $f_k = x_1^{m_{k1}} ... x_d^{m_{kd}}$, se cumple la siguiente ecuación:

$$\mathfrak{a} = \langle f_1, ..., f_k \rangle = \mathfrak{b} + \langle f_k \rangle = \mathfrak{b} + \langle x_1^{m_{k1}} ... x_d^{m_{kd}} \rangle$$

Por el caso base de la demostración y el lema 3.4.12, podemos escribir:

$$\mathfrak{b} + \langle x_1^{m_{k1}} ... x_d^{m_{kd}} \rangle = \mathfrak{b} + \bigcap_{i_k=1}^{d} \langle x_i^{m_{ki_k}} \rangle = \bigcap_{i_k=1}^{d} \left(\mathfrak{b} + \langle x_i^{m_{ki_k}} \rangle \right)$$

Aplicando ahora la hipótesis de inducción, obtenemos la siguiente igualdad para $\mathfrak{a}$:

$$\mathfrak{a} = \bigcap_{i_k=1}^{d} \left(\mathfrak{b} + \langle x_i^{m_{ki_k}} \rangle \right) = \bigcap_{i_k=1}^{d} \left(\left(\bigcap_{i_1=1}^{d} ... \bigcap_{i_{k-1}=1}^{d} \langle x_{i_1}^{m_{1i_1}}, ..., x_{i_{k-1}}^{m_{(k-1)i_{k-1}}} \rangle \right) + \langle x_i^{m_{ki_k}} \rangle \right)$$

Por el lema 3.4.12, conmutamos la intersección de ideales con la suma:

$$\begin{aligned}\mathfrak{a} &= \bigcap_{i_k=1}^{d}\left(\bigcap_{i_1=1}^{d}\dots\bigcap_{i_{k-1}=1}^{d}\left(\langle x_{i_1}^{m_{1i_1}},\dots,x_{i_{k-1}}^{m_{(k-1)i_{k-1}}}\rangle+\langle x_i^{m_{ki_k}}\rangle\right)\right)\\ &= \bigcap_{i_1=1}^{d}\dots\bigcap_{i_k=1}^{d}\langle x_{i_1}^{m_{1i_1}},\dots,x_{i_k}^{m_{ki_k}}\rangle\end{aligned}$$

donde la última igualdad viene dada por la definición de la suma de ideales y por la asociatividad de la intersección. Esto nos da el resultado esperado. □

A partir de este resultado, desarrollar un algoritmo para obtener la descomposición m-irreducible de cualquier ideal monomial se vuelve inmediato.

3. Descomposición m-irreducible de un ideal monomial

Sean $A = R[x_1,\dots,x_d]$, $\mathfrak{a}$ un ideal monomial de A y F una secuencia generadora de monomios para $\mathfrak{a}$.

1. Aplicar el algoritmo de obtención de una s.g.i.m. (1) a F.
2. Aplicar el teorema 3.4.14 para obtener una descomposición m-irreducible de $\mathfrak{a}$.
3. Aplicar de nuevo el algoritmo de obtención de una s.g.i.m. (1) a cada ideal de la intersección.
4. Aplicar el algoritmo de eliminación de redundancias (2) a la intersección de ideales de manera que la descomposición sea irredundante.

Se presenta a continuación un ejemplo del algoritmo:

Ejemplo 3.4.15. Sea $A = R[x,y,z]$ un anillo. Definimos el ideal $\mathfrak{a} \subseteq A$ como:

$$\mathfrak{a} = \langle x^4yz^2, x^2z^3, x^5y^3\rangle$$

Ejecutamos el algoritmo:

Paso 1: Como el ideal ya se encuentra generado por una s.g.i.m. de monomios, no es necesario realizar ningún cambio.

Paso 2: Aplicamos el teorema 3.4.14, que nos da una descomposición m-irreducible de $\mathfrak{a}$ a partir de sus generadores, que ya son monomios. Consideramos todos los divisores monomiales de los generadores, variando cada variable por separado:

$$\begin{aligned}\mathfrak{a} =&\langle x^4,x^2,x^5\rangle\cap\langle x^4,x^2,y^3\rangle\cap\langle x^4,z^3,x^5\rangle\cap\langle x^4,z^3,y^3\rangle\\ &\cap\langle y,x^2,x^5\rangle\cap\langle y,x^2,y^3\rangle\cap\langle y,z^3,x^5\rangle\cap\langle y,z^3,y^3\rangle\\ &\cap\langle z^2,x^2,x^5\rangle\cap\langle z^2,x^2,y^3\rangle\cap\langle z^2,z^3,x^5\rangle\cap\langle z^2,z^3,y^3\rangle\end{aligned}$$

Paso 3: Simplificamos la secuencia generadora de cada ideal para obtener una irredundante. Aquí usamos el algoritmo de obtención de una s.g.i.m para encontrar una base mínima de generadores monomiales:

$$\begin{aligned}\mathfrak{a} =&\langle x^2\rangle\cap\langle x^2,y^3\rangle\cap\langle x^4,z^3\rangle\cap\langle x^4,z^3,y^3\rangle\cap\langle y,x^2\rangle\cap\langle y,x^2\rangle\\ &\cap\langle y,z^3,x^5\rangle\cap\langle y,z^3\rangle\cap\langle z^2,x^2\rangle\cap\langle z^2,x^2,y^3\rangle\cap\langle z^2,x^5\rangle\cap\langle z^2,y^3\rangle\end{aligned}$$

Paso 4. Eliminamos repeticiones y términos redundantes (aquellos que contienen la intersección del resto). El resultado final es la descomposición m-irreducible minimal:

$$\mathfrak{a} = \langle x^2 \rangle \cap \langle x^4, z^3 \rangle \cap \langle y, z^3 \rangle \cap \langle z^2, x^5 \rangle \cap \langle z^2, y^3 \rangle$$

3.5. Descomposición Primaria de Ideales Monomiales en Anillos Noetherianos

En esta sección estudiaremos las descomposiciones primarias de ideales monomiales. Veremos que, bajo ciertas hipótesis, incluyendo la noetherianedad del anillo sobre el que trabajamos, todo ideal monomial admite una descomposición primaria minimal explícita. Este resultado se apoya en el hecho de que, en anillos noetherianos, toda descomposición irreducible es una descomposición primaria (véase la sección 2.3).

Para ello, estableceremos primero un marco bajo el cual todo ideal monomial m-irreducible es irreducible, lo que permitirá descomponer cualquier ideal monomial como intersección finita de ideales irreducibles. El siguiente paso servirá de apoyo para el resultado que nos permita relacionar la irreducibilidad con la m-irreducibilidad. Con este fin, comenzamos dando dos definiciones relevantes para la prueba:

Definición 3.5.1. Sea $A = R[x_1, ..., x_d]$. El **grafo** de un ideal monomial $\mathfrak{a}$ es el conjunto $\Gamma(\mathfrak{a}) = \{\underline{n} \in \mathbb{N}^d \mid \underline{x}^{\underline{n}} \in \mathfrak{a}\}$.

Definición 3.5.2. Sea $f = \sum_{\underline{n} \in S} a_{\underline{n}} \underline{x}^{\underline{n}} \in R[x_1, ..., x_d]$, con $S \subseteq \mathbb{N}^d$ finito. Definimos el conjunto $\gamma(f) = \{\underline{n} \in \mathbb{N}^d \mid a_{\underline{n}} \neq 0\}$, al que se conoce como el **soporte** de f.

Lema 3.5.3. *Sea $A = R[x_1, ..., x_d]$, y fijemos enteros $k, m_1, ..., m_k \geq 1$, con $k \leq d$. Definimos el ideal $\mathfrak{a} = \langle x_1^{m_1}, ..., x_k^{m_k} \rangle$. Sea $\mathfrak{b} \subseteq A$ un ideal tal que $\mathfrak{a} \subsetneq \mathfrak{b}$. Entonces, existe un polinomio $h_k = z\hat{h}(x_{k+1}, ..., x_d) \in \mathfrak{b} \backslash \mathfrak{a}$, donde $z = x_1^{m_1 - 1} ... x_k^{m_k - 1}$.*

Demostración.

Para demostrar que existe h_k, lo haremos por inducción en el número de variables del polinomio z. Es decir, queremos demostrar que, para cada $j \in \{1, ..., k\}$, existe un polinomio $h_j = x_1^{m_1 - 1} ... x_j^{m_j - 1} x_{j+1}^{p_{j+1}} ... x_k^{p_k} \hat{h}(x_{k+1}, ..., x_d) \in \mathfrak{b} \backslash \mathfrak{a}$, donde $p_i < m_i$ para todo $j + 1 \leq i \leq k$.

Sean $h = \sum_{\underline{n} \in \gamma(h)} a_{\underline{n}} \underline{x}^{\underline{n}}$ un polinomio de $\mathfrak{b} \backslash \mathfrak{a}$ y $\gamma(h)$ su soporte. Podemos suponer que $\gamma(h) \cap \Gamma(\mathfrak{a}) = \emptyset$ pues, en caso contrario, si existe $\underline{n} \in \gamma(h) \cap \Gamma(\mathfrak{a})$, entonces escogemos $h - a_{\underline{n}} \underline{x}^{\underline{n}} \in \mathfrak{b} \backslash \mathfrak{a}$, y su soporte no contiene a $\underline{n}$. Analizando el soporte de h, deducimos que, para todo $\underline{n} \in \gamma(h)$ y para todo $i \in \{1, ..., k\}$, se cumple que $n_i < m_i$, ya que h no pertenece al ideal $\mathfrak{a}$.

En el caso $j = 1$, consideramos $r_1 = \min\{n_1 \in \mathbb{N} \mid \underline{n} \in \gamma(h)\} < m_1$, y escribimos h como:

$$h = \sum_{\substack{\underline{n} \in \gamma(f) \\ n_1 = r_1}} a_{\underline{n}} \underline{x}^{\underline{n}} + \sum_{\substack{\underline{n} \in \gamma(f) \\ n_1 > r_1}} a_{\underline{n}} \underline{x}^{\underline{n}} = f_1 + g_1$$

donde $\gamma(f_1) = \{\underline{n} \in \gamma(h) \mid n_1 = r_1\}$ y $\gamma(g_1) = \{\underline{n} \in \gamma(h) \mid n_1 \geq r_1 + 1\}$. Observar que $m_1 - r_1 > 0$ y, por tanto, podemos considerar $h_1 = x_1^{m_1 - r_1 - 1} f_1 \neq 0$.

Constatamos que todo monomio de la forma $x_1^{m_1 - r_1 - 1} g_1$ tienen exponente en x_1 igual a $m_1 - r_1 - 1 + n_1$, donde $\underline{n} \in \gamma(g_1)$. Como $n_1 \geq r_1 + 1$, se tiene $m_1 - r_1 - 1 + n_1 \geq m_1$. Por tanto, todos los monomios de este polinomio son divisibles por $x_1^{m_1}$, es decir, pertenecen a $\mathfrak{a} \subseteq \mathfrak{b}$,

y no pueden utilizarse en la construcción buscada. Concluimos que $x_1^{m_1-r_1-1}g_1 \in \mathfrak{b}$ y, como $h \in \mathfrak{b}$, se tiene que $h_1 = x_1^{m_1-r_1-1}h - x_1^{m_1-r_1-1}g_1 \in \mathfrak{b}$.

Sea $\underline{x}^{\underline{p}}$ un monomio de h_1, que es de la forma $\underline{x}^{\underline{p}} = x_1^{m_1-r_1-1}\underline{x}^{\underline{n}}$ para algún $\underline{n} \in \gamma(f_1)$. Como $n_1 = r_1$, entonces se cumple que $p_1 = m_1 - r_1 + r_1 - 1 = m_1 - 1$. Inspeccionando los índices $2 \leq i \leq k$, vemos que la condición $\underline{n} \in \gamma(f_1) \subseteq \gamma(h)$ implica que $p_i = n_i \leq m_i - 1$, ya que $\underline{n} \notin \Gamma(\mathfrak{a})$. Por lo tanto, $\underline{x}^{\underline{p}} \notin \mathfrak{a}$, y concluimos que $h_1 \notin \mathfrak{a}$, por el lema 3.1.10. Asimismo, nuestro polinomio se puede escribir de la forma $h_1 = x_1^{m_1-1}h'(x_2, ..., x_d)$, por lo que tiene la forma deseada.

Paso inductivo: supongamos ahora que hemos construido un polinomio $h_j \in \mathfrak{b} \setminus \mathfrak{a}$ tal que, para todo $\underline{p} \in \gamma(h_j)$, se cumple que $p_i = m_i - 1$ para todo $1 \leq i \leq j$ y $p_i \leq m_i - 1$ para $j+1 \leq i \leq k$, con $j < k$. Queremos construir un polinomio h_{j+1} que tenga la misma propiedad extendida hasta $j+1$.

Definimos $r_{j+1} = \min\{n_{j+1} \in \mathbb{N} \mid \underline{n} \in \gamma(h_j)\} \leq m_{j+1} - 1$, por la hipótesis sobre h_j, el cual descomponemos como:

$$h_j = \sum_{\substack{\underline{n}\in\gamma(h_j) \\ n_{j+1}=r_{j+1}}} a_{\underline{n}}\underline{x}^{\underline{n}} + \sum_{\substack{\underline{n}\in\gamma(h_j) \\ n_{j+1}>r_{j+1}}} a_{\underline{n}}\underline{x}^{\underline{n}} = f_{j+1} + g_{j+1}$$

y definimos $h_{j+1} = x_{j+1}^{m_{j+1}-r_{j+1}-1}f_{j+1}$. Por el mismo argumento del caso base, se tiene que $h_{j+1} \in \mathfrak{b}$. Sea $\underline{p} \in \gamma(h_{j+1})$. Entonces, para $i \in \{1, ..., j\}$, se cumple que $p_i = m_i - 1$ por definición, y para $j+1 < i \leq k$, los exponentes siguen cumpliendo que $p_i \leq m_i - 1$. Adicionalmente, la coordenada $j+1$ tiene la forma $p_{j+1} = r_{j+1} + (m_{j+1} - r_{j+1} - 1) = m_{j+1} - 1$. Finalmente, ya que todos los monomios de h_{j+1} tienen exponente menor estrictamente que m_i en cada coordenada, se tiene que $\underline{x}^{\underline{p}} \notin \mathfrak{a}$ para todo $\underline{p} \in \gamma(h_{j+1})$, y por el lema 3.1.10, se concluye que $h_{j+1} \notin \mathfrak{a}$. Esto completa el paso inductivo y, cuando $j = k$, obtenemos el resultado. □

Gracias a esta herramienta, podemos observar que la noción de m-irreducibilidad, coincide con la de irreducibilidad, siempre que trabajemos sobre un dominio de integridad:

Teorema 3.5.4. *Sea R un dominio de integridad, y denotamos $A = R[x_1, ..., x_d]$. Un ideal monomial $\mathfrak{a} \neq \langle 0 \rangle$ de A es irreducible si y solo si es m-irreducible.*

Demostración.

La implicación a la derecha es directa, por definición de ideal irreducible. Para la otra implicación, asumimos que $\mathfrak{a}$ es m-irreducible. Por el teorema 3.3.7, sabemos que podemos expresar $\mathfrak{a} = \langle x_1^{m_1}, ..., x_k^{m_k} \rangle$ para algún $k \leq d$, reordenando las variables si es necesario. Procedemos por contradicción.

Supongamos que $\mathfrak{a}$ no es irreducible, es decir, existen ideales $\mathfrak{b}_1$ y $\mathfrak{b}_2$ tales que $\mathfrak{a} = \mathfrak{b}_1 \cap \mathfrak{b}_2$ y $\mathfrak{a} \neq \mathfrak{b}_1, \mathfrak{b}_2$. Por el lema anterior, existen dos polinomios $f_k \in \mathfrak{b}_1 \setminus \mathfrak{a}, g_k \in \mathfrak{b}_2 \setminus \mathfrak{a}$ de la forma $f_k = z\hat{f}(x_{k+1}, ..., x_d), g_k = z\hat{g}(x_{k+1}, ..., x_d)$, donde $z = x_1^{m_1-1}...x_k^{m_k-1}$. Debido a que $f_k \in \mathfrak{b}_1$, podemos deducir que $z\hat{f}\hat{g} = f_k\hat{g} \in \mathfrak{b}_1$ y, de manera análoga, $z\hat{f}\hat{g} \in \mathfrak{b}_2$. Por lo tanto, $z\hat{f}\hat{g} \in \mathfrak{b}_1 \cap \mathfrak{b}_2 = \mathfrak{a}$.

Analizando este polinomio, como los polinomios $\hat{f}$ y $\hat{g}$ están en las variables $x_{k+1}, ..., x_d$, entonces el producto no afecta a los exponentes de $x_1, ..., x_k$, y cada monomio de $z\hat{f}\hat{g}$ tendrá la forma $y = x_1^{m_1-1} \cdots x_k^{m_k-1}x_{k+1}^{\alpha_{k+1}} \cdots x_d^{\alpha_d}$, que, por el lema 3.1.10, debe pertenecer a $\mathfrak{a}$. Esto nos da una contradicción con el teorema 3.1.9, ya que $y \notin \langle x_i^{m_i} \rangle$ para ningún $i \in \{1, ..., k\}$. Concluimos que el polinomio $z\hat{f}\hat{g}$ no puede tener ningún monomio, por lo que es el polinomio nulo. Además, aplicando que R es un dominio de integridad y z es un monomio no nulo,

necesariamente se cumple que $\hat{f} = 0$ o $\hat{g} = 0$. Sin pérdida de generalidad, asumimos el primer caso. Entonces, $z\hat{f} = f_k = 0 \in \mathfrak{b}_1 \backslash \mathfrak{a}$, pero esto es imposible, pues $0 \in \mathfrak{a}$. Hemos obtenido nuestra contradicción, y concluimos que el ideal $\mathfrak{a}$ es irreducible. □

Culminamos esta sección con el resultado central del trabajo, en la que se recogen los resultados anteriores y se establece formalmente la existencia de descomposición primaria para ideales monomiales en un contexto noetheriano:

Corolario 3.5.5. *Sea $A = R[x_1, ..., x_d]$ un dominio de integridad noetheriano. Entonces, todo ideal monomial tiene una descomposición primaria. En concreto, si $\mathfrak{a}$ es un ideal monomial, una descomposición primaria para $\mathfrak{a}$ es la intersección finita de ideales monomiales m-irreducibles que aparece en su descomposición m-irreducible irredundante.*

Demostración.

Sea $\mathfrak{a} \subseteq A$ un ideal monomial propio. Entonces, por el corolario 3.4.9, sabemos que este ideal tiene una descomposición m-irreducible irredundante. Debido a la hipótesis de que R es un dominio de integridad, podemos aplicar el teorema anterior (3.5.4), del que concluimos que la descomposición de $\mathfrak{a}$ es una descomposición en factores irreducibles. Terminamos aplicando el lema 2.3.3, y concluimos que la descomposición irreducible de $\mathfrak{a}$ es una descomposición primaria. Por lo tanto, la descomposición m-irreducible irredundante de $\mathfrak{a}$ es una descomposición primaria. □

Este resultado completa el puente entre las herramientas desarrolladas a lo largo del capítulo y las nociones clásicas de la teoría de ideales. Además, garantiza que las descomposiciones m-irreducibles, obtenidas de forma explícita mediante el algoritmo de obtención de descomposiciones m-irreducibles de un ideal monomial, son descomposiciones primarias.

Nota 3.5.6. Una condición necesaria y suficiente para que se cumplan las hipótesis del corolario anterior es suponer que el anillo R es un dominio de integridad noetheriano, ya que, por el teorema de Hilbert sobre bases finitas (B.0.1), si R es noetheriano, entonces $A = R[x_1, ..., x_d]$ también lo es.

Bibliografía

[1] Michael F. Atiyah and Ian G. Macdonald. *Introduction to Commutative Algebra*. Addison-Wesley Series in Mathematics, Reading, Massachusetts, 1969.

[2] David Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Undergraduate Texts in Mathematics. Springer, 4th edition, 2015.

[3] Harm Derksen and Gregor Kemper. *Computational Invariant Theory*, volume 130 of *Encyclopaedia of Mathematical Sciences*. Springer, 2002.

[4] David Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995.

[5] Elisa Gorla and Alberto Ravagnani. Generalized weights of codes over rings and invariants of monomial ideals. *Contributions to Discrete Mathematics*, 18(3):17–44, 2023.

[6] Paul R. Halmos. *Naive Set Theory*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1974.

[7] Serkan Hoşten and Gregory G. Smith. *Monomial Ideals*. Algorithms and Computation in Mathematics, vol. 8. Computations in Algebraic Geometry with Macaulay 2, Springer-Verlag, 2002.

[8] Emanuel Lasker. Zur theorie der moduln und ideale. *Mathematische Annalen*, 60:20–116, 1905.

[9] Ezra Miller and Bernd Sturmfels. Monomial ideals and planar graphs. In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (AAECC-13)*, volume 1719 of *Lecture Notes in Computer Science*, pages 19–28, Berlin, Heidelberg, 1999. Springer.

[10] Ezra Miller and Bernd Sturmfels. *Combinatorial Commutative Algebra*, volume 227 of *Graduate Texts in Mathematics*. Springer, New York, 2005.

[11] Masayoshi Miyanishi. *Algebraic Geometry*, volume 136. Providence, R.I. : American Mathematical Society, 1994.

[12] W. Frank Moore, Mark Rogers, and Sean Sather-Wagstaff. *Monomial Ideals and Their Decompositions*. Universitext. Springer Cham, 2018.

[13] Emmy Noether. Idealtheorie in ringbereichen. *Mathematische Annalen*, 83:24–66, 1921.

[14] Miles Reid. *Undergraduate Commutative Algebra*. London Mathematical Society Student Texts, vol. 29. Cambridge University Press, 1995.

APÉNDICE A
Demostraciones

A.1 Proposición 1.1.4. *Sea R un anillo. Se tienen las siguientes propiedades:*

i) Un ideal $\mathfrak{p}$ es primo si y solo si el anillo $R/\mathfrak{p}$ es un dominio de integridad.

ii) Un ideal $\mathfrak{m}$ es maximal si y solo si el anillo $R/\mathfrak{m}$ es un cuerpo.

Demostración.

i) Para ver la implicación a la derecha, estudiamos la existencia de divisores de cero en el anillo cociente. Es decir, buscamos ver que no existen dos elementos $a, b \in R$ que cumplan que $\overline{ab} = \overline{a}\overline{b} = 0$ con $\overline{a}, \overline{b} \neq 0$. Supongamos que existen dos elementos $a, b \in R$ tales que $\overline{ab} = 0$. Por la definición de anillo cociente, la hipótesis implica que $ab \in \mathfrak{p}$ y, por la definición de ideal primo, entonces $a \in \mathfrak{p}$ o $b \in \mathfrak{p}$, por lo que se sigue que $\overline{a} = 0$ o $\overline{b} = 0$. Deducimos entonces que $R/\mathfrak{p}$ es un dominio de integridad.

Continuamos con la implicación hacia la izquierda: sean $a, b \in R$ tales que $ab \in \mathfrak{p}$. Su imagen en $R/\mathfrak{p}$ es $\overline{a}\overline{b} = 0$ y, aplicando que no existen divisores de cero, necesariamente se cumple que $\overline{a} = 0$ o $\overline{b} = 0$. Volviendo a R, deducimos que $a \in \mathfrak{p}$ o $b \in \mathfrak{p}$, es decir, $\mathfrak{p}$ es primo.

ii) Comenzamos con la implicación a la derecha: sea $\mathfrak{m} \subset R$ un ideal maximal. Fijamos un $\overline{a} \in (R/\mathfrak{m})\backslash\{0\}$ y seleccionamos $a \in \pi^{-1}(\overline{a})$. Claramente, $\langle a, \mathfrak{m}\rangle = R$ por la maximalidad de $\mathfrak{m}$. Entonces, tenemos que $1 = m + ra$ para algunos $m \in \mathfrak{m}$, $r \in R\backslash\mathfrak{m}$. Por tanto, en el anillo cociente se tiene la igualdad $1 = \overline{ra}$. Es decir, $\overline{a}$ es una unidad y, como es un elemento cualquiera distinto de 0, $R/\mathfrak{m}$ es un cuerpo.

La otra implicación viene dada por el hecho de que los únicos ideales de un cuerpo K son $\{0\}$ y K. Teniendo esto en cuenta, no puede haber ningún ideal $\mathfrak{a}$ que cumpla que $\mathfrak{m} \subsetneq \mathfrak{a} \subsetneq R$ ya que, de ser así, la existencia de dicho $\mathfrak{a}$ implicaría, por la biyección (1.1), la existencia de $\langle 0\rangle \neq \mathfrak{a}/\mathfrak{m} \subsetneq R/\mathfrak{m}$, contradiciendo el hecho de que $R/\mathfrak{m}$ es un cuerpo. Concluimos que $\mathfrak{m}$ es maximal. □

A.2 Proposición 1.1.5. *Sea $\mathfrak{a} \subseteq R$ un ideal. Entonces:*

i) Un ideal $\mathfrak{p} \subseteq R$ tal que $\mathfrak{a} \subseteq \mathfrak{p}$ es primo si y solo si $\mathfrak{p}/\mathfrak{a}$ es un ideal primo en $R/\mathfrak{a}$.

ii) Un ideal $\mathfrak{m} \subseteq R$ tal que $\mathfrak{a} \subseteq \mathfrak{m}$ es maximal si y solo si $\mathfrak{m}/\mathfrak{a}$ es un ideal maximal en $R/\mathfrak{a}$.

Demostración.

i) Sea $\mathfrak{p} \subseteq R$ un ideal que contiene a $\mathfrak{a}$. Comencemos viendo que, si $\mathfrak{p}$ es primo, entonces $\mathfrak{p}/\mathfrak{a}$ es primo en $R/\mathfrak{a}$. Sean $\overline{a}, \overline{b} \in R/\mathfrak{a}$ tales que $\overline{ab} = \overline{a}\overline{b} \in \mathfrak{p}/\mathfrak{a}$ y consideremos un representante de cada clase, $a, b \in R$. Como $\overline{a}\overline{b} \in \mathfrak{p}/\mathfrak{a}$, y $\mathfrak{a} \subseteq \mathfrak{p}$, se tiene que $ab \in \mathfrak{p}$ y, como $\mathfrak{p}$ es primo, $a \in \mathfrak{p}$ o

$b \in \mathfrak{p}$. Volviendo al anillo cociente, se tiene que $\overline{a} \in \mathfrak{p}/\mathfrak{a}$ o $\overline{b} \in \mathfrak{p}/\mathfrak{a}$, de donde concluimos que $\mathfrak{p}/\mathfrak{a}$ es primo.

Para el recíproco, supongamos que $\mathfrak{p}/\mathfrak{a}$ es primo en $R/\mathfrak{a}$. Si $ab \in \mathfrak{p}$, entonces $\overline{ab} \in \mathfrak{p}/\mathfrak{a}$. Como $\mathfrak{p}/\mathfrak{a}$ es primo, tenemos que $\overline{a} = a + \mathfrak{a} \in \mathfrak{p}/\mathfrak{a}$ o $\overline{b} = b + \mathfrak{a} \in \mathfrak{p}/\mathfrak{a}$. Debido a que $\mathfrak{a} \subseteq \mathfrak{p}$, esto implica que $a \in \mathfrak{p}$ o $b \in \mathfrak{p}$.

ii) Sea $\mathfrak{m} \subseteq R$ un ideal que contiene a $\mathfrak{a}$. Comencemos viendo que, si $\mathfrak{m}$ es maximal en R, entonces $\mathfrak{m}/\mathfrak{a}$ es maximal en $R/\mathfrak{a}$. Supongamos que $\mathfrak{m}/\mathfrak{a} \subsetneq \mathfrak{q} \subsetneq R/\mathfrak{a}$. Por la correspondencia entre los ideales de R que contienen a $\mathfrak{a}$ y los ideales de $R/\mathfrak{a}$, existe un ideal $\mathfrak{b} \subseteq R$ tal que $\mathfrak{q} = \mathfrak{b}/\mathfrak{a}$. Como dicha correspondencia mantiene las inclusiones, esto implica que $\mathfrak{m} \subsetneq \mathfrak{b} \subsetneq R$, lo que contradice la maximalidad de $\mathfrak{m}$.

Para el recíproco, supongamos que $\mathfrak{m}/\mathfrak{a}$ es maximal en $R/\mathfrak{a}$. Si $\mathfrak{m} \subsetneq \mathfrak{b} \subsetneq R$, entonces $\mathfrak{b}/\mathfrak{a}$ es un ideal en $R/\mathfrak{a}$ con $\mathfrak{m}/\mathfrak{a} \subsetneq \mathfrak{b}/\mathfrak{a} \subsetneq R/\mathfrak{a}$, lo que contradice la maximalidad de $\mathfrak{m}/\mathfrak{a}$. □

APÉNDICE B

Teorema de Hilbert sobre bases finitas

En la sección 3.5, hemos estudiado cómo, bajo la hipótesis de que el anillo de polinomios sobre el que trabajamos sea noetheriano, podemos obtener una descomposición primaria de cualquier ideal monomial que tenga la forma de descomposición m-irreducible. En este capítulo, presentamos dos resultados que permiten, como condición suficiente para garantizar la existencia de dichas descomposiciones, que el anillo de coeficientes del anillo de polinomios sea noetheriano.

Teorema B.0.1. (Teorema de Hilbert sobre bases finitas) *Si R es un anillo noetheriano, entonces su anillo de polinomios $R[x]$ es un anillo noetheriano.*

Demostración.

Para demostrar este teorema, procederemos por reducción al absurdo, suponiendo que existe un ideal no finitamente generado en $R[x]$. Esta hipótesis nos permitirá construir una secuencia infinita de polinomios en dicho ideal cuyos grados no disminuyen. Analizando los coeficientes líderes de estos polinomios, obtendremos una cadena ascendente de elementos en R, la cual, al estabilizarse, nos conducirá a una contradicción.

Sea $\mathfrak{b} \subseteq R[x]$, con $\mathfrak{b} \neq \langle 0 \rangle$, $\mathfrak{b} \neq R[x]$, un ideal no finitamente generado. Entonces, podemos tomar f_1 de manera que $\deg(f_1) = d_1 = \min\{\deg(g) \mid g \in \mathfrak{b}, g \neq 0\}$, y definimos $\mathfrak{a}_1 = \langle f_1 \rangle$. Es claro que $\mathfrak{a}_1 \subsetneq \mathfrak{b}$. Realizamos de nuevo el proceso de una manera similar: tomamos $f_2 \in \mathfrak{b} \backslash \mathfrak{a}_1$ de manera que f_2 tenga grado mínimo, y definimos $\mathfrak{a}_2 = \langle f_1, f_2 \rangle$. Repitiendo esta idea, encontramos una sucesión de polinomios $f_1, f_2, f_3, ...$ cuyos grados cumplen que $d_1 \leq d_2 \leq d_3 \leq ...$, y permiten construir una cadena estrictamente creciente de ideales donde el elemento n de la cadena es $\mathfrak{a}_n = \langle f_1, f_2, ..., f_n \rangle$.

Denotamos al coeficiente principal de f_i como r_i. Entonces, considerando estos elementos, podemos construir una cadena ascendente de ideales en R: $\langle r_1 \rangle \subset \langle r_1, r_2 \rangle \subset \langle r_1, r_2, r_3 \rangle \subset ....$ Por hipótesis, esta cadena se estabiliza, de manera que existe un entero positivo N tal que $r_N = \alpha_1 r_1 + ... + \alpha_{N-1} r_{N-1}$. Definimos ahora el polinomio $g_N \in \mathfrak{b}$ como:

$$g_N = f_N - \sum_{i=1}^{N-1} \alpha_i x^{d_N - d_i} f_i$$

con el objetivo de que, al multiplicar en cada término de la suma, el grado del polinomio sea N. Desarrollamos a continuación la suma:

$$g_N = r_N x^{d_N} + (...) - \sum_{i=1}^{N-1} \alpha_i x^{d_N - d_i}(r_i x^i + (...)) = \sum_{i=1}^{N-1} \alpha_i r_i x^{d_N} + (...) - \sum_{i=1}^{N-1} \alpha_i r_i x^{d_N} + (...)$$

por lo que concluimos que el coeficiente de x^{d_N} es nulo, y $\deg(g_N) < d_N$. Además, de la definición de g_N, observamos que, necesariamente, $g_N \notin \mathfrak{a}_{N-1}$, ya que, de otra manera, implicaría que $f_N \in \mathfrak{a}_{N-1}$. Es decir, $g_N, f_N \in \mathfrak{b}\backslash\mathfrak{a}_{N-1}$, pero esto contradice la minimalidad del grado de f_N por lo que hemos obtenido nuestra contradicción, y concluimos que todo ideal es finitamente generado. □

Este resultado, al extenderse inductivamente a múltiples variables, garantiza que el anillo de polinomios en d variables sea noetheriano, siempre que el anillo R lo sea.

Corolario B.0.2. *Si R es un anillo noetheriano, entonces $R[x_1, ..., x_d]$ también lo es.*

Demostración.

Por el teorema anterior (B.0.1), si $d = 1$, el resultado es cierto. Supongamos que, si R es noetheriano, entonces el anillo $A' = R[x_1, ..., x_{d-1}]$ también lo es, y consideremos $A = R[x_1, ..., x_d]$. El resultado es automático considerando $A = A'[x_d]$ y aplicando de nuevo el teorema de Hilbert sobre bases finitas. □