UNIVERSIDAD DE EL SALVADOR

FACULTAD MULTIDISCIPLINARIA ORIENTAL

DEPARTAMENTO DE CIENCIAS NATURALES Y MATEMÁTICA

SECCIÓN DE MATEMÁTICA.

TEMA:

ANILLOS DE NOETHER Y DE ARTIN.

PRESENTADO POR:

CRISTIAN ERNESTO MARTÍNEZ MOREJÓN.

PEDRO VALENTÍN BATRES PÁIZ.

PARA OPTAR AL TITULO DE:

LICENCIADO EN MATEMÁTICA

CIUDAD UNIVERSITARIA DE ORIENTE, FEBRERO DE 2011

UNIVERSIDAD DE EL SALVADOR

FACULTAD MULTIDISCIPLINARIA ORIENTAL

DEPARTAMENTO DE CIENCIAS NATURALES Y MATEMÁTICA

SECCIÓN DE MATEMÁTICA.

TEMA:

ANILLOS DE NOETHER Y DE ARTIN.

PRESENTADO POR:

CRISTIAN ERNESTO MARTÍNEZ MOREJÓN.

PEDRO VALENTÍN BATRES PÁIZ.

ASESOR DIRECTOR:

LIC. JOSÉ FREDY VÁSQUEZ

ASESOR METODOLÓGICO:

LIC. SONIA DEL CARMEN MARTÍNEZ DE LÓPEZ

PARA OPTAR AL TITULO DE:

LICENCIADO EN MATEMÁTICA

CIUDAD UNIVERSITARIA DE ORIENTE, FEBRERO DE 2011

UNIVERSIDAD DE EL SALVADOR.

RECTOR: MSC. RUFINO ANTONIO QUEZADA SÁNCHEZ.

VICERRECTOR ACADEMICO: MSC. MIGUEL ÁNGEL PÉREZ RAMOS.

VICERRECTOR ADMINISTRATIVO: MSC. ÓSCAR NOÉ NAVARRETE.

SECRETARIO GENERAL: LIC. DOUGLAS VLADIMIR ALFARO CHÁVEZ.

FACULTAD MULTIDISCPLINARIA ORIENTAL.

DECANA INTERINA: DRA. ANA JUDITH GUATEMALA DE CASTRO.

SECRETARIO: ING. JORGE ALBERTO RUGAMAS RAMÍREZ.

ADMINISTRADOR ACADÉMICO: LIC. CRISTOBAL HERNÁN RÍOS BENÍTEZ**.**

DEPARTAMENTO DE CIENCIA NATURALES Y MATEMÁTICAS.

JEFE: LIC. ABEL MARTINEZ LÓPEZ

SECCIÓN DE MATEMATICAS.

COORDINADORA: LICDA. MARIA OLGA QUINTANILLA DE LOVO.

<u>TRABAJO DE GRADUACIÓN APROBADO POR:</u>

Lic. Raúl Antonio Alfaro Hernández.
Coordinador de Procesos de Graduación
Depto. Ciencia Naturales y Matemática.

Lic. José Fredy Vásquez.
Asesor Director.

Licda. Sonia del Carmen Martínez de López.
Asesor Metodológico.

AGRADECIMIENTOS.

- A **Dios** todo poderoso por darnos salud, confianza y la sabiduría para lograr levantarnos ante las adversidades surgidas en nuestra carrera.

- Al **Consejo de Becas Estudiantiles de la Universidad de El Salvador,** por los medios económicos que me han aportado durante mi carrera. (**Cristian Ernesto Martínez Morejón**).

- A nuestros **familiares, amig@s** por sus consejos y apoyo incondicional para alcanzar este triunfo.

- A nuestros Asesores **Licda. Sonia del Carmen Martínez de López, Lic. José Fredy Vásquez** por haber aceptado colaborar con su experiencia y dedicación para lograr terminar con éxito nuestro trabajo de tesis.

- A todos los maestros que participaron en nuestra formación académica, en especial al **Lic. José Fredy Vásquez** por sus aportes valiosos en todo el transcurso de nuestra carrera e investigación, pues siempre estuvo disponible y muchas veces hizo a un lado sus actividades para colaborar con nosotros.

- A todos los que estuvieron pendientes de cada una de las defensas ya que de esa forma colaboraron con el desarrollo de la investigación.

Cristian Ernesto Martínez Morejón.
Pedro Valentin Batres Páiz.

<u>INDICE DE CONTENIDOS.</u>

BREVE DESCRIPCION DE LA INVESTIGACION:

El desarrollo de este trabajo se realiza en tres capítulos, de los cuales a continuación se hace una breve descripción:

El **capítulo I** se ha dividido en dos secciones. En la primera se enuncian algunas definiciones y propiedades de anillos, ideales y módulos, que se utilizan en la prueba de las proposiciones de este documento. En la segunda se hace una introducción a los anillos de fracciones, su construcción y propiedades elementales, finalizando con la contracción y extensión de ideales en anillos de fracciones.

En el **capítulo II** se estudia uno de los elementos importantes del algebra conmutativa; la descomposición de ideales (es decir, ideales que se pueden escribir como una intersección finita de ciertos ideales; los ideales **primarios**) y se desarrollan algunas propiedades. Luego se definen los elementos enteros y las extensiones de anillos, estando especialmente interesados en aquellos anillos $\mathbf{B}$ tal que todos sus elementos son enteros sobre un subanillo $\mathbf{A}$, de $\mathbf{B}$ (**Extensiones enteras de anillos**).

En el **capítulo III** se procede con la parte fundamental de esta investigación, definir la estructura de los anillos que satisfacen la condición de cadena ascendente (**Noetherianos**) y descendente (**Artinianos**), en ideales y algunas de sus propiedades.

En cada capítulo se encuentran resultados donde se da una demostración, la cual puede ser no única por lo que no se descarta la posibilidad de mejorarla.

INTRODUCCIÓN.

El propósito de este trabajo es brindar una introducción en el estudio de los anillos de cadena con el objetivo principal de presentar algunos resultados sobre anillos noetherianos y artinianos.

Se inicia haciendo un enfoque teórico de conceptos y propiedades algebraicas de anillos, ideales y módulos; elementos que se han considerado necesarios para el desarrollo del resto del trabajo. Luego se hace una introducción a dos de los más importantes instrumentos del algebra conmutativa, como son la formación de anillos de fracciones (**su construcción**) y el proceso asociado de localización, que desde un punto de vista algebraico permite de forma dual al anillo cociente, estudiar los ideales primos contendidos en un ideal primo de $\mathbf{A}$.

Se exponen la existencia de descomposiciones primarias de ideales y las extensiones enteras; definiendo ideales primarios, elementos enteros, dominios normales, clausura entera, estableciendo los teoremas clásicos sobre la unicidad en la descomposición primaria (**los teoremas primero y segundo de unicidad**); resultados que relacionan cadenas de ideales primos en extensiones de anillos (**los teoremas del Ascenso y del Descenso de Cohen-Seidenberg**). Además, se investiga el comportamiento de ideales primarios y extensiones enteras con respecto a los procesos de localización.

Se introduce el concepto de dimensión de Krull, de anillos, siendo de mayor prioridad los anillos con una dimensión de Krull igual a cero. Posteriormente se hace uso de las condiciones de cadenas ascendente y descendente en ideales, para definir la estructura de una clase muy importante de anillos como son los anillos noetherianos y artinianos. La importancia de ellos es que son mínimamente tratables; es decir que todo ideal admite un sistema finito de generadores. Ya definidos los anillos de cadenas (**Es decir; anillos donde el conjunto de sus ideales está totalmente ordenado con respecto a la relación de inclusión)**, se pasa a la deducción de un número de propiedades de carácter noetherianas, artinianas y su relación; los anillos artinianos se pueden caracterizar como los anillos noetherianos de dimensión cero (**El teorema de caracterización de los anillos de artin)**, se desarrollarán elementos, que relacionan descomposiciones primarias de ideales, extensiones enteras y la existencia de sólo un número finito de ideales primos minimales en anillos de noether y maximales en un anillo de artin, el teorema de estructura para anillos artinianos, (**Todo anillo de artin es el producto directo finito de anillos locales artinianos**), incluyendo la demostración de uno de los teoremas más importantes del álgebra conmutativa, el **teorema de la base de Hilbert**, que es una herramienta poderosa para probar, en casos específicos, la noetherianidad de un anillo.

NOTA HISTORICA.

Sobre el siglo XIX, matemáticos como Klein, Hilbert, Minskoski, Noether, Artin, Dedekind trabajaban entre otras cosas en **Geometría Algebraica y Teoría de Números**, tras un exhaustivo estudio, se dieron cuenta de que ambos campos, tenían elementos en común, así que los unificaron para poder argumentarlos, dando lugar a una nueva área de la matemática a la que se le llamo **Algebra Conmutativa**, que es el campo de estudio de los anillos conmutativos, sus ideales, módulos, álgebras; con objeto central el ideal primo, el cual proporciona una generalización de los números primos de la aritmética.

En el caso de la geometría algebraica, el álgebra conmutativa se encarga de estudiar el anillo de polinomios en varias variables sobre un cuerpo, mientras que en la teoría de números el objeto de estudio es el anillo de los números enteros.

Emmy Noether y el inicio del Algebra Abstracta.

Herman Weyl divide la producción científica de Noether en tres épocas agrupadas en los periodos 1908-1919, **1920-1926** y 1927-1936.

Las investigaciones de Emmy Noether en el periodo de **1920-1926** están en torno a la teoría de anillos conmutativos y de lo que, en su tiempo, fue llamado **La Teoría General de Ideales**. Uno de los trabajos más importantes que realizó en esta área es: **Idealtheorie in Ringbereichen (Teoría de ideales en los dominios de integridad)** de 1921. El cual fue catalogado por I. Kaplansky de revolucionario por su enfoque abstracto muy novedoso por aquel tiempo, y en los que además obtuvo resultados nuevos y significativos que no habían sido probados, en los casos particulares. Sus resultados indicaban de forma tangible el potencial del enfoque axiomático así como presagiaban la riqueza de nuevas matemáticas.

Históricamente la teoría de anillos e ideales tiene dos puntos de partida: **La teoría de ideales de anillos de enteros algebraicos** de R. Dedekind y **la teoría de ideales en anillos de polinomios** iniciadas por Hilbert, Lasker y Macaulay. Sin embargo estas dos teorías se desarrollaron para problemas completamente diferentes. En el primer caso, el problema central era el de factorización, esto es, la formulación de un teorema fundamental de la aritmética (**cada número entero se expresa de forma única como el producto de números primos**). Mientras que en el caso de ideales en anillos de polinomios, las cuestiones que se planteaban eran la determinación de los ceros de un ideal (esto es, las soluciones de un sistema de ecuaciones polinómicas), y el establecimiento de las condiciones necesarias y suficientes para que un polinomio pertenezca a un ideal.

La teoría de anillos e ideales estaba en aquel tiempo en su etapa inicial R. Dedekind en 1871 introduce el término de ideal, para anillos de enteros algebraicos aunque no el concepto moderno (brevemente por un entero algebraico se extiende a un número complejo que es raíz de un polinomio mónico con coeficientes enteros). Posteriormente Hilbert en 1894 usó el término de anillo también en el contexto de números algebraicos.

Los conceptos modernos de anillo, ideal y módulo sobre un anillo aparecen por primera vez en el artículo de noether (aunque parece que la definición actual de anillo conmutativo fue previamente establecida por M. Sono en 1917). Noether extiende la definición de ideal en un anillo (de enteros o de polinomios), a anillos conmutativos en abstracto. Pero sin duda el concepto más importante es el de la **condición de cadena ascendente para ideales**.

Esta condición había sido estudiada por Dedekind 1894 y Lasker en 1905. La principal contribución de Noether fue definirla en un contexto abstracto y mostrar su importancia y naturalidad. Es fundamentalmente por el artículo "**Teoría de ideales en los dominios de integridad**" que los anillos que verifican la condición de cadena ascendente se llaman **anillos noetherianos**.

En 1890 Hilbert había probado el, hoy en día conocido como, **Teorema de la base de Hilbert** para el cuerpo $\mathbb{C}$ de los números complejos, en el que establece que todo ideal en el anillo de polinomios $\mathbb{C}[X_1, \ldots, X_n]$ es finitamente generado. Noether demuestra que este resultado también es cierto para anillos noetherianos, es decir: Un anillo conmutativo $\mathbf{A}$ satisface la condición de cadena descendente para ideales si, y solamente si todo ideal $\mathfrak{a}$ de $\mathbf{A}$ es finitamente generado. La otra forma familiar equivalente a la condición de cadena descendente es la condición de maximalidad. Uno de los objetivos principales de Noether es obtener, en el contexto general de anillos conmutativos noetherianos, la **descomposición primaria de ideales**. Se explica esto, en el anillo de los números enteros $\mathbb{Z}$ todo ideal es principal y entonces por el teorema fundamental de la aritmética, todo ideal en $\mathbb{Z}$ se expresa como producto finito de ideales primos. Sin embargo, aún en el caso noetheriano, no cabe esperar dicha descomposición de ideales, el concepto que aquí aparece, es el ideal **primario**.

Noether moviéndose de lo concreto, anillos de polinomios, a lo abstracto, un anillo conmutativo noetheriano, obtiene cuatro teoremas de descomposición de ideales. De estos cuatro, el segundo, es conocido como el teorema de **Lasker-Noether** (**Todo ideal propio $\mathfrak{a}$ en un anillo noetheriano $\mathbf{A}$, admite una descomposición primaria minimal).** Noether demuestra que el conjunto de ideales primos **asociados** a un ideal descomponible es independiente de la descomposición elegida. Por otro lado también demuestra la unicidad de las **componentes aisladas**.

La unicidad de las **componentes aisladas** y de los **primos asociados** a una descomposición primaria minimal son ejemplos de resultados importantes que noether obtuvo y que no aparecían en los trabajos anteriores de Lasker y Macaulay en el contexto concreto de anillos de polinomios.

Poco después de Noether y de su condición de cadena ascendente E. Artin en 1927 descubre anillos de condiciones mínimas (**anillos que satisfacen la condición de cadena descendente**) para ideales, los llamados en su honor, anillos de Artin.

JUSTIFICACIÓN

El álgebra conmutativa, es una de las ramas importantes en el área de matemática abstracta, y en ella se encuentran una serie de temas que sirven como fundamentación básica para el estudio de otros campos.

La motivación de este trabajo es dar a conocer resultados sobre la construcción de anillos de fracciones, existencia descomposición primaria de ideales, extensiones enteras, anillos noetherianos y artinianos; con mayor interés aquellas propiedades que se relacionan con las operaciones de localización y anillos de cadenas, con el propósito principal de crear las bases y la inquietud en los estudiantes de licenciatura en matemática, para que realicen estudios de los temas desarrollados en este documento en otras estructuras algebraicas.

La realización de este trabajo proporciona herramientas en estudios del álgebra conmutativa. Por tal razón se ha diseñado de manera que contenga desde definiciones, proposiciones y corolarios, con mayor detalle con la intención de mejorar la compresión del lector.

Para la lectura de este trabajo, sólo se requiere conocimientos básicos sobre teoría de anillos e ideales y la noción de módulo, no obstante para el lector no familiarizado con estos elementos, se incluye una sección que contiene definiciones y resultados, que se utilizan en la demostración de las proposiciones que se presentan.

OBJETIVOS

Objetivos Generales:

- Aplicar razonamientos lógicos adquiridos en la formación académica como egresado en la licenciatura en matemática, para presentar temas en álgebra conmutativa de manera, que flexibilice la comprensión del lector.
- Presentar un estudio de propiedades sobre anillos de fracciones, descomposición primaria de ideales, extensiones enteras y anillos de cadenas (**Noetherianos y Artinianos**).

Objetivos Específicos:

- Elaborar un trabajo que proporcione elementos necesarios para estudios posteriores en teorías del álgebra conmutativa.
- Proporcionar al lector elementos relacionados con la teoría de anillos, ideales y la construcción de anillos de fracciones.
- Enriquecer el conocimiento sobre la existencia de descomposiciones primarias de ideales, extensiones enteras y su relación bajo las operaciones de localización.
- Exponer algunas propiedades de los anillos Noetherianos y Artinianos.

CAPITULO I: ELEMENTOS INTRODUCTORIOS.

Este capítulo se ha dividido en dos secciones. En la primera se enuncian algunas definiciones y propiedades de anillos, ideales y módulos, que se utilizan en la prueba de cada una de las proposiciones de este documento. En la segunda se hace una introducción a los anillos de fracciones, su construcción y propiedades elementales.

Sección 1: Preliminares:

1.1: Anillos e ideales.

Definición 1.1.1: Un **anillo conmutativo con unidad** es un conjunto $\mathbf{A}$ no vacío, dotado de dos operaciones binarias denotadas por $(+)$ y $(\cdot)$ las cuales se llamarán suma y producto respectivamente, con las cuales se cumplen:

$\mathbf{A}_1$: $(\mathbf{A}, +)$ es un grupo abeliano.

$\mathbf{A}_2$: (*La multiplicación es asociativa*), para cada, a, b, y $c \in \mathbf{A}$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

$\mathbf{A}_3$: (*La multiplicación es distributiva respecto a la adición*), para cada, a, b, y $c \in \mathbf{A}$, $a \cdot (b + c) = a \cdot b + a \cdot c$.

$\mathbf{A}_4$: (*La multiplicación es conmutativa*), para todo, $a, b \in \mathbf{A}$, $a \cdot b = b \cdot a$.

$\mathbf{A}_5$: (*Existencia de elemento unidad*), existe $1 \in \mathbf{A}$ tal que $a \cdot 1 = 1 \cdot a = a$, para todo $a \in \mathbf{A}$.

Nota: A lo largo de este documento:

1. La palabra "**anillo**" denotará a un anillo conmutativo con elemento unidad.
2. El elemento 1 de $\mathbf{A}$ será denotado por $1_{\mathbf{A}}$.
3. Si $1 = 0$ en $\mathbf{A}_5$, entonces $\mathbf{A}$ es el **anillo cero**. El cual se indica por $\mathbf{0}$.

Definición 1.1.2: Sea $\mathbf{A}$ un anillo y $\mathbf{B} \subseteq \mathbf{A}$. Diremos que $\mathbf{B}$, es un **subanillo** de $\mathbf{A}$, si:

(i) $\mathbf{B}$ es un subgrupo de $\mathbf{A}$.

(ii) $\mathbf{B}$ es cerrado para la multiplicación en $\mathbf{A}$.

(iii) $1_{\mathbf{A}} \in \mathbf{B}$.

Definición 1.1.3: Un **homomorfismo de anillos** es una función f de un anillo $\mathbf{A}$ en un anillo $\mathbf{B}$ tal que:

1. $f(a+b) = f(a) + f(b)$.
2. $f(a \cdot b) = f(a) \cdot f(b)$.
3. $f(1_{\mathbf{A}}) = 1_{\mathbf{B}}$.

Para todo a y $b \in \mathbf{A}$.

Definición 1.1.4: Sea $\mathbf{A}$ un anillo. Un elemento $a \in \mathbf{A}$ es un **divisor de cero** en $\mathbf{A}$, si divide a 0, es decir, si existe $b \in \mathbf{A}$ no nulo, tal que $ab = 0$.

Definición 1.1.5: Un anillo $\mathbf{A} \neq \mathbf{0}$, sin divisores de cero se llama **dominio de integridad** o simplemente **dominio**.

Definición 1.1.6: Un elemento $a \in \mathbf{A}$ es **unidad** en $\mathbf{A}$, si divide a 1, es decir, si existe $b \in \mathbf{A}$ tal que $ab = 1$, el cual se denomina **inverso** de a.

Definición 1.1.7: Un **cuerpo** es un anillo $\mathbf{A}$ en el que $1 \neq 0$ y cada elemento no nulo es una unidad.

Definición 1.1.8: Un elemento $a \in \mathbf{A}$ se llama **nilpotente** si existe $n \in \mathbb{N}$, tal que $a^n = 0$.

Si $\mathbf{A}$ no tiene elementos nilpotentes se dice que es un anillo **reducido**.

Observación:

1. Si $\mathbf{A} \neq \mathbf{0}$, un elemento nilpotente es divisor de cero. Pero no recíprocamente en general.

Definición 1.1.9: Un **ideal** de un anillo $\mathbf{A}$ es un subconjunto $\mathfrak{a}$ de $\mathbf{A}$ tal que:

(i) Si $a, b \in \mathfrak{a}$, entonces $a + b \in \mathfrak{a}$.

(ii) $ab \in \mathfrak{a}$, para todo $a \in \mathfrak{a}$ y $b \in \mathbf{A}$.

Observación: Evidentemente, $\{\mathbf{0}\}$ y $\mathbf{A}$ son ideales en $\mathbf{A}$, denominados **ideal cero** e **ideal total**, respectivamente. Un ideal $\mathfrak{a}$ de $\mathbf{A}$ es **propio** si $\mathfrak{a} \neq \mathbf{A}$, y **trivial** si $\mathfrak{a} = \{\mathbf{0}\}$.

Definición 1.1.10: Si $\mathfrak{a}, \mathfrak{b}$ son ideales en un anillo $\mathbf{A}$, su **ideal cociente** es:

$$(\mathfrak{a} : \mathfrak{b}) = \{x \in \mathbf{A} \mid x\mathfrak{b} \subseteq \mathfrak{a}\}.$$

En particular:

1. $(0 : \mathfrak{b})$ es llamado el **anulador** de $\mathfrak{b}$ y se indica por $\operatorname{Ann}(\mathfrak{b})$. Se define como

$$\operatorname{Ann}(\mathfrak{b}) = \{\, x \in \mathbf{A} \mid x\mathfrak{b} = 0 \,\}$$

2. Si $\mathfrak{b} = (x)$, se escribe $(\mathfrak{a} : x)$ y $\operatorname{Ann}(x)$ en lugar de $(\mathfrak{a} : (x))$ y $\operatorname{Ann}((x))$.

3. Si $\mathfrak{a}$ es un ideal en $\mathbf{A}$ y $x \in \mathbf{A}$ entonces $(\mathfrak{a} : x) = \operatorname{Ann}(\bar{x})$ donde $\bar{x} = x + \mathfrak{a} \in \mathbf{A}/\mathfrak{a}$.

Proposición 1.1.11: Si $\mathfrak{a}, \mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n$ y $\mathfrak{b}$ son ideales en un anillo $\mathbf{A}$, entonces:

(i) $\mathfrak{a} \subseteq (\mathfrak{a} : \mathfrak{b})$.

(ii) $\left(\bigcap_{j=1}^{n} \mathfrak{a}_j : \mathfrak{b}\right) = \bigcap_{j=1}^{n} (\mathfrak{a}_j : \mathfrak{b})$.

Definición 1.1.12: Sea $\mathbf{A}$ un anillo. Se dice que un ideal $\mathfrak{a}$ es **finitamente generado** si existen $\{a_1, \ldots, a_r\} \in \mathfrak{a}$ tal que:

$$\mathfrak{a} = \sum_{j=1}^{n} a_j \mathbf{A}.$$

Proposición 1.1.13: Sea $f:\mathbf{A}\to\mathbf{B}$ un homomorfismo de anillos y $\mathfrak{a}$ un ideal en $\mathbf{A}$ tal que $\mathfrak{a}\subseteq\mathbf{ker}(f)$, entonces f induce un homomorfismo $\overline{f}:\mathbf{A}/\mathfrak{a}\to\mathbf{B}$ definido por: $\overline{f}(x+\mathfrak{a})=f(x)$. En particular si $\mathfrak{a}=\mathbf{ker}(f)$, existe un isomorfismo de anillos de $\mathbf{A}/\mathfrak{a}$ en $\mathbf{Im}(f)$.

Proposición 1.1.14: Existe una correspondencia biyectiva que conserva el orden entre los ideales $\mathfrak{b}$ de $\mathbf{A}$ que contienen a $\mathfrak{a}$ y los ideales $\overline{\mathfrak{b}}$ de $\mathbf{A}/\mathfrak{a}$, dada por $\mathfrak{b}=\xi^{-1}\left(\overline{\mathfrak{b}}\right)$.

Observación: De manera similar los ideal **maximales** de $\mathbf{A}$ que contienen a $\mathfrak{a}$ se corresponden con los ideales **maximales** de $\mathbf{A}/\mathfrak{a}$.

Proposición 1.1.15: Sea $\mathbf{A}=\prod_{i=1}^{n}\mathbf{A}_i$ un producto de anillos. Entonces cada ideal $\mathfrak{a}$ en $\mathbf{A}$ es de la forma $\mathfrak{a}=\prod_{i=1}^{n}\mathfrak{a}_i$, donde cada $\mathfrak{a}_i$ es ideal en $\mathbf{A}_i$.(**Cap. III. Pág. 321-322**).

Definición 1.1.16: Sea $\mathbf{A}$ un anillo. Un ideal $\mathfrak{a}$ de $\mathbf{A}$ es **principal** si existe $a\in\mathbf{A}$ tal que $\mathfrak{a}=a\mathbf{A}$.

Definición 1.1.17: Un **dominio de ideales principales** es un anillo íntegro donde cada ideal es principal.

Definición 1.1.18: Sea $\mathfrak{J}$ un conjunto no vacío. Se dice $(\mathfrak{J},\preceq)$ es un conjunto parcialmente ordenado si $\preceq$ es una relación reflexiva, transitiva tal que:

$$x\preceq y,\ \ y\preceq x \quad\Rightarrow\quad x=y.$$

Un subconjunto no vacío $\mathfrak{F}$ de $\mathfrak{J}$:

1. Es una **cadena** si está totalmente ordenado, es decir, si para cualquiera elementos $x,\ y \in \mathfrak{F},$ se tiene que $x \preceq y$ o bien $y \preceq x.$
2. $\mathfrak{F}$ es **acotado superiormente** si existe $x' \in \mathfrak{J}$ tal que $x \preceq x'$ para todo $x \in \mathfrak{F}.$

La forma más habitual de enunciar el lema de **Zorn** es la siguiente:

Proposición 1.1.19 (Lema de Zorn): Sea $(\Gamma,\ \preceq)$ un conjunto no vacío parcialmente ordenado. Si toda cadena $\mathfrak{I}$ tiene una cota superior $c_{\mathfrak{J}} \in \mathfrak{J},$ entonces $\mathfrak{J}$ tiene al menos un elemento maximal.

1.2: Ideales primos y maximales.

Definición 1.2.1: Sea $\mathbf{A}$ un anillo, un ideal propio $\mathfrak{p}$ de $\mathbf{A}$ se llama un **ideal primo** si para cualesquiera $a, b \in \mathbf{A}$ tal que $ab \in \mathfrak{p},$ se tiene $a \in \mathfrak{p}$ ó $b \in \mathfrak{p}.$

Observación: El ideal **cero** es primo si y sólo si $\mathbf{A}$ es dominio de integridad.

Definición 1.2.2: Sea $\mathbf{A}$ un anillo. Un ideal propio $\mathfrak{m}$ de $\mathbf{A}$ se llama **maximal** si para cada ideal $\mathfrak{a} \neq \mathbf{(1)}$ de $\mathbf{A}$ tal que $\mathfrak{m} \subseteq \mathfrak{a} \subsetneq \mathbf{A}$ se tiene $\mathfrak{m} = \mathfrak{a}.$

Proposición 1.2.3: Sea $\mathbf{A}$ un anillo, $\mathfrak{m}$ y $\mathfrak{p}$ ideales propios en $\mathbf{A},$ entonces:

(i) $(\mathfrak{p}$ es un ideal primo$) \Leftrightarrow (\mathbf{A}/\mathfrak{p}$ es un dominio de integridad$)$.

(ii) $(\mathfrak{m}$ es un ideal maximal $\Leftrightarrow$ $(\mathbf{A}/\mathfrak{m}$ es un cuerpo$)$.

Proposición 1.2.4: Sea $\mathbf{A}$ un anillo, si $\mathfrak{m}$ es maximal entonces es primo.

Teorema 1.2.5: Sea $\mathbf{A} \neq \mathbf{0}$ un anillo, existe al menos un ideal maximal de $\mathbf{A}$.

Corolario 1.2.6: Sea $\mathbf{A}$ un anillo y $\mathfrak{a}$ un ideal propio de $\mathbf{A}$, entonces existe un ideal maximal $\mathfrak{m}$ tal que $\mathfrak{a} \subseteq \mathfrak{m}$.

Definición 1.2.7: Un anillo $\mathbf{A}$ se llama **local** si tiene un único ideal maximal.

Observación:

1. Los cuerpos son anillos con exactamente un ideal maximal.
2. Si $\mathbf{A}$ es un anillo local con ideal maximal $\mathfrak{m}$, entonces el cuerpo $\mathbf{k} = \mathbf{A}/\mathfrak{m}$ se llama **cuerpo residual** de $\mathbf{A}$.

Proposición 1.2.8: Sea $\mathbf{A}$ un anillo y $\mathfrak{m} \neq \mathbf{A}$ tal que cada elemento $x \in \mathbf{A} - \mathfrak{m}$ es una unidad, entonces $\mathbf{A}$ es un anillo local con ideal maximal $\mathfrak{m}$.

Proposición 1.2.9:

(i) Sean $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ ideales primos en un anillo $\mathbf{A}$ y sea $\mathfrak{a}$ un ideal contenido en $\bigcup_{i=1}^{n} \mathfrak{p}_i$. Entonces $\mathfrak{a} \subseteq \mathfrak{p}_i$, para algún i.

(ii) Sean $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ ideales en un anillo $\mathbf{A}$ y sea $\mathfrak{p}$ un ideal primo que contiene a $\bigcap_{i=1}^{n} \mathfrak{a}_i$. Entonces $\mathfrak{p} \supseteq \mathfrak{a}_i$ para algún i. Si $\mathfrak{p} = \bigcap_{i=1}^{n} \mathfrak{a}_i$, entonces $\mathfrak{p} = \mathfrak{a}_i$ para algún i.

Proposición 1.2.10: El conjunto $\mathfrak{R}_{\mathbf{A}} = \{x \in \mathbf{A} \mid x^n = 0 \text{ para algún } n \in \mathbb{N}\}$ es un ideal de $\mathbf{A}$. El ideal $\mathfrak{R}_{\mathbf{A}}$ se denomina **nilradical** de $\mathbf{A}$.

Definición 1.2.11: El **nilradical** $\mathfrak{R}_{\mathbf{A}}$ de $\mathbf{A}$ se define como la intersección de todos los ideales primos de $\mathbf{A}$; es decir:

$$\mathfrak{R}_{\mathbf{A}} = \bigcap \{\, \mathfrak{p} \mid \mathfrak{p} \text{ es un ideal primo de } \mathbf{A}\}.$$

Definición 1.2.12: El **radical de Jacobson** $\mathfrak{I}_{\mathbf{A}}$ de $\mathbf{A}$ se define como la intersección de todos los ideales maximales de $\mathbf{A}$; es decir:

$$\mathfrak{I}_{\mathbf{A}} = \bigcap \{\, \mathfrak{m} \mid \mathfrak{m} \text{ es un ideal maximal de } \mathbf{A}\}.$$

Definición 1.2.13: Sea $\mathfrak{a}$ un ideal en un anillo $\mathbf{A}$, se llama **radical** de $\mathfrak{a}$ al ideal,

$$r(\mathfrak{a}) = \{x \in \mathbf{A} \mid x^n \in \mathfrak{a} \text{ para algún } n \in \mathbb{N}\}.$$

Se dice que $\mathfrak{a}$ es un **ideal radical** si $\mathfrak{a} = r(\mathfrak{a})$.

Observación:

1. Si $\mathfrak{a} = \mathbf{A}$, de la definición, se tiene $r(\mathfrak{a}) = \mathbf{A}$, y si $\mathfrak{a} = \{\mathbf{0}\}$, entonces $r(\mathfrak{a}) = \mathfrak{R}_{\mathbf{A}}$.

Proposición 1.2.14: El **radical** de un ideal $\mathfrak{a}$ es la intersección de todos los ideales primos que contienen a $\mathfrak{a}$; es decir;

$$r(\mathfrak{a}) = \bigcap\{\mathfrak{p} \mid \mathfrak{p} \text{ es un ideal primo de } \mathbf{A} \text{ y } \mathfrak{p} \supseteq \mathfrak{a}\}.$$

Proposición 1.2.15: Si $\mathfrak{a}$, $\mathfrak{b}$ son ideales en un anillo $\mathbf{A}$, entonces:

(i) $\mathfrak{a} \subseteq r(\mathfrak{a}) = r(r(\mathfrak{a}))$.

(ii) Si $\mathfrak{a} \subseteq \mathfrak{b}$, entonces $r(\mathfrak{a}) \subseteq r(\mathfrak{b})$.

(iii) $r(\mathfrak{a} \cdot \mathfrak{b}) = r(\mathfrak{a} \cap \mathfrak{b}) = r(\mathfrak{a}) \cap r(\mathfrak{b})$.

(iv) $r(\mathfrak{a}) = (1) \Leftrightarrow \mathfrak{a} = (1)$.

(v) Si $\mathfrak{p}$ es primo, $r(\mathfrak{p}^n) = \mathfrak{p}$ para todo $n \in \mathbb{N}$.

(vi) $r(\mathfrak{a} + \mathfrak{b}) = r(r(\mathfrak{a}) + r(\mathfrak{b}))$.

Definición 1.2.16: Sea $\mathfrak{a}$ un ideal en un anillo $\mathbf{A}$, un ideal primo $\mathfrak{p}$ es **minimal** sobre $\mathfrak{a}$ si $\mathfrak{a} \subseteq \mathfrak{p}$ y para cualquier otro ideal primo $\mathfrak{q}$ tal que $\mathfrak{a} \subseteq \mathfrak{q} \subseteq \mathfrak{p}$ se tiene que $\mathfrak{q} = \mathfrak{p}$.

Nota: Se llamarán **primos minimales** de $\mathbf{A}$, a los ideales primos minimales del ideal cero.

Proposición 1.2.17: Sea $\mathbf{A}$ un anillo y $\mathfrak{a} \neq \mathbf{A}$, entonces existen ideales primos minimales sobre $\mathfrak{a}$ y cada ideal primo que contiene a $\mathfrak{a}$ contiene un ideal primo minimal sobre $\mathfrak{a}$.

Observación:

En consecuencia para cada ideal $\mathfrak{a}$ el radical de $\mathfrak{a}$ es la intersección de todos los ideales primos minimales sobre $\mathfrak{a}$.

$$r(\mathfrak{a}) = \bigcap \{ \mathfrak{p} \mid \mathfrak{p} \text{ es un ideal primo minimal sobre } \mathfrak{a} \}.$$

Este resultado será de interés cuando se tenga solamente un número finito de ideales primos minimales que contienen a $\mathfrak{a}$.

Proposición 1.2.18: Sea D el conjunto de los divisores de cero de $\mathbf{A}$, entonces:

$$\mathrm{D} = \bigcup_{x \neq \mathbf{0}} r\left(\mathrm{Ann}(x)\right) = \bigcup_{x \neq \mathbf{0}} r(\mathbf{0} : x).$$

Proposición 1.2.19: Sea $\mathbf{A}$ un anillo $\mathfrak{p}$ un ideal tal que $\mathfrak{p} \neq \mathbf{A}$. Entonces los siguientes enunciados son equivalentes:

(i) $\mathfrak{p}$ es primo;

(ii) Si $\mathfrak{ab} \subseteq \mathfrak{p}$, entonces $\mathfrak{a} \subseteq \mathfrak{p}$, ó $\mathfrak{b} \subseteq \mathfrak{p}$, para cualesquiera ideales $\mathfrak{a}, \mathfrak{b}$ de $\mathbf{A}$.

Definición 1.2.20: Un anillo $\mathbf{A}$ se llama **semilocal** si tiene sólo un número finito de ideales maximales.

Definición 1.2.21: Dos ideales en un anillo $\mathbf{A}$ se llaman **comaximales** ó **primos relativos** si $\mathfrak{a} + \mathfrak{b} = (1)$.

Proposición 1.2.22: Sea $\mathbf{A}$ un anillo, $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n,$ ideales de $\mathbf{A}$ y se considera la aplicación canónica:

$$\varphi : \mathbf{A} \to \prod_{i=1}^{n} \left(\mathbf{A}/\mathfrak{a}_i \right), \quad \varphi(a) = \left(a + \mathfrak{a}_1, \ldots, a + \mathfrak{a}_n \right), \text{ con } a \in \mathbf{A}.$$

Entonces se verifican las siguientes propiedades:

(i) Si $\mathfrak{a}_i$ y $\mathfrak{a}_j$ son comaximales, cuando $i \neq j$, entonces $\mathfrak{a}_1 \cdot \cdot \cdot \mathfrak{a}_n = \mathfrak{a}_1 \cap, \ldots, \cap \mathfrak{a}_n$.

(ii) φ es sobreyectiva si y sólo si $\mathfrak{a}_i$ y $\mathfrak{a}_j$ son comaximales con $i \neq j$ para todos los índices i, j.

(iii) φ es inyectiva si y sólo si $\mathfrak{a}_1 \cap, \ldots, \cap \mathfrak{a}_n = \mathbf{0}$.

1.3: Extensión y contracción de ideales.

Sea $f : \mathbf{A} \to \mathbf{B}$ un homomorfismo de anillos. Si $\mathfrak{a}$ es un ideal en $\mathbf{A}$, el conjunto $f(\mathfrak{a})$ no es necesariamente un ideal en $\mathbf{B}$.

Definición 1.3.1: Sea $f : \mathbf{A} \to \mathbf{B}$ un homomorfismo de anillos. Si $\mathfrak{a}$ es un ideal en $\mathbf{A}$. Se define la **extensión** de $\mathfrak{a}$ como el ideal $\mathbf{B} f(\mathfrak{a})$ generado por $f(\mathfrak{a})$ en $\mathbf{B}$, denotado por, $\mathfrak{a}^e$. En forma más explícita se puede definir $\mathfrak{a}^e$ como el conjunto:

$$\mathfrak{a}^e = \left\{ x \in \mathbf{B} \mid x = \sum_{finita} y_i f(x_i), \text{ donde } x_i \in \mathfrak{a}, \; y_i \in \mathbf{B} \right\}.$$

Definición 1.3.2: Sea $f : \mathbf{A} \to \mathbf{B}$ un homomorfismo de anillos. Si $\mathfrak{b}$ es un ideal de $\mathbf{B}$, entonces $f^{-1}(\mathfrak{b})$ es siempre un ideal de $\mathbf{A}$, llamado la **contracción** de $\mathfrak{b}$, denotado por $\mathfrak{b}^c$.

Observación:

1. Si $\mathfrak{a}$ es un ideal primo en $\mathbf{A}$, $\mathfrak{a}^e$ no ha de ser necesariamente un ideal primo en $\mathbf{B}$.
2. Si $\mathfrak{b}$ es primo, entonces $\mathfrak{b}^c$ es primo.

Proposición 1.3.3: Sea $f : \mathbf{A} \to \mathbf{B}$ un homomorfismo de anillos.

(i) Si $\mathfrak{a}_1 \subseteq \mathfrak{a}_2$ son ideales de $\mathbf{A}$, entonces $\mathfrak{a}_1^e \subseteq \mathfrak{a}_2^e$.

(ii) Si $\mathfrak{b}_1 \subseteq \mathfrak{b}_2$ son ideales de $\mathbf{B}$, entonces $\mathfrak{b}_1^c \subseteq \mathfrak{b}_2^c$.

(iii) Si $\mathfrak{a}$ es un ideal de $\mathbf{A}$, entonces $\mathfrak{a} \subseteq \mathfrak{a}^{ec}$.

(iv) Si $\mathfrak{b}$ es un ideal de $\mathbf{B}$, entonces $\mathfrak{b} \supseteq \mathfrak{b}^{ce}$.

(v) Si $\mathfrak{a}$ es un ideal de $\mathbf{A}$, entonces $\mathfrak{a}^e = \mathfrak{a}^{ece}$.

(vi) Si $\mathfrak{b}$ es un ideal de $\mathbf{B}$, entonces $\mathfrak{b}^c = \mathfrak{b}^{cec}$.

Proposición 1.3.4: Sea $f : \mathbf{A} \to \mathbf{B}$ un homomorfismo de anillos, $\mathfrak{a}_1, \mathfrak{a}_2$ ideales de $\mathbf{A}$ y $\mathfrak{b}_1, \mathfrak{b}_2$ ideales de $\mathbf{B}$. Entonces:

(i) $(\mathfrak{a}_1 + \mathfrak{a}_2)^e = \mathfrak{a}_1^e + \mathfrak{a}_2^e$.

(ii) $\left(\mathfrak{a}_1 \cap \mathfrak{a}_2\right)^e \subseteq \mathfrak{a}_1^e \cap \mathfrak{a}_2^e$.

(iii) $\left(\mathfrak{a}_1 \mathfrak{a}_2\right)^e = \mathfrak{a}_1^e \mathfrak{a}_2^e$.

(iv) $\left(r\left(\mathfrak{a}_1\right)\right)^e \subseteq r\left(\mathfrak{a}_1^e\right)$.

(v) $\left(\mathfrak{b}_1 \cap \mathfrak{b}_2\right)^c = \mathfrak{b}_1^c \cap \mathfrak{b}_2^c$.

Proposición 1.3.5: Si $\alpha : \mathbf{A} \rightarrow \mathbf{B}$ es un homomorfismo de anillos sobreyectivo y $\mathfrak{a}$ es un ideal de $\mathbf{A}$, entonces $\alpha\left(\mathfrak{a}\right)$ es un ideal en $\mathbf{B}$.

1.4: Módulos.

A continuación se define la estructura de módulo y se enuncian resultados que serán de mucha utilidad.

Definición 1.4.1: Sea $\mathbf{A}$ un anillo (conmutativo con elemento unidad). Se llamará $\mathbf{A}-$ módulo al par $\left(\mathbf{M}, \mu\right)$ formado por un grupo aditivo abeliano $\mathbf{M}$ y una aplicación:

$$\mu : \mathbf{A} \times \mathbf{M} \rightarrow \mathbf{M},$$

que actúa linealmente sobre $\mathbf{M}$, es decir, tal que:

(i) $\mu\left(a, m_1 + m_2\right) = \mu\left(a, m_1\right) + \mu\left(a, m_2\right)$;

(ii) $\mu\left(a + b, m\right) = \mu\left(a, m\right) + \mu\left(b, m\right)$;

(iii) $\mu\left(ab, m\right) = \mu\left(a, \mu\left(b, m\right)\right)$;

(iv) $\mu\left(1, m\right) = m.$ Para todo $a,\ b \in \mathbf{A}$; $m_1,\ m_2$ y $m \in \mathbf{M}$.

Definición 1.4.2: Sea $\mathbf{A}$ un anillo y $\mathbf{M}$ un $\mathbf{A}-$módulo. Un subgrupo abeliano $\mathbf{N}$ de $\mathbf{M}$ es un **submódulo** de $\mathbf{M}$, si para cada $a \in \mathbf{A}$ **y** cada $n \in \mathbf{N}$ se tiene $an \in \mathbf{N}$.

La introducción de los módulos se justifica por diversas razones. La primera es que los ideales y sus cocientes son módulos. Además que amplía el espacio y flexibiliza las operaciones básicas como, cocientes, producto y suma directa entre otras.

Observación:

1. Un ideal $\mathfrak{a}$ en $\mathbf{A}$ es un $\mathbf{A}-$módulo. En particular el anillo $\mathbf{A}$ es un $\mathbf{A}-$módulo.
2. Si $\mathbf{A}$ es un cuerpo $\mathbf{k}$, entonces $\mathbf{A}-$ modulo $\equiv \mathbf{k}-$ espacio vectorial.

En consecuencia, todas las definiciones y resultados subsiguientes sobre módulos se aplican en teoría de anillos. Pero no recíprocamente en general.

Definición 1.4.3: Sea $\mathbf{A}$ un anillo. Se dice que un $\mathbf{A}-$módulo está **finitamente generado** si posee un sistemas de generadores finito. Es decir, si existe un conjunto finito $\{m_1 , \ldots , m_n\}$ de elementos de $\mathbf{M}$ tal que:

$$\mathbf{M} = \sum_{j=1}^{n} \mathbf{A}\, m_j .$$

Proposición 1.4.4:(Lema de Nakayama). Sea $\mathbf{M}$ un $\mathbf{A}-$módulo finitamente generado. Si $\mathfrak{a}$ es un ideal en $\mathbf{A}$ contenido en el nilradical de Jacobson $\mathfrak{J}_{\mathbf{A}}$. Si $\mathfrak{a}\mathbf{M} = \mathbf{M}$ implica $\mathbf{M} = \mathbf{0}$.

Sección 2: Anillo de Fracciones.

1.5: Construcción y propiedades.

El propósito de esta sección es construir anillos de fracciones, las fracciones se construirán con elementos de un anillo $\mathbf{A}$. La construcción del cuerpo $\mathbb{Q}$ de los números racionales por medio de una relación de equivalencia definida sobre el producto cartesiano $\mathbb{Z}\times(\mathbb{Z}-\{0\})$, puede ser generalizada a un dominio de integridad arbitrario $\mathbf{A}$, obteniéndose el llamado **cuerpo de fracciones** del dominio $\mathbf{A}$. Esta situación puede ser ampliada a anillos conmutativos cualesquiera, no siendo necesariamente el nuevo objeto construido un cuerpo.

Definición 1.5.1: Sea $\mathbf{A}$ un anillo y $\mathbf{S}\subseteq\mathbf{A}$. Se dice que $\mathbf{S}$ es un sistema multiplicativo si:

(i) $1\in\mathbf{S}$.

(ii) Si $a, b\in\mathbf{S}$, entonces $ab\in\mathbf{S}$.

Dado un sistema multiplicativo $\mathbf{S}$ de un anillo arbitrario $\mathbf{A}$ se construye el anillo de fracciones con numerador en $\mathbf{A}$ y denominador en $\mathbf{S}$; para lo cual se considera en $\mathbf{A}\times\mathbf{S}$ la siguiente relación:

$$(a, s)\equiv(a', s') \Leftrightarrow \exists \quad t\in\mathbf{S} \quad \text{t. q.} \quad t(as'-a's)=0, \qquad \textbf{(}\Theta\textbf{)}$$

donde $a, a'\in\mathbf{A}$ y $s, s'\in\mathrm{S}$.

Lema 1.5.2: Sea $\mathbf{A}$ un anillo y $\mathbf{S}$ un sistema multiplicativo de $\mathbf{A}$. En el conjunto $\mathbf{A}\times\mathbf{S}$ la relación $\equiv$ es de equivalencia.

Demostración:

Reflexiva:

Sea $(a,\, s)\in \mathbf{A}\times\mathbf{S}$.

$$(as-as)=0 \quad \forall\, a,s\in\mathbf{A} \qquad \Rightarrow\ (as-as)=0 \qquad \forall\, a\in\mathbf{A} \text{ y } s\in\mathbf{S}$$

$$\Rightarrow\ u(as-as)=u(0) \quad \forall\, u\in\mathbf{S}$$

$$\Rightarrow\ \exists\ u\in\mathbf{S} \text{ t. q. } u(as-as)=0$$

$$\Rightarrow\ (a,\, s)\equiv(a,\, s).$$

$\therefore\ \equiv$ es reflexiva.

Simétrica:

Sea $(a,\, s),\ (b,\, t)\in\mathbf{A}\times\mathbf{S}$ t. q. $(a,\, s)\equiv(b,\, t)$.

$$(a,\, s)\equiv(b,\, t)\ \Rightarrow\ \exists\ u\in\mathbf{S} \text{ t. q. } u(at-bs)=0$$

$$\Rightarrow\ (-1)\big[u(at-bs)\big]=0(-1)$$

$$\Rightarrow\ u(-at+bs)=0$$

$$\Rightarrow\ u(bs-at)=0$$

$$\Rightarrow\ \exists\ u\in\mathbf{S} \text{ t. q. } u(at-bs)=0$$

$$\Rightarrow\ (b,\, t)\equiv(a,\, s).$$

$\therefore\ \equiv$ es simétrica.

Transitividad:

Sea $(a_1, s_1), (a_2, s_2)$ y $(a_3, s_3) \in \mathbf{A} \times \mathbf{S}$ t. q. $(a_1, s_1) \equiv (a_2, s_2)$ y $(a_2, s_2) \equiv (a_3, s_3)$.

$$(a_1, s_1) \equiv (a_2, s_2) \Rightarrow \exists\ t_1 \in \mathbf{S} \text{ t. q. } t_1(a_1 s_2 - a_2 s_1) = 0.$$

$$(a_2, s_2) \equiv (a_3, s_3) \Rightarrow \exists\ t_2 \in \mathbf{S} \text{ t. q. } t_2(a_2 s_3 - a_3 s_2) = 0.$$

Ahora multiplicando la primera igualdad por $t_2 s_3$ y la segunda por $t_1 s_1$ se obtiene,

$$t_2 s_3 t_1 (a_1 s_2 - a_2 s_1) = 0.$$

$$t_1 s_1 t_2 (a_2 s_3 - a_3 s_2) = 0.$$

Sumando,

$$0 = t_2 s_3 t_1 (a_1 s_2 - a_2 s_1) + t_1 s_1 t_2 (a_2 s_3 - a_3 s_2)$$

$$= t_2 s_3 t_1 (a_1 s_2) - \cancel{t_2 s_3 t_1 (a_2 s_1)} + \cancel{t_1 s_1 t_2 (a_2 s_3)} - t_1 s_1 t_2 (a_3 s_2)$$

$$= t_1\, t_2\, s_2 (a_1\, s_3) - t_1\, t_2\, s_2 (a_3\, s_1).$$

Sacando factor común $t_1\, t_2\, s_2$ resulta,

$$t_1\, t_2\, s_2 (a_1\, s_3 - a_3\, s_1) = 0.$$

Puesto que $\mathbf{S}$ es cerrado respecto a la multiplicación $t_1\, t_2\, s_2 \in \mathbf{S}$, así existe $t_1\, t_2\, s_2 \in \mathbf{S}$ tal que $t_1\, t_2\, s_2 (a_1\, s_3 - a_3\, s_1) = 0$, entonces, $(a_1, s_1) \equiv (a_3, s_3)$.

$\therefore\ \equiv$ es transitiva.

Luego $\equiv$ es una relación de equivalencia. ■

Se denota por $\frac{a}{s}$ a la clase de equivalencia de representante (a, s), es decir; al conjunto de todos los pares equivalentes a (a, s). En forma más explícita se puede definir $\frac{a}{s}$ como;

$$\frac{a}{s} = \{(b, t) \in \mathbf{A} \times \mathbf{S} \;\mid\; (a, \mathrm{s}) \equiv (b, t) \;\; b \in \mathbf{A} \text{ y } t \in \mathbf{S}\},$$

y es llamada fracción. Se indica por $\mathbf{S}^{-1}\,\mathbf{A}$ el conjunto de todas las fracciones, es decir:

$$\mathbf{S}^{-1}\,\mathbf{A} = \left\{ \frac{a}{s} \;\mid\; a \in \mathbf{A} \;\text{ y }\; s \in \mathbf{S} \right\}.$$

Se define una suma y multiplicación de fracciones en $\mathbf{S}^{-1}\,\mathbf{A}$, como sigue:

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}. \qquad [\mathbf{1}]$$

$$\frac{a}{s}\frac{b}{t} = \frac{ab}{st}. \qquad [\mathbf{2}]$$

Las cuales dan lugar a la siguiente proposición:

Proposición 1.5.3: El conjunto $\mathbf{S}^{-1}\mathbf{A}$ con las operaciones inducidas, en $[1]$ y $[2]$ define una estructura de anillo conmutativo con elemento unidad, denominado **anillo de fracciones** de $\mathbf{A}$ con respecto a S.

Demostración:

Teniendo en cuenta que se trabaja con clases de equivalencia, se demuestra inicialmente que las operaciones están definidas correctamente.

Para la suma:

Sean (a, s), (a', s'), (b, t) y $(b', t') \in \mathbf{S}^{-1}\mathbf{A}$ t. q. $(a, s) \equiv (a', s')$ y $(b, t) \equiv (b', t')$.

$$\begin{aligned}(a, s) \equiv (a', s') \quad &\Rightarrow\ \exists\, u_1 \in \mathbf{S} \ \text{ t. q. } \ u_1(as' - a's) = 0\\ &\Rightarrow\ as'u_1 - a'su_1 = 0\\ &\Rightarrow\ as'u_1 = a'su_1.\end{aligned}$$

$$\begin{aligned}(b, t) \equiv (b', t') \quad &\Rightarrow\ \exists\, u_2 \in \mathbf{S} \ \text{ t. q. } \ u_2(bt' - b't) = 0\\ &\Rightarrow\ bt'u_2 - b'tu_2 = 0\\ &\Rightarrow\ bt'u_2 = b'tu_2.\end{aligned}$$

Multiplicando la primera igualdad por $t'tu_2$ y la segunda por $s'su_1$, se tiene,

$$as'u_1(t'tu_2) = a'su_1(t'tu_2);$$

$$bt'u_2(s'su_1) = b'tu_2(s'su_1).$$

Sumando ambas expresiones,

$$as'u_1(t'tu_2) + bt'u_2(s'su_1) = a'su_1(t'tu_2) + b'tu_2(s'su_1).$$

Sacando factor común $s't'$ y st,

$$(atu_1u_2 + bsu_1u_2)s't' = (a't'u_1u_2 + b's'u_1u_2)st.$$

Como $\mathbf{S}$ es multiplicativamente cerrado, $u = u_1 u_2 \in \mathbf{S}$, entonces

$$(atu + bsu)s't' = (a't'u + b's'u)st.$$

Llegando a que,

$$((at + bs)s't' - (a't' + b's')st)u = 0.$$

Por otro lado, también $st \in \mathbf{S}$ y $s't' \in \mathbf{S}$, de donde se deduce,

$$((at + bs), st) \equiv ((a't' + b's'), s't').$$

Luego si sus representantes se relacionan, entonces las clases son iguales, es decir:

$$\frac{at + bs}{st} = \frac{a't' + b's'}{s't'}.$$

$\therefore$ La suma está bien definida en $\mathbf{S}^{-1}\mathbf{A}$.

Para el producto:

Sea (a, s), (a', s'), (b, t) y $(b', t') \in \mathbf{S}^{-1}\mathbf{A}$ t. q. $(a, s) \equiv (a', s')$ y $(b, t) \equiv (b', t')$.

$$(a, s) \equiv (a', s') \quad \Rightarrow \quad \exists \ u_1 \in \mathbf{S} \quad \text{t. q.} \quad u_1(as' - a's) = 0$$

$$\Rightarrow \quad as'u_1 = a'su_1.$$

$$(b, t) \equiv (b', t') \quad \Rightarrow \quad \exists \ u_2 \in \mathbf{S} \quad \text{t. q.} \quad u_2(bt' - b't) = 0$$

$$\Rightarrow \quad bt'u_2 = b'tu_2.$$

Multiplicando la primera igualdad por $bt'u_2$ y la segunda por $a'su_1$,

$$as'u_1\left(bt'u_2\right)=a'su_1\left(bt'u_2\right);$$

$$bt'u_2\left(as'u_1\right)=bt'u_2\left(a'su_1\right).$$

Sumando ambas expresiones,

$$as'u_1\left(bt'u_2\right)+\cancel{bt'u_2\left(a'su_1\right)}=\cancel{a'su_1\left(bt'u_2\right)}+bt'u_2\left(a'su_1\right).$$

Restando y sacando factor común u_2u_1,

$$\left(abs't'-a'b'st\right)u_2u_1=0.$$

Haciendo $u=u_2u_1$, como $\mathbf{S}$ es multiplicativamente cerrado, $u\in\mathbf{S}$, entonces

$$\left(\left(ab\right)s't'-\left(a'b'\right)st\right)u=0.$$

De forma análoga $st\in\mathbf{S}$ y $s't'\in\mathbf{S}$, de donde se deduce que,

$$\left(ab,\, st\right)\equiv\left(a'b',\, s't'\right).$$

Luego si sus representantes se relacionan, entonces las clases son iguales, es decir:

$$\frac{ab}{st}=\frac{a'b'}{s't'}.$$

$\therefore$ El producto está bien definido en $\mathbf{S}^{-1}\mathbf{A}$.

Se verifica que $\mathbf{S^{-1}A}$ satisface los axiomas de anillo conmutativo con elemento unidad.

$\mathbf{A_1}$: Se demuestra que $(\mathbf{S^{-1}A},+)$ es un grupo abeliano.

Asociatividad para la adición:

Sean $\frac{a}{s}, \frac{b}{t}$ y $\frac{m}{n} \in \mathbf{S^{-1}A}$.

$$\frac{a}{s}+\left(\frac{b}{t}+\frac{m}{n}\right)=\frac{a}{s}+\frac{bn+mt}{tn}$$

$$=\frac{atn+(bn+mt)s}{stn}$$

$$=\frac{atn+bns+mts}{stn}$$

$$=\frac{(atn+bns)+mts}{stn}$$

$$=\frac{(at+bs)n+m(ts)}{(st)n}$$

$$=\frac{at+bs}{st}+\frac{m}{n}$$

$$=\frac{at+bs}{st}+\frac{m}{n}=\left(\frac{a}{s}+\frac{b}{t}\right)+\frac{m}{n}.$$

$\therefore$ $\mathbf{S^{-1}A}$ es asociativo respecto a la adición.

La adición es conmutativa:

Sean $\dfrac{a}{s}, \dfrac{b}{t} \in \mathbf{S}^{-1}\mathbf{A}$.

$$\frac{a}{s}, \frac{b}{t} \in \mathbf{S}^{-1}\mathbf{A} \quad \Rightarrow \quad \frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st}$$

$$= \frac{bs+at}{st}$$

$$= \frac{b}{t} + \frac{a}{s}.$$

$\therefore$ $\mathbf{S}^{-1}\mathbf{A}$ es conmutativo respecto a la adicion.

Existencia de elemento identidad para la adición:

Para todo $\dfrac{a}{s}$ en $\mathbf{S}^{-1}\mathbf{A}$ existe $\dfrac{b}{t}$ en $\mathbf{S}^{-1}\mathbf{A}$ tal que $\dfrac{a}{s} + \dfrac{b}{t} = \dfrac{b}{t} + \dfrac{a}{s} = \dfrac{a}{s}$.

$$\frac{a}{s} + \frac{b}{t} = \frac{a}{s} \quad \Rightarrow \quad \frac{at+bs}{st} = \frac{a}{s}$$

$$\Rightarrow \left((at+bs), st \right) \equiv (a, s)$$

$$\Rightarrow \exists \ u \in \mathbf{S} \quad \text{t. q.} \ u\left((at+bs)s - a(st) \right) = 0$$

$$\Rightarrow u(at+bs)s - ua(st) = 0$$

$$\Rightarrow \cancel{uats} + ubss - \cancel{ua(st)} = 0$$

$$\Rightarrow ussb = 0$$

$$\Rightarrow h(b\cdot 1 - 0\cdot t) = 0, \quad \text{donde } h = uss \in \mathbf{S}, \quad t \in \mathbf{S}$$

$$\Rightarrow \exists \ h \in \mathbf{S} \ \text{ t. q. } \ h(b\cdot 1 - 0\cdot t) = 0$$

$$\Rightarrow (b, t) \equiv (0, 1)$$

$$\Rightarrow \frac{b}{t} = \frac{0}{1}.$$

Entonces $\frac{a}{s} + \frac{b}{t} = \frac{a}{s} + \frac{0}{1} = \frac{a\cdot 1 + 0\cdot s}{s\cdot 1} = \frac{a}{s}.$

Nota: La existencia de identidad por la izquierda, se obtiene de la conmutatividad de la adición.

$\therefore \ \frac{0}{1}$ es el elemento identidad para la adición en $\mathbf{S}^{-1}\mathbf{A}$.

Existencia de inverso aditivo:

Para cada $\frac{a}{s}$ en $\mathbf{S}^{-1}\mathbf{A}$ existe $\frac{b}{t}$ en $\mathbf{S}^{-1}\mathbf{A}$ tal que $\frac{a}{s} + \frac{b}{t} = \frac{b}{t} + \frac{a}{s} = \frac{0}{1}.$

$$\frac{a}{s} + \frac{b}{t} = \frac{0}{1} \quad \Rightarrow \quad \frac{at + bs}{st} = \frac{0}{1}$$

$$\Rightarrow \left((at+bs),\, st \right) \equiv (0,\, 1)$$

$$\Rightarrow \exists\ u \in \mathbf{S} \ \text{ t. q. } \ u\left((at+bs)\cdot 1 - 0 \cdot (st) \right) = 0$$

$$\Rightarrow u\left(at+bs \right) = 0$$

$$\Rightarrow u\left(bs-(-a)t \right) = 0$$

$$\Rightarrow \exists\ u \in \mathbf{S} \ \text{ t. q. } \ u\left(bs-(-a)t \right) = 0$$

$$\Rightarrow (b,\, t) \equiv (-a,\, s)$$

$$\Rightarrow \frac{b}{t} = \frac{-a}{s}.$$

Entonces $\dfrac{a}{s} + \dfrac{b}{t} = \dfrac{a}{s} + \left(-\dfrac{a}{s} \right) = \dfrac{as-as}{ss} = \dfrac{0}{ss} = \dfrac{0}{1}.$

Nota: La existencia del elemento identidad por la izquierda, se obtiene de la conmutatividad de la adición. Luego existen inversos aditivos en $\mathbf{S}^{-1}\mathbf{A}$.

$\therefore$ **($\mathbf{S}^{-1}\mathbf{A}$, +)** es un grupo abeliano.

$\mathbf{A}_2$ **: La multiplicación es asociativa:**

Sean $\frac{a}{s}$, $\frac{b}{t}$ y $\frac{m}{n} \in \mathbf{S}^{-1}\mathbf{A}$. Se demuestra que $\frac{a}{s}\left(\frac{b}{t}\frac{m}{n}\right) = \left(\frac{a}{s}\frac{b}{t}\right)\frac{m}{n}$.

$$\frac{a}{s}\left(\frac{b}{t}\frac{m}{n}\right) = \frac{a}{s}\left(\frac{bm}{tn}\right)$$

$$= \frac{a}{s}\left(\frac{bm}{tn}\right)$$

$$= \frac{abm}{stn}$$

$$= \left(\frac{ab}{st}\right)\frac{m}{n}.$$

$\therefore$ $\mathbf{S}^{-1}\mathbf{A}$ es asociativo respecto a la multiplicación.

$\mathbf{A}_3$: **La multiplicación es distributiva respecto a la adición:**

Sean $\frac{a}{s}$, $\frac{b}{t}$ y $\frac{m}{n} \in \mathbf{S}^{-1}\mathbf{A}$. Se demuestra que $\frac{a}{s}\left(\frac{b}{t}+\frac{m}{n}\right) = \frac{a}{s}\frac{b}{t}+\frac{a}{s}\frac{m}{n}$.

$$\frac{a}{s}\left(\frac{b}{t}+\frac{m}{n}\right) = \frac{a}{s}\left(\frac{bn+mt}{tn}\right)$$

$$= \frac{a}{s}\left(\frac{s}{s}\right)\left(\frac{bn+mt}{tn}\right)$$

$$=\frac{as(bn+mt)}{sstn}$$

$$=\frac{asbn+asmt}{sstn}$$

$$=\frac{(ab)sn+(am)st}{(st)(sn)}$$

$$=\frac{ab}{st}+\frac{am}{sn}$$

$$=\frac{a}{s}\frac{b}{t}+\frac{a}{s}\frac{m}{n}.$$

$\therefore$ La multiplicación en $\mathbf{S}^{-1}\mathbf{A}$ es distributiva respecto a la adición.

$\mathbf{A}_4$: La multiplicación es conmutativa:

Sean $\frac{a}{s},\ \frac{b}{t}\in\mathbf{S}^{-1}\mathbf{A}$.

$$\frac{a}{s},\ \frac{b}{t}\in\mathbf{S}^{-1}\mathbf{A}\quad\Rightarrow\quad\left(\frac{a}{s}\right)\left(\frac{b}{t}\right)=\frac{ab}{st}$$

$$=\frac{ba}{ts}$$

$$=\left(\frac{b}{t}\right)\left(\frac{a}{s}\right).$$

$\therefore$ $\mathbf{S}^{-1}\mathbf{A}$ es conmutativo respecto a la multiplicación.

$\mathbf{A}_5$: **Existencia de elemento unidad:**

Para cada $\frac{a}{s}$ en $\mathbf{S}^{-1}\mathbf{A}$, existe $\frac{1}{1}$ en $\mathbf{S}^{-1}\mathbf{A}$ tal que $\frac{a}{s}\frac{1}{1}=\frac{a}{s}$.

$\mathbf{S}$ es un sistema multiplicativo $\Rightarrow 1\in\mathbf{S}$

$$\Rightarrow \frac{1}{1}\in\mathbf{S}^{-1}\mathbf{A}$$

$$\Rightarrow \frac{a}{s}\frac{1}{1}=\frac{a\cdot 1}{s\cdot 1}=\frac{a}{s} \qquad \forall\ \frac{a}{s}\in\mathbf{S}^{-1}\mathbf{A}.$$

$$\therefore\ \frac{1}{1} \text{ es el elemento unidad en } \mathbf{S}^{-1}\mathbf{A}.$$

Se concluye que $\left(\mathbf{S}^{-1}\mathbf{A},+,\ \cdot\right)$ es un anillo conmutativo con elemento unidad.■

Proposición 1.5.4: Sea $\mathbf{A}$ un anillo y $\mathbf{S}$ un sistema multiplicativo de $\mathbf{A}$:

$$\mathbf{S}^{-1}\mathbf{A}=\{0\} \iff 0\in\mathbf{S}.$$

Demostración:

"$\Rightarrow$".

Sea $s\in\mathbf{S}$.

$$s\in\mathbf{S} \Rightarrow \frac{1}{s}\in\mathbf{S}^{-1}\mathbf{A}=\{0\}$$

$$\Rightarrow \quad \frac{1}{s} = \frac{0}{1}, \quad \left(\left(\frac{0}{1} \right) \text{ el cero en } \mathbf{S}^{-1}\mathbf{A} \right)$$

$$\Rightarrow \quad (1, s) \equiv (0, 1)$$

$$\Rightarrow \quad \exists \ u \in \mathbf{S} \ \text{ t. q. } \ u(1 \cdot 1 - 0 \cdot s) = 0$$

$$\Rightarrow \quad u = 0$$

$$\Rightarrow \quad 0 \in \mathbf{S}.$$

$\therefore$ Si $\mathbf{S}^{-1}\mathbf{A}$ es el anillo trivial, entonces $0 \in \mathbf{S}$.

"$\Leftarrow$"

Sea $\dfrac{a}{s} \in \mathbf{S}^{-1}\mathbf{A}$.

$$0 \in \mathbf{S} \ \Rightarrow \ 0(a \cdot 1 - 0 \cdot s) = 0, \ \forall \ a \in \mathbf{A} \ \text{ y } \ s \in \mathbf{S}$$

$$\Rightarrow (a, s) \equiv (0, 1)$$

$$\Rightarrow \frac{a}{s} = \frac{0}{1}$$

$$\Rightarrow \mathbf{S}^{-1}\mathbf{A} = \{0\}.$$

$\therefore$ Si $0 \in \mathbf{S}$, entonces $\mathbf{S}^{-1}\mathbf{A}$ es el anillo trivial.

Por tanto se supone que si no se especifica lo contrario, $\mathbf{S}$ no contiene al elemento cero.■

Observación: El sentido de incluir t en la relación de equivalencia en **(Θ)** es para asegurar que una fracción $\frac{a}{s}$ es la fracción cero si y solo si existe $t \in \mathbf{S}$ tal que $at = 0$ y es necesaria ya que el anillo $\mathbf{A}$ no tiene que ser necesariamente un dominio de integridad. Se observa que si no se incluye t en la definición de la relación de equivalencia y se supone que $as' = 0$ para algún $s' \in \mathbf{S}$ y $a \in \mathbf{A}$ tal que $a \neq 0$.

Entonces:

$$\frac{a}{1} = \left(\frac{a}{1}\right)\left(\frac{1}{1}\right) = \left(\frac{a}{1}\right)\left(\frac{s'}{s'}\right) = \frac{a \cdot s'}{1 \cdot s'} = \frac{0}{1}.$$

$$\frac{a}{1} = \frac{0}{1} \quad \Rightarrow \quad (a,\ 1) \equiv (0,\ 1)$$

$$\Rightarrow \ a \cdot 1 - 1 \cdot 0 = 0, \quad (\text{Sin la exigencia del } t)$$

$$\Rightarrow \ a = 0,\ (\rightarrow\leftarrow).$$

Proposición 1.5.5: La aplicación.

$$\psi : \mathbf{A} \rightarrow \mathbf{S}^{-1}\mathbf{A}$$

$$a \rightarrow \psi(a) = \frac{a}{1}.$$

Cumple las siguientes propiedades:

(i) ψ es un homomorfismo de anillos (**No es en general inyectivo**).

(ii) Si $s \in \mathbf{S}$, entonces $\psi(s)$ es unidad en $\mathbf{S}^{-1}\mathbf{A}$.

(iii) Si $\psi(a) = \frac{0}{1}$, entonces $as = 0$ para algún $s \in \mathbf{S}$.

(iv) Todo elemento de $\mathbf{S}^{-1}\mathbf{A}$ es de la forma $\psi(a)\left[\psi(s)\right]^{-1}$ para algunos $a \in \mathbf{A}$ y $s \in \mathbf{S}$.

Demostración (i):

Se verifica que $\psi : \mathbf{A} \to \mathbf{S}^{-1}\mathbf{A}$ definida por $a \to \psi(a) = \frac{a}{1}$ es un homomorfismo de anillos.

Sean $a, b \in \mathbf{A}$ tal que $a = b$.

$$a, b \in \mathbf{A} \quad \Rightarrow \quad \psi(a) = \frac{a}{1} \quad \text{y} \quad \psi(b) = \frac{b}{1}$$

$$\Rightarrow \quad \psi(a) - \psi(b) = \frac{a}{1} - \frac{b}{1} = \frac{a \cdot 1 - b \cdot 1}{1 \cdot 1} = \frac{0}{1}$$

$$\Rightarrow \quad \psi(a) = \psi(b). \qquad \therefore \ \psi \text{ esta bien definida.}$$

Para $a, b \in \mathbf{A}$.

- $\psi(a+b) = \dfrac{(a+b)}{1} = \left(\dfrac{a}{1}\right) + \left(\dfrac{b}{1}\right) = \psi(a) + \psi(b).$

- $\psi(ab) = \dfrac{(ab)}{1} = \left(\dfrac{a}{1}\right)\left(\dfrac{b}{1}\right) = \psi(a)\psi(b).$

- $\psi(1_{\mathbf{A}}) = \dfrac{1}{1} = 1_{\mathbf{S}^{-1}\mathbf{A}}.$

$\therefore$ ψ es un homomorfismo de anillos.

Demostración (ii):

Sea $s \in \mathbf{S}$.

$$s \in \mathbf{S} \;\Rightarrow\; \psi(s) = \frac{s}{1} \text{ y } \frac{1}{s} \in \mathbf{S}^{-1}\mathbf{A}$$

$$\Rightarrow\; \psi(s)\left(\frac{1}{s}\right) = \left(\frac{s}{1}\right)\left(\frac{1}{s}\right) = \frac{s\cdot 1}{1\cdot s} = \frac{1}{1}, \qquad \left(\left(\frac{1}{1}\right) \text{ la unidad en } \mathbf{S}^{-1}\mathbf{A}\right)$$

$$\Rightarrow\; \psi(s) \text{ es unidad en } \mathbf{S}^{-1}\mathbf{A} \quad \forall\; s \in \mathbf{S}.$$

$\therefore$ Si $s \in \mathbf{S}$, entonces $\psi(s)$ es unidad en $\mathbf{S}^{-1}\mathbf{A}$.

Demostración (iii):

Sea $a \in \mathbf{A}$ t. q. $\psi(a) = \dfrac{0}{1}$.

$$\psi(a) = \frac{0}{1} \;\Rightarrow\; \frac{a}{1} = \frac{0}{1}$$

$$\Rightarrow\; (a\,,1) \equiv (0\,,1)$$

$$\Rightarrow\; \exists\;\; s \in \mathbf{S} \;\text{ t. q. }\; s(a \cdot 1 - 0 \cdot 1) = 0$$

$$\Rightarrow\; as = 0 \;\text{ para algún } s \in \mathbf{S}.$$

$\therefore$ Si $\psi(a) = \dfrac{0}{1}$, entonces $as = 0$ para algún $s \in \mathbf{S}$.

Demostración (iv):

Sea $\dfrac{a}{s} \in \mathbf{S}^{-1}\mathbf{A}$.

Dado $s \in \mathbf{S}$, $\psi(s)$ es unidad en $\mathbf{S}^{-1}\mathbf{A}$ con inverso multiplicativo $\left(\dfrac{1}{s}\right)$ (por lo hecho en (ii)), entonces;

$$\left(\frac{a}{s}\right) = \left(\frac{a}{1}\right)\left(\frac{1}{s}\right) = \left(\frac{a}{1}\right)\left(\frac{s}{1}\right)^{-1} = \psi(a)\left[\psi(s)\right]^{-1}.$$

$\therefore$ Todo elemento de $\mathbf{S}^{-1}\mathbf{A}$ es de la forma $\psi(a)\left[\psi(s)\right]^{-1}$ para algunos $a \in \mathbf{A}$ y $s \in \mathbf{S}$.

Proposición 1.5.6: Sea $\mathbf{A}$ un anillo y $\mathbf{S}$ un sistema multiplicativo de $\mathbf{A}$; se verifica.

$$\mathbf{ker}(\psi) = \{a \in \mathbf{A} \mid \exists\ s \in \mathbf{S} \quad \text{t. q.} \quad as = 0\}.$$

En particular los siguientes enunciados son equivalentes:

(i) $\psi : \mathbf{A} \to \mathbf{S}^{-1}\mathbf{A}$ es inyectivo.

(ii) $\mathbf{S}$ no contiene divisores de cero.

Demostración:

$$\mathbf{ker}(\psi) = \left\{ x \in \mathbf{A} \mid \psi(x) = \frac{0}{1} \right\}$$

$$= \left\{ x \in \mathbf{A} \mid \frac{x}{1} = \frac{0}{1} \right\}$$

$$= \left\{ x \in \mathbf{A} \mid (x, 1) \equiv (0, 1) \right\}$$

$$= \left\{ x \in \mathbf{A} \mid \exists\ s \in \mathbf{S} \quad \text{t. q.} \ s(x \cdot 1 - 0 \cdot 1) = 0 \right\}$$

$$= \left\{ x \in \mathbf{A} \mid \exists\ s \in \mathbf{S} \quad \text{t. q.} \ sx = 0 \right\}.$$

$$\therefore\ \mathbf{ker}(\psi) = \left\{ x \in \mathbf{A} \mid \exists\ s \in \mathbf{S} \quad \text{t. q.} \ sx = 0 \right\}.$$

Para la equivalencia se tiene,

$(i) \Rightarrow (\mathrm{ii})$.

Se supone que ψ es inyectiva y sea s en $\mathbf{S}$ un divisor de cero en $\mathbf{A}$.

$s \in \mathbf{S}$ divide a cero $\Rightarrow \exists\, x \in \mathbf{A},\ x \neq 0$ t. q. $sx = 0$

$$\Rightarrow s(x \cdot 1 - 1 \cdot 0) = 0$$

$$\Rightarrow (x, 1) \equiv (0, 1)$$

$$\Rightarrow \frac{x}{1} = \frac{0}{1}$$

$$\Rightarrow \psi(x) = \frac{0}{1}$$

$$\Rightarrow x = 0, \quad (\rightarrow\leftarrow)(\psi \text{ es inyectivo}).$$

$\therefore$ $\mathbf{S}$ no tiene divisores de cero.

$(ii) \Rightarrow (\mathrm{i})$.

Suponga que $\psi : \mathbf{A} \rightarrow \mathbf{S}^{-1}\mathbf{A}$ no es inyectiva y sea $x \in \mathbf{A},\ x \neq 0$ tal que $\psi(x) = \dfrac{0}{1}$.

$$\psi(x) = \frac{0}{1} \quad \Rightarrow \quad \frac{x}{1} = \frac{0}{1}$$

$\Rightarrow \ (x, 1) \equiv (0, 1)$

$\Rightarrow \ \exists \ s \in \mathbf{S}$ t. q. $s(x \cdot 1 - 0 \cdot 1) = 0$

$\Rightarrow \ \exists \ s \in \mathbf{S}$ t. q. $sx = 0$

$\Rightarrow \ s$ divide a cero.

$\therefore \ \psi$ es inyectiva. ■

Se dice que $\mathbf{A}$ tiene un anillo de fracciones respecto de $\mathbf{S}$, si existe un anillo $\mathbf{B}$ y una función $f: \mathbf{A} \to \mathbf{B}$ tal que se cumplen las condiciones de la proposición 1.5.5. En tal caso se dice que $\mathbf{B}$ es un anillo de fracciones de $\mathbf{A}$ con respecto a $\mathbf{S}$.

En virtud de la proposición 1.5.6, no se puede considerar en general que $\mathbf{A}$ se inyecte en el anillo de fracciones $\mathbf{S}^{-1}\mathbf{A}$ (es decir, $\mathbf{A} \subseteq \mathbf{S}^{-1}\mathbf{A}$). Una interrogante que puede surgir es sobre la unicidad del anillo construido. Las siguientes proposiciones muestran la existencia y unicidad de tal anillo.

Proposición 1.5.7: (**Propiedad universal del anillo de fracciones**) Sea $f: \mathbf{A} \to \mathbf{B}$ un homomorfismo de anillos tal que $f(s)$ es unidad en $\mathbf{B}$ para todo $s \in \mathbf{S}$. Entonces existe un único homomorfismo $g: \mathbf{S}^{-1}\mathbf{A} \to \mathbf{B}$ tal que $g \circ \psi = f$. Además, si f es inyectivo, entonces g también es inyectivo.

Demostración:

Se considera el siguiente diagrama,

$$\begin{tikzcd}
\mathbf{A} \arrow[rr, "\psi"] \arrow[dr, "f"'] & & \mathbf{S}^{-1}\mathbf{A} \arrow[dl, "g"] \\
& \mathbf{B} &
\end{tikzcd} \qquad g \circ \psi = f$$

Existencia:

Se define g de la siguiente manera:

$$g: \mathbf{S}^{-1}\mathbf{A} \longrightarrow \mathbf{B}$$

$$\frac{a}{s} \quad \rightarrow \quad g\left(\frac{a}{s}\right) = f(a)\left[f(s)\right]^{-1}.$$

Se demuestra que g satisface lo siguiente:

(1) g está bien definida.

(2) g es un homomorfismo.

(3) $g \circ \psi = f$.

(4) $(f$ es inyectiva$) \Rightarrow (g$ es inyectiva$)$.

Demostración (1)**:**

Sean $\frac{a_1}{s_1}$, $\frac{a_2}{s_2} \in \mathbf{S}^{-1}\mathbf{A}$ tal que $\frac{a_1}{s_1} = \frac{a_2}{s_2}$.

$$\frac{a_1}{s_1} = \frac{a_2}{s_2} \quad \Rightarrow \quad (a_1,\, s_1) \equiv (a_2,\, s_2)$$

$$\Rightarrow \quad \exists \ t \in \mathbf{S} \quad \text{t. q.} \quad t(a_1 s_2 - a_2 s_1) = 0.$$

Aplicando f y las propiedades de homomorfismo a $t(a_1 s_2 - a_2 s_1) = 0$ se obtiene,

$$\begin{aligned} f\left(t(a_1 s_2 - a_2 s_1)\right) = f(0) = 0 \ &\Rightarrow \ f\left(t(a_1 s_2 - a_2 s_1)\right) = 0 \\ &\Rightarrow \ f(t) f(a_1 s_2 - a_2 s_1) = 0 \\ &\Rightarrow \ f(t)\left[f(a_1) f(s_2) - f(a_2) f(s_1)\right] = 0. \end{aligned}$$

Como $f(t)$ es unidad en $\mathbf{B}$,

$$f(a_1) f(s_2) - f(a_2) f(s_1) = 0.$$

De donde,

$$f(a_1) f(s_2) = f(a_2) f(s_1).$$

Y como $f(s_1)$ y $f(s_2)$ son unidades en $\mathbf{B}$,

$$f(a_1)\left[f(s_1)\right]^{-1} = f(a_2)\left[f(s_2)\right]^{-1}.$$

De lo anterior, se deduce:

$$g\left(\frac{a_1}{s_1}\right) = g\left(\frac{a_2}{s_2}\right).$$

$$\therefore \quad g \ \text{ está bien definida.}$$

Demostración (2)**:**

Sean $\dfrac{a_1}{s_1},\ \dfrac{a_2}{s_2} \in \mathbf{S}^{-1}\,\mathbf{A}$, se demuestra que $g\left(\left(\dfrac{a_1}{s_1}\right)+\left(\dfrac{a_2}{s_2}\right)\right)=g\left(\dfrac{a_1}{s_1}\right)+g\left(\dfrac{a_2}{s_2}\right)$.

$$g\left(\left(\frac{a_1}{s_1}\right)+\left(\frac{a_2}{s_2}\right)\right)=g\left(\frac{a_1s_2+a_2s_1}{s_1s_2}\right)$$

$$=f\left(a_1s_2+a_2s_1\right)\left[f\left(s_1s_2\right)\right]^{-1}$$

$$=\left[f\left(a_1s_2\right)+f\left(a_2s_1\right)\right]\left[f\left(s_1\right)f\left(s_2\right)\right]^{-1}$$

$$=\left[f\left(a_1\right)f\left(s_2\right)+f\left(a_2\right)f\left(s_1\right)\right]\left[f\left(s_1\right)\right]^{-1}\left[f\left(s_2\right)\right]^{-1}$$

$$=f\left(a_1\right)f\left(s_2\right)\left[f\left(s_1\right)\right]^{-1}\left[f\left(s_2\right)\right]^{-1}+f\left(a_2\right)f\left(s_1\right)\left[f\left(s_1\right)\right]^{-1}\left[f\left(s_2\right)\right]^{-1}$$

$$=f\left(a_1\right)\left[f\left(s_1\right)\right]^{-1}\left\{f\left(s_2\right)\left[f\left(s_2\right)\right]^{-1}\right\}+f\left(a_2\right)\left\{f\left(s_1\right)\left[f\left(s_1\right)\right]^{-1}\right\}\left[f\left(s_2\right)\right]^{-1}$$

$$=f\left(a_1\right)\left[f\left(s_1\right)\right]^{-1}+f\left(a_2\right)\left[f\left(s_2\right)\right]^{-1}$$

$$=g\left(\frac{a_1}{s_1}\right)+g\left(\frac{a_2}{s_2}\right).$$

$$\therefore\ \ g\left(\left(\frac{a_1}{s_1}\right)+\left(\frac{a_2}{s_2}\right)\right)=g\left(\frac{a_1}{s_1}\right)+g\left(\frac{a_2}{s_2}\right).$$

Sean $\left(\frac{a_1}{s_1}\right)$, $\left(\frac{a_2}{s_2}\right) \in \mathbf{S}^{-1}\,\mathbf{A}$, se demuestra que $g\left(\left(\frac{a_1}{s_1}\right)\left(\frac{a_2}{s_2}\right)\right) = g\left(\frac{a_1}{s_1}\right) g\left(\frac{a_2}{s_2}\right)$.

$$g\left[\left(\frac{a_1}{s_1}\right)\cdot\left(\frac{a_2}{s_2}\right)\right] = g\left(\frac{a_1 a_2}{s_1 s_2}\right)$$

$$= f\left(a_1 a_2\right)\left[f\left(s_1 s_2\right)\right]^{-1}$$

$$= f\left(a_1\right) f\left(a_2\right)\left[f\left(s_1\right) f\left(s_2\right)\right]^{-1}$$

$$= f\left(a_1\right) f\left(a_2\right)\left[f\left(s_1\right)\right]^{-1}\left[f\left(s_2\right)\right]^{-1}$$

$$= \left\{f\left(a_1\right)\left[f\left(s_1\right)\right]^{-1}\right\}\left\{f\left(a_2\right)\left[f\left(s_2\right)\right]^{-1}\right\}$$

$$= g\left(\frac{a_1}{s_1}\right) g\left(\frac{a_2}{s_2}\right).$$

$$\therefore \quad g\left(\left(\frac{a_1}{s_1}\right)\left(\frac{a_2}{s_2}\right)\right) = g\left(\frac{a_1}{s_1}\right) g\left(\frac{a_2}{s_2}\right).$$

Sea $1_{\mathbf{S}^{-1}\mathbf{A}} \in \mathbf{S}^{-1}\mathbf{A}$, se demuestra que $g\left(1_{\mathbf{S}^{-1}\mathbf{A}}\right) = 1_{\mathbf{B}}$.

$$g\left(1_{\mathbf{S}^{-1}\mathbf{A}}\right) = g\left(\frac{1}{1}\right) = f(1)\left[f(1)\right]^{-1}$$

$$= f(1)\, f\left(1^{-1}\right)$$

$$= f\left(1 \cdot 1^{-1}\right)$$

$$= f(1)$$

$$= 1_{\mathbf{B}}.$$

$\therefore\ g$ es un homomorfismo de anillos.

Demostración (3)**:**

Se prueba que el diagrama es conmutativo.

Sea $a \in \mathbf{A}$.

$$a \in \mathbf{A} \;\Rightarrow\; (g \circ \psi)(a) = g(\psi(a))$$

$$= g\left(\frac{a}{1}\right)$$

$$= f(a)\left[f(1)\right]^{-1}$$

$$= f(a).$$

$$\therefore \quad g \circ \psi = f.$$

Demostración (4)**:**

Se demuestra que $\left(f \text{ es inyectiva}\right) \Rightarrow \left(g \text{ es inyectiva}\right)$.

Sea $\dfrac{a}{s} \in \mathbf{ker}(g)$.

$$\frac{a}{s} \in \mathbf{ker}(g) \Rightarrow g\left(\frac{a}{s}\right) = 0$$

$$\Rightarrow f(a)\left[f(s)\right]^{-1} = 0$$

$$\Rightarrow f(a) = 0, \qquad \left(f(s) \text{ es unidad en } \mathbf{B}\right)$$

$$\Rightarrow a = 0, \qquad \left(f \text{ es inyectiva } \right)$$

$$\Rightarrow \frac{a}{s} = \frac{0}{1}, \qquad \left(\left(\frac{0}{1}\right) \text{ el cero en } \mathbf{S}^{-1}\mathbf{A} \right)$$

$$\Rightarrow \mathbf{ker}(g) = \{\mathbf{0}\}.$$

$\therefore$ Si f es inyectiva, entonces g es inyectiva. ■

Unicidad:

Suponga que $g': \mathbf{S}^{-1}\mathbf{A} \rightarrow \mathbf{B}$ es un homomorfismo de anillos tal que $g' \circ \psi = f$.

$$g' \circ \psi = f \Rightarrow g' \circ \psi = g \circ \psi.$$

Sean $\dfrac{a}{s} \in \mathbf{S}^{-1}\,\mathbf{A}$.

$$\frac{a}{s} \in \mathbf{S}^{-1}\,\mathbf{A} \Rightarrow g\left(\frac{a}{s}\right) = f(a)\left[f(s)\right]^{-1}$$

$$= \left\{(g' \circ \psi)(a)\right\} \left\{\left[(g' \circ \psi)(s)\right]^{-1}\right\}$$

$$= g'(\psi(a))\left[g'(\psi(s))\right]^{-1}$$

$$= g'\left(\frac{a}{1}\right)\left[g'\left(\frac{s}{1}\right)\right]^{-1}$$

$$= g'\left(\frac{a}{1}\right)g'\left(\left(\frac{s}{1}\right)^{-1}\right)$$

$$= g'\left(\frac{a}{1}\right)g'\left(\frac{1}{s}\right)$$

$$= g'\left(\left(\frac{a}{1}\right)\left(\frac{1}{s}\right)\right)$$

$$= g'\left(\frac{a}{s}\right).$$

$$\therefore\ g = g'.$$

$\therefore$ Existe un único homomorfismo $g : \mathbf{S}^{-1}\,\mathbf{A} \to \mathbf{B}$ tal que $g \circ \psi = f$.

Si el anillo $\mathbf{A}$ se puede inyectar en el anillo de fracciones $\mathbf{S}^{-1}\mathbf{A}$, entonces $\mathbf{S}^{-1}\mathbf{A}$ es el menor anillo que contiene a $\mathbf{A}$ en el cual todos los elementos de $\mathbf{S}$ son unidades.

Corolario 1.5.8: Si $f:\mathbf{A}\to\mathbf{B}$ es un homomorfismo de anillos tal que:

(i) Si $s\in\mathbf{S}$, entonces $f(s)$ es unidad en $\mathbf{B}$.

(ii) Si $f(a)=0$, entonces $as=0$ para algún $s\in\mathbf{S}$.

(iii) Todo elemento de $\mathbf{B}$ es de la forma $f(a)\left[f(s)\right]^{-1}$ para algunos $a\in\mathbf{A}$ y $s\in\mathbf{S}$.

Entonces existe un único isomorfismo de anillos $g:\mathbf{S}^{-1}\mathbf{A}\to\mathbf{B}$ tal que $f=g\circ\psi$.

Demostración:

Se demuestra que existe un único isomorfismo de anillos $g:\mathbf{S}^{-1}\mathbf{A}\to\mathbf{B}$ t. q. $f=g\circ\psi$.

Por la proposición 1.5.7, existe un único homomorfismo de anillos bien definido $g:\mathbf{S}^{-1}\mathbf{A}\to\mathbf{B}$ tal que $f=g\circ\psi$.

Es decir; que hace conmutativo, el siguiente diagrama:

$$\begin{tikzcd}
\mathbf{A} \arrow[rr, "\psi"] \arrow[dr, "f"'] & & \mathbf{S}^{-1}\mathbf{A} \arrow[dl, "g"] \\
& \mathbf{B} &
\end{tikzcd}
\qquad g\circ\psi=f.$$

Ahora se verifica que $g : \mathbf{S}^{-1}\mathbf{A} \to \mathbf{B}$ definida por;

$$g\left(\frac{a}{s}\right) = f(a)\left[f(s)\right]^{-1}.$$

Satisface las condiciones siguientes:

(1) g es monomorfismo.

(2) g es epimorfismo.

Demostración (1)**:**

Sea $\frac{a}{s} \in \mathbf{ker}(g)$.

$$\begin{aligned}
\frac{a}{s} \in \mathbf{ker}(g) \quad &\Rightarrow \quad g\left(\frac{a}{s}\right) = 0 \\
&\Rightarrow \quad f(a)\left[f(s)\right]^{-1} = 0 \\
&\Rightarrow \quad f(a) = 0, \qquad \left(\text{Por el inciso (i)}\right) \\
&\Rightarrow \quad \exists\ t \in \mathbf{S} \ \text{ t. q. } \ at = 0, \qquad \left(\text{Por el inciso (ii)}\right) \\
&\Rightarrow \quad t(a \cdot 1 - 0 \cdot s) = 0 \\
&\Rightarrow \quad (a, s) \equiv (0, 1) \\
&\Rightarrow \quad \frac{a}{s} = \frac{0}{1} \\
&\Rightarrow \quad \mathbf{ker}(g) = \{0\}.
\end{aligned}$$

Luego si $\mathbf{ker}(g) = \{0\}$, entonces g es un homomorfismo inyectivo (**Monomorfismo**).

Demostración (2)**:**

Sea $b \in \mathbf{B}$.

Por el inciso (iii). Si $b \in \mathbf{B}$, entonces existen $a \in \mathbf{A}$, $s \in \mathbf{S}$ tal que $b = f(a)\left[f(s)\right]^{-1}$.

$$
\begin{aligned}
b = f(a)\left[f(s)\right]^{-1} &= \{(g \circ \psi)(a)\}\left\{\left[(g \circ \psi)(s)\right]^{-1}\right\} \\
&= g(\psi(a))\left[g(\psi(s))\right]^{-1} \\
&= g\left(\frac{a}{1}\right)\left[g\left(\frac{s}{1}\right)\right]^{-1} \\
&= g\left(\frac{a}{1}\right)g\left(\frac{1}{s}\right) \\
&= g\left(\frac{a}{s}\right).
\end{aligned}
$$

Luego $b \in \mathbf{Im}(g)$, así g es un homomorfismo sobreyectivo (**Epimorfismo**).

$$\therefore \ \mathbf{S}^{-1}\mathbf{A} \approx \mathbf{B}.$$

Observación: La proposición anterior muestra la unicidad del anillo de fracciones $\mathbf{S}^{-1}\mathbf{A}$.

La siguiente proposición muestra otra forma de caracterizar el anillo de fracciones mediante la propiedad universal de la proposición 1.5.7.

Proposición 1.5.9: Sea $g:\mathbf{A}\to\mathbf{B}$ un homomorfismo de anillos tal que $g(s)$ es unidad en $\mathbf{B}$ para todo $s\in\mathbf{S}$, se supone que $\mathbf{B}$ también cumple la propiedad universal de la proposición 1.5.7, entonces $\mathbf{B}\approx\mathbf{S}^{-1}\mathbf{A}$.

Demostración:

Como $\mathbf{S}^{-1}\mathbf{A}$ satisface la propiedad universal de la proposición 1.5.7, entonces existe un único homomorfismo $h:\mathbf{S}^{-1}\mathbf{A}\to\mathbf{B}$ que hace conmutativo el siguiente diagrama:

$$\begin{tikzcd}
\mathbf{A} \arrow[rr, "\psi"] \arrow[dr, "g"'] & & \mathbf{S}^{-1}\mathbf{A} \arrow[dl, "h"] \\
& \mathbf{B} &
\end{tikzcd} \qquad h\circ\psi=g.$$

Por hipótesis $\mathbf{B}$ también tiene la propiedad universal, entonces existe un único homomorfismo $t:\mathbf{B}\to\mathbf{S}^{-1}\mathbf{A}$ que hace conmutativo el siguiente diagrama:

$$\begin{tikzcd}
\mathbf{A} \arrow[rr, "g"] \arrow[dr, "\psi"'] & & \mathbf{B} \arrow[dl, "t"] \\
& \mathbf{S}^{-1}\mathbf{A} &
\end{tikzcd} \qquad t\circ g=\psi.$$

Se demuestra que $t\circ h$ es la identidad en $\mathbf{S}^{-1}\mathbf{A}$ y $h\circ t$ es la identidad en $\mathbf{B}$. Sustituyendo g y ψ se tiene las siguientes composiciones:

$$g=h\circ\psi=h\circ(t\circ g)=(h\circ t)\circ g.$$

$$\psi=t\circ g=t\circ(h\circ\psi)=(t\circ h)\circ\psi.$$

Entonces por la unicidad en la propiedad universal resulta:

$$(h \circ t) = \mathrm{I}_{\mathbf{B}} \text{ y } (t \circ h) = \mathrm{I}_{\mathbf{S}^{-1}\mathbf{A}}.$$

Luego existe un homomorfismo $t : \mathbf{B} \to \mathbf{S}^{-1}\mathbf{A}$ tal que $(h \circ t) = \mathrm{I}_{\mathbf{B}}$ y $(t \circ h) = \mathrm{I}_{\mathbf{S}^{-1}\mathbf{A}}$, entonces $h : \mathbf{S}^{-1}\mathbf{A} \to \mathbf{B}$ es un isomorfismo de anillos.■

Un importante ejemplo de anillo de fracciones viene dado por el siguiente resultado.

Proposición 1.5.10: Si $\mathbf{A}$ es un dominio, entonces $\mathbf{S} = \mathbf{A} - \{0\}$ un sistema multiplicativo de $\mathbf{A}$, el anillo de fracciones $\mathbf{S}^{-1}\mathbf{A}$ es un cuerpo, llamado **cuerpo de fracciones** de $\mathbf{A}$, el homomorfismo $\psi : \mathbf{A} \to \mathbf{S}^{-1}\mathbf{A}$ definido por $a \to \psi(a) = \frac{a}{1}$ es inyectivo.

Demostración:

Si $\mathbf{A}$ es un dominio de integridad, $\mathbf{S} = \mathbf{A} - \{0\}$ es un sistema multiplicativo porque en $\mathbf{A}$ el producto de elementos no nulos nunca es nulo y $1 \neq 0$.

Ahora se demuestra que $\mathbf{S}^{-1}\mathbf{A}$ es un cuerpo para ello se verifican las condiciones de la definición 1.1.7:

(1) $\frac{1}{1} \neq \frac{0}{1}$.

(2) Cada elemento no nulo es unidad.

Demostración (1)**:** Se supone que $\frac{1}{1}=\frac{0}{1}$.

$$\frac{1}{1}=\frac{0}{1} \;\Rightarrow\; (1,\,1)\equiv(0,\,1)$$

$$\Rightarrow\; \exists\;\; t\in\mathbf{S}\;\;\text{ t. q. }\; t\left(\,1\cdot 1-0\cdot 1\right)=0$$

$$\Rightarrow\; t=0$$

$$\Rightarrow\; 0\in\mathbf{S},\quad (\rightarrow\leftarrow). \qquad\qquad \therefore\;\; \frac{1}{1}\neq\frac{0}{1}.$$

Demostración (2):

Sea $\frac{a}{s}\in\mathbf{S}^{-1}\mathbf{A}$ t. q. $\frac{a}{s}\neq\frac{0}{1}$.

$$\frac{a}{s}\neq\frac{0}{1} \;\Rightarrow\; a\neq 0 \;\;\wedge\;\; s\neq 0,\quad \left(\text{pues } s\in\mathbf{S}\right)$$

$$\Rightarrow\; a\in\mathbf{S}$$

$$\Rightarrow\; \frac{s}{a}\in\mathbf{S}^{-1}\mathbf{A}$$

$$\Rightarrow\; \left(\frac{s}{a}\right)\left(\frac{a}{s}\right)=\frac{1}{1},\qquad \left(\left(\frac{1}{1}\right)\text{ la unidad en } \mathbf{S}^{-1}\mathbf{A}\right)$$

$$\Rightarrow\; \frac{a}{s}\;\text{ es unidad en }\; \mathbf{S}^{-1}\mathbf{A}.$$

Luego cada elemento no nulo en $\mathbf{S}^{-1}\mathbf{A}$ es una unidad.

$$\therefore\ \mathbf{S}^{-1}\mathbf{A} \text{ es un cuerpo.}$$

Si $\mathbf{A}$ es un dominio de integridad, $\mathbf{S}=\mathbf{A}-\{0\}$ no contiene divisores de cero, entonces por la proposición 1.5.6 el homomorfismo $\psi : \mathbf{A} \rightarrow \mathbf{S}^{-1}\mathbf{A}$ es inyectivo. ■

Se denota por $\mathbf{k}_{\mathbf{A}}$ al cuerpo de fracciones de un dominio de integridad.

1.6: Localización por ideales primos.

A continuación se estudia el proceso de localización por ideales primos.

Proposición 1.6.1: Sea $\mathbf{A}$ un anillo y $\mathfrak{p}$ un ideal de $\mathbf{A}$. $\mathbf{S}=\mathbf{A}-\mathfrak{p}$ es un sistema multiplicativo de $\mathbf{A}$ sí y sólo si $\mathfrak{p}$ es un ideal primo.

Demostración:

$$\left(\mathbf{S}=\mathbf{A}-\mathfrak{p} \text{ es un sistema multiplicativo de } \mathbf{A}\right) \Leftrightarrow \left(\mathfrak{p} \text{ es un ideal primo}\right)$$

"$\Rightarrow$" Se supone que $\mathbf{S}$ es un sistema multiplicativo. Se prueba que $\mathfrak{p}$ es un ideal primo en $\mathbf{A}$, es decir:

(1) $\mathfrak{p} \neq (1)$.

(2) $xy \in \mathfrak{p} \Rightarrow x \in \mathfrak{p} \vee y \in \mathfrak{p}$.

Demostración (1):

$\mathbf{S}$ es un sistema multiplicativo de $\mathbf{A}$ $\Rightarrow$ $1 \in \mathbf{S} = \mathbf{A} - \mathfrak{p}$

$$\Rightarrow 1 \notin \mathfrak{p}$$

$$\Rightarrow \mathfrak{p} \neq (1).$$

$$\therefore \mathfrak{p} \neq (1).$$

Demostración (2):

$xy \in \mathfrak{p} \Rightarrow x \in \mathfrak{p} \quad \vee \quad y \in \mathfrak{p}$. Que equivale a demostrar que si $x,\ y \notin \mathfrak{p}$, entonces $xy \notin \mathfrak{p}$.

Sean $x, y \in \mathbf{A}$ t. q. $x, y \notin \mathfrak{p}$.

$$x, y \notin \mathfrak{p} \Rightarrow x, y \in \mathbf{A} - \mathfrak{p} = \mathbf{S}$$

$$\Rightarrow xy \in \mathbf{S}, \quad (\mathbf{S} \text{ es un sistema multiplicativo de } \mathbf{A})$$

$$\Rightarrow xy \notin \mathfrak{p}.$$

Luego si $x,\ y \notin \mathfrak{p}$, entonces $xy \notin \mathfrak{p}$, lo que demuestra que $\mathfrak{p}$ es un ideal primo de $\mathbf{A}$.

$$\therefore \mathfrak{p} \text{ es un ideal primo de } \mathbf{A}.$$

"$\Leftarrow$".

Suponga que $\mathfrak{p}$ es un ideal primo en $\mathbf{A}$. Se prueba que $\mathbf{S}$ es un sistema multiplicativo de $\mathbf{A}$ para ello se verifica lo siguiente:

(1) $1 \in \mathbf{S}$.

(2) $x, y \in \mathbf{S} \;\Rightarrow\; xy \in \mathbf{S}$.

Demostración (1):

$\mathfrak{p}$ es un ideal primo en $\mathbf{A} \;\Rightarrow\; 1 \notin \mathfrak{p}$

$$\Rightarrow\; 1 \in \mathbf{S} = \mathbf{A} - \mathfrak{p}.$$

$$\therefore 1 \in \mathbf{S}.$$

Demostración (2):

Sean $x, y \in \mathbf{S}$.

$$x, y \in \mathbf{S} \;\Rightarrow\; x,\; y \notin \mathfrak{p}$$

$$\Rightarrow\; xy \notin \mathfrak{p}$$

$$\Rightarrow\; xy \in \mathbf{S}.$$

$$\therefore\; x, y \in \mathbf{S} \Rightarrow\; xy \in \mathbf{S}.$$

Luego $\mathbf{S}$ es un sistema multiplicativo de $\mathbf{A}$.■

Si $\mathbf{A}$ es un anillo y $\mathfrak{p}$ un ideal primo de $\mathbf{A}$, entonces $\mathbf{A}-\mathfrak{p}$ es un sistema multiplicativo de $\mathbf{A}$ en virtud de la proposición 1.6.1. En este caso el anillo de fracciones $\mathbf{S}^{-1}\mathbf{A}$ se denota por $\mathbf{A}_{\mathfrak{p}}$.

Proposición 1.6.2: El conjunto $\mathfrak{m}=\left\{\frac{a}{s}\in\mathbf{A}_{\mathfrak{p}} \mid a\in\mathfrak{p} \text{ y } s\in\mathbf{A}-\mathfrak{p}\right\}$ forma un ideal maximal en $\mathbf{A}_{\mathfrak{p}}$**.** Además $\mathfrak{m}$ es el único ideal maximal en $\mathbf{A}_{\mathfrak{p}}$**.**

Demostración:

Se verifica que $\mathfrak{m}$ satisface las condiciones de la definición 1.1.9 de ideal:

(1) Si $\frac{a}{s}, \frac{b}{t}\in\mathfrak{m}$, se demuestra que $\frac{a}{s}+\frac{b}{t}\in\mathfrak{m}$.

Sean $\frac{a}{s}, \frac{b}{t}\in\mathfrak{m}$.

$$\begin{aligned}
\frac{a}{s}, \frac{b}{t}\in\mathfrak{m} &\Rightarrow a, b\in\mathfrak{p} \quad\wedge\quad s, t\in\mathbf{S}\\
&\Rightarrow at\in\mathfrak{p} \quad\wedge\quad bs\in\mathfrak{p}\\
&\Rightarrow at+bs\in\mathfrak{p} \quad\wedge\quad st\in\mathbf{S}\\
&\Rightarrow \frac{at+bs}{st}\in\mathfrak{m}
\end{aligned}$$

$$\Rightarrow \quad \frac{at+bs}{st} = \frac{a}{s} + \frac{b}{t} \in \mathfrak{m}$$

$$\Rightarrow \quad \frac{a}{s} + \frac{b}{t} \in \mathfrak{m}.$$

$$\therefore \quad \frac{a}{s} + \frac{b}{t} \in \mathfrak{m}.$$

(2) Se demuestra que $\mathbf{A}_{\mathfrak{p}}\,\mathfrak{m} \subseteq \mathfrak{m}$.

Sea $x \in \mathbf{A}_{\mathfrak{p}}\,\mathfrak{m}$.

$x \in \mathbf{A}_{\mathfrak{p}}\,\mathfrak{m} \;\Rightarrow\; x = yz,$ donde $y \in \mathbf{A}_{\mathfrak{p}}$ y $z \in \mathfrak{m}$

$$\Rightarrow \; y = \frac{a}{s} \quad \text{y} \quad z = \frac{b}{t}, \quad \text{con } a \in \mathbf{A}, b \in \mathfrak{p} \; \text{ y } \; s, t \in \mathbf{S}$$

$$\Rightarrow \; yz = \left(\frac{a}{s}\right)\left(\frac{b}{t}\right) = \left(\frac{ab}{st}\right) \in \mathfrak{m},$$ ($\mathfrak{p}$ es ideal en $\mathbf{A}$ y $\mathbf{S}$ un sist. multip. de $\mathbf{A}$)

$$\Rightarrow \; x \in \mathfrak{m}.$$

Luego efectivamente $\mathbf{A}_{\mathfrak{p}}\,\mathfrak{m} \subseteq \mathfrak{m}$.

$$\therefore \; \mathfrak{m} \text{ es ideal de } \mathbf{A}_{\mathfrak{p}}.$$

Ahora se demuestra que $\mathfrak{m}$ es maximal.

Se verifica lo siguiente:

(1) $\mathfrak{m} \neq (1_{\mathbf{S}^{-1}\mathbf{A}})$.

(2) Si $x \in \mathbf{A}_{\mathfrak{p}} - \mathfrak{m}$, entonces x es una unidad en $\mathbf{A}_{\mathfrak{p}}$.

(1) Suponga que $\mathfrak{m} = (1_{\mathbf{S}^{-1}\mathbf{A}})$.

$$\mathfrak{m} = (1_{\mathbf{S}^{-1}\mathbf{A}}) \Rightarrow \exists\ a \in \mathfrak{p} \text{ y } s \in \mathbf{S}, \text{ t. q. } \frac{a}{s} = \frac{1}{1}$$

$$\Rightarrow (a, s) \equiv (1, 1)$$

$$\Rightarrow \exists\ t \in \mathbf{S} \text{ t. q. } t(a \cdot 1 - 1 \cdot s) = 0$$

$$\Rightarrow ta = ts$$

$$\Rightarrow ts \in \mathfrak{p} \text{ y } ts \in \mathbf{S}$$

$$\Rightarrow ts \in \mathfrak{p} \cap \mathbf{S} = \varnothing, \quad (\rightarrow\leftarrow). \qquad \therefore\ \mathfrak{m} \neq (1_{\mathbf{S}^{-1}\mathbf{A}}).$$

Sea $\frac{a}{s} \in \mathbf{A}_{\mathfrak{p}} - \mathfrak{m}$.

$$\frac{a}{s} \in \mathbf{A}_{\mathfrak{p}} - \mathfrak{m} \Rightarrow \frac{a}{s} \notin \mathfrak{m}$$

$$\Rightarrow a \notin \mathfrak{p}$$

$\Rightarrow \; a \in \mathbf{S}$

$\Rightarrow \; \dfrac{s}{a} \in \mathbf{A}_{\mathfrak{p}}$

$\Rightarrow \; \left(\dfrac{a}{s}\right)\left(\dfrac{s}{a}\right) = \dfrac{1}{1}, \qquad \left(\dfrac{1}{1} \text{ la unidad en } \mathbf{A}_{\mathfrak{p}}\right)$

$\Rightarrow \; \dfrac{a}{s}$ es una unidad en $\mathbf{A}_{\mathfrak{p}}$.

Luego todo elemento $x \in \mathbf{A}_{\mathfrak{p}} - \mathfrak{m}$, es una unidad en $\mathbf{A}_{\mathfrak{p}}$, por tanto en virtud de la proposición (1.2.8) $\mathbf{A}_{\mathfrak{p}}$ es un anillo local con ideal maximal $\mathfrak{m}$; es decir que $\mathfrak{m}$ es el único ideal maximal en $\mathbf{A}_{\mathfrak{p}}$. ■

Definición 1.6.3: El proceso de paso de $\mathbf{A}$ a $\mathbf{A}_{\mathfrak{p}}$ se llama **Localización de $\mathbf{A}$** en $\mathfrak{p}$.

1.7: Extensión y contracción de ideales en anillos de fracciones.

Sea $\mathbf{A}$ un anillo, $\mathbf{S}$ un sistema multiplicativo de $\mathbf{A}$ y $\psi : \mathbf{A} \to \mathbf{S}^{-1}\mathbf{A}$ el homomorfismo natural definido por $\psi(x) = \dfrac{x}{1}$. Sea $\mathbf{C} = \{\mathfrak{a} \;/\; \mathfrak{a}^{ec} = \mathfrak{a}\}$ el conjunto de todos los ideales **contraídos** en $\mathbf{A}$ y $\mathbf{E} = \{\mathfrak{b} \;/\; \mathfrak{b}^{ce} = \mathfrak{b}\}$ el conjunto de todos los ideales **extendidos** en $\mathbf{S}^{-1}\mathbf{A}$.

Proposición 1.7.1: Sea $\mathbf{A}$ un anillo, $\mathbf{S}$ un sistema multiplicativo de $\mathbf{A}$. Cada ideal en $\mathbf{S}^{-1}\mathbf{A}$ es un ideal extendido de $\mathbf{A}$.

Demostración:

Se demuestra que si $\mathfrak{b}$ es un ideal de $\mathbf{S}^{-1}\mathbf{A}$, entonces existe un ideal $\mathfrak{a}$ en $\mathbf{A}$ tal que $\mathfrak{b} = \mathfrak{a}^e$.

Sea $\frac{a}{s} \in \mathfrak{b}$, con $a \in \mathbf{A}$, $s \in \mathbf{S}$.

$\mathbf{S}$ es un sistema multiplicativo $\Rightarrow$ $1 \in \mathbf{S}$

$$\Rightarrow \frac{s}{1} \in \mathbf{S}^{-1}\mathbf{A} \quad \forall s \in \mathbf{S}$$

$$\Rightarrow \left(\frac{a}{s}\right)\left(\frac{s}{1}\right) = \left(\frac{a}{s}\right)\left(\frac{s}{1}\right) = \frac{a}{1} \in \mathfrak{b}, \ \textbf{(} \ \mathfrak{b} \text{ ideal en } \mathbf{S}^{-1}\mathbf{A}\textbf{)}$$

$$\Rightarrow \psi(a) \in \mathfrak{b}$$

$$\Rightarrow a \in \mathfrak{b}^c$$

$$\Rightarrow \frac{a}{1} = \left(\frac{1}{1}\right)\psi(a) \in \left(\mathfrak{b}^c\right)^e$$

$$\Rightarrow \left(\frac{1}{s}\right)\left(\frac{a}{1}\right) = \frac{a}{s} \in \left(\mathfrak{b}^c\right)^e, \ \textbf{(} \left(\mathfrak{b}^c\right)^e \text{ es un ideal en } \mathbf{S}^{-1}\mathbf{A}\textbf{)}.$$

Lo que prueba que $\mathfrak{b} \subseteq \left(\mathfrak{b}^c\right)^e$. En consecuencia del inciso (iv) de la proposición 1.3.3 $\left(\mathfrak{b}^c\right)^e \subseteq \mathfrak{b}$ por tanto $\left(\mathfrak{b}^c\right)^e = \mathfrak{b}$.

$\therefore$ Si $\mathfrak{b}$ es un ideal en $\mathbf{S}^{-1}\mathbf{A}$, entonces existe un ideal $\mathfrak{a}$ en $\mathbf{A}$ tal que $\left(\mathfrak{b}^c\right)^e = \mathfrak{b}$. ■

Observación: Según la proposición anterior, se tiene que todo ideal en $\mathbf{S}^{-1}\mathbf{A}$, es un ideal extendido o que coincide con el ideal generado por la imagen directa, vía $\psi : \mathbf{A} \to \mathbf{S}^{-1}\mathbf{A}$, de algún ideal de $\mathbf{A}$.

En lo sucesivo a los ideales de $\mathbf{S}^{-1}\mathbf{A}$ se denotarán por $\mathbf{S}^{-1}\mathfrak{a}$. Esta notación no es casual ya que el ideal de $\mathbf{S}^{-1}\mathbf{A}$, que genera la imagen vía ψ de $\mathfrak{a}$ coincide con el ideal de $\mathbf{S}^{-1}\mathbf{A}$ generado por las fracciones con numerador en $\mathfrak{a}$ y denominador en $\mathbf{S}$ (**véase la siguiente proposición**).

Proposición 1.7.2: Sea $\mathbf{A}$ un anillo y $\mathbf{S}$ un sistema multiplicativo de $\mathbf{A}$. Si $\mathfrak{a}$ es un ideal en $\mathbf{A}$, entonces el subconjunto de fracciones con numerador en $\mathfrak{a}$ es un ideal, que coincide con $\mathfrak{a}^e$ y se denotara por $\mathbf{S}^{-1}\mathfrak{a}$.

Demostración:

Ahora se demuestra que: $\mathfrak{a}^e = \mathbf{S}^{-1}\mathfrak{a} = \left\{ \frac{a}{s} \in \mathbf{S}^{-1}\mathbf{A} \;\middle|\; a \in \mathfrak{a},\ s \in \mathbf{S} \right\}$.

Sea $x \in \mathfrak{a}^e$.

$$x \in \mathfrak{a}^e \;\Rightarrow\; x \;=\; \sum_{i=1}^{n}\left(\frac{a_i}{s_i}\right)\psi\left(b_i\right),\ \text{donde}\ a_i \in \mathbf{A},\ \ s_i \in \mathbf{S}\ \ b_i \in \mathfrak{a}$$

$$= \sum_{i=1}^{n}\left(\frac{a_i}{s_i}\right)\left(\frac{b_i}{1}\right)$$

$$= \sum_{i=1}^{n}\left(\frac{x_i}{s_i}\right); \qquad x_i = a_i b_i \in \mathfrak{a},\ s_i \in \mathbf{S}$$

$$= \sum_{i=1}^{n}\left(\frac{x_i t_i}{\mathbf{s}}\right); \quad \text{donde}\ \mathbf{s} = \prod_{i=1}^{n} s_i\ \ \text{y}\ \ t_i = \prod_{\substack{j=1\\ j\neq i}}^{n} s_j$$

$$= \frac{\sum_{i=1}^{n} x_i t_i}{\mathbf{s}}$$

$$= \frac{\sum_{i=1}^{n} x_i t_i}{\prod_{i=1}^{n} s_i} \in \mathbf{S}^{-1}\,\mathfrak{a}.$$

$$\therefore\ \ \mathfrak{a}^e \subseteq \mathbf{S}^{-1}\,\mathfrak{a}.$$

Sea $x \in \mathbf{S}^{-1}\,\mathfrak{a}$.

$$x \in \mathbf{S}^{-1}\,\mathfrak{a} \;\Rightarrow\; x = \frac{a}{s},\ \ a \in \mathfrak{a}\ \ \text{y}\ \ s \in \mathbf{S}$$

$$\Rightarrow\ x = \left(\frac{a}{1}\right)\left(\frac{1}{s}\right);\ \ \text{donde}\ \ \frac{a}{1}, \frac{1}{s} \in \mathbf{S}^{-1}\,\mathbf{A}$$

$$\Rightarrow \quad x = \psi(a)\left(\frac{1}{s}\right) \in \mathfrak{a}^e$$

$$\Rightarrow \quad x \in \mathfrak{a}^e.$$

$$\therefore \quad \mathbf{S}^{-1}\mathfrak{a} \subseteq \mathfrak{a}^e.$$

Por lo tanto $\mathbf{S}^{-1}\mathfrak{a} = \mathfrak{a}^e$. Se deduce que si $\mathfrak{a}$ es un ideal en $\mathbf{A}$, entonces el subconjunto de fracciones con numerador en $\mathfrak{a}$ es un ideal, que coincide con $\mathfrak{a}^e$. ■

Proposición 1.7.3: Sea $\mathbf{A}$ un anillo y $\mathbf{S}$ un sistema multiplicativo de $\mathbf{A}$.

(i) Si $\mathfrak{a}$ es un ideal en $\mathbf{A}$, entonces $\mathfrak{a}^{ec} = \bigcup_{s \in \mathbf{S}} (\mathfrak{a} : s)$.

(ii) $\mathfrak{a}^e = (1_{\mathbf{S}^{-1}\mathbf{A}})$ si y sólo si $\mathfrak{a} \cap \mathbf{S} \neq \varnothing$.

(iii) $(\mathfrak{a} \in \mathbf{C}\ ) \Leftrightarrow ($ningún elemento de $\mathbf{S}$ es divisor de cero en $\mathbf{A}/\mathfrak{a})$.

Demostración (i):

Se define el conjunto, $(\mathfrak{a} : s) = \{\ x \in \mathbf{A} \ \mid \ sx \in \mathfrak{a}\ \}$. Se verifica lo siguiente:

(1) $\mathfrak{a}^{ec} \subseteq \bigcup_{s \in \mathbf{S}} (\mathfrak{a} : s)$.

(2) $\bigcup_{s \in \mathbf{S}} (\mathfrak{a} : s) \subseteq \mathfrak{a}^{ec}$.

(1) Sea $x \in \mathfrak{a}^{ec}$.

$$x \in \mathfrak{a}^{ec} \Rightarrow \psi(x) \in \mathfrak{a}^{e} = \mathbf{S}^{-1}\,\mathfrak{a}$$

$$\Rightarrow \frac{x}{1} \in \mathfrak{a}^{e} = \mathbf{S}^{-1}\,\mathfrak{a}$$

$$\Rightarrow \frac{x}{1} = \frac{a}{s}, \quad \text{para algún } a \in \mathfrak{a} \text{ y } s \in \mathbf{S}$$

$$\Rightarrow (x, 1) \equiv (a, s)$$

$$\Rightarrow \exists\ u \in \mathbf{S} \text{ t. q. } u(x \cdot s - a \cdot 1) = 0$$

$$\Rightarrow x(us) = au$$

$$\Rightarrow xh = au, \qquad \text{donde } h = us \in \mathbf{S}$$

$$\Rightarrow xh \in \mathfrak{a}, \qquad (\mathfrak{a} \text{ es un ideal de } \mathbf{A})$$

$$\Rightarrow x \in (\mathfrak{a} : h) \subseteq \bigcup_{s \in \mathbf{S}} (\mathfrak{a} : s)$$

$$\Rightarrow x \in \bigcup_{s \in \mathbf{S}} (\mathfrak{a} : s).$$

$$\therefore \quad \mathfrak{a}^{ec} \subseteq \bigcup_{s \in \mathbf{S}} (\mathfrak{a} : s).$$

(2) Sea $x \in \bigcup_{s \in \mathbf{S}} (\mathfrak{a} : s)$.

$$x \in \bigcup_{s \in \mathbf{S}} (\mathfrak{a} : s) \;\Rightarrow\; x \in (\mathfrak{a} : s), \text{ para algún } s \in \mathbf{S}$$

$$\Rightarrow\; xs \in \mathfrak{a}$$

$$\Rightarrow\; \frac{xs}{s} \in \mathbf{S}^{-1}\,\mathfrak{a} = \mathfrak{a}^e$$

$$\Rightarrow\; \left(\frac{x}{1}\right)\left(\frac{s}{s}\right) \in \mathfrak{a}^e$$

$$\Rightarrow\; \frac{x}{1} \in \mathfrak{a}^e$$

$$\Rightarrow\; \psi(x) \in \mathfrak{a}^e$$

$$\Rightarrow\; x \in \left(\mathfrak{a}^e\right)^c.$$

$$\therefore\; \bigcup_{s \in \mathbf{S}} (\mathfrak{a} : s) \subseteq \mathfrak{a}^{ec}.$$

De lo probado en (1) y (2) se concluye que $\mathfrak{a}^{ec} = \bigcup_{s \in \mathbf{S}} (\mathfrak{a} : s)$.

Demostración (ii):

Se prueba que $\left(\mathfrak{a}^e = (1_{\mathbf{S}^{-1}\mathbf{A}})\right) \Leftrightarrow \left(\mathfrak{a} \cap \mathbf{S} \neq \varnothing\right)$.

"$\Rightarrow$".

$\mathfrak{a}^e = (1_{\mathbf{S}^{-1}\mathbf{A}}) \ \Rightarrow \ \exists \quad a \in \mathfrak{a} \ \text{ y } \ s \in \mathbf{S} \quad \text{t. q.} \ \ \dfrac{a}{s} = \dfrac{1}{1}$

$\Rightarrow \ (a\,, s) \equiv (1, 1)$

$\Rightarrow \ \exists \ \ t \in \mathbf{S} \ \ \text{t. q.} \ \ t(a \cdot 1 - 1 \cdot s) = 0$

$\Rightarrow \ ta = ts$

$\Rightarrow \ ta \in \mathfrak{a} \ \ y \ \ ts \in \mathbf{S},$ **(**$\mathfrak{a}$ ideal en **A** y **S** un sistema multiplicativo)

$\Rightarrow \ ta \in \mathfrak{a} \cap \mathbf{S}$

$\Rightarrow \ \mathfrak{a} \cap \mathbf{S} \neq \varnothing.$

$$\therefore \ \ \mathfrak{a}^e = (1_{\mathbf{S}^{-1}\mathbf{A}}) \ \Rightarrow \ \mathfrak{a} \cap \mathbf{S} \neq \varnothing.$$

"$\Leftarrow$" Se supone que $\mathfrak{a} \cap \mathbf{S} \neq \varnothing$.

$\mathfrak{a} \cap \mathbf{S} \neq \varnothing \ \Rightarrow \ \exists \ x \in \mathbf{A} \ \ \text{t. q.} \ \ x \in \mathfrak{a} \cap \mathbf{S}$

$\Rightarrow \ x \in \mathfrak{a} \ \text{ y } \ x \in \mathbf{S}$

$\Rightarrow \ \dfrac{x}{x} \in \mathbf{S}^{-1}\mathfrak{a} = \mathfrak{a}^e, \qquad \left(\dfrac{x}{x} \text{ la unidad en } \mathbf{S}^{-1}\mathbf{A}\right)$

$$\Rightarrow \ \frac{1}{1} \in \mathfrak{a}^e$$

$$\Rightarrow \ (1_{\mathbf{S}^{-1}\mathbf{A}}) \subseteq \mathfrak{a}^e \subseteq (1_{\mathbf{S}^{-1}\mathbf{A}})$$

$$\Rightarrow \ \mathfrak{a}^e = (1_{\mathbf{S}^{-1}\mathbf{A}}).$$

$$\therefore \ \ \mathfrak{a} \cap \mathbf{S} \neq \varnothing \ \Rightarrow \ \mathfrak{a}^e = (1_{\mathbf{S}^{-1}\mathbf{A}}).$$

Demostración (iii):

Sea $\mathfrak{a} \in \mathbf{C} = \left\{ \mathfrak{a} \ \mid \ \mathfrak{a}^{ec} = \mathfrak{a} \right\}$ y $\mathbf{S}$ un sistema multiplicativo en $\mathbf{A}$.

Se demuestra que: $\left(\mathfrak{a} \in \mathbf{C}\right) \Leftrightarrow$ (ningún elemento de $\mathbf{S}$ es divisor de cero en $\mathbf{A}/\mathfrak{a}$).

"$\Rightarrow$"

$\mathfrak{a} \in \mathbf{C} \ \Rightarrow \ \mathfrak{a} = \mathfrak{a}^{ec} = \bigcup_{s \in \mathbf{S}} \left(\mathfrak{a} : s\right),$ (Por inciso (i)).

Sea $s \in \mathbf{S}$ un divisor de cero en $\mathbf{A}/\mathfrak{a}$.

s divide a cero en $\mathbf{A}/\mathfrak{a} \ \Rightarrow \ \exists \ x + \mathfrak{a} \in \mathbf{A}/\mathfrak{a}, \ x + \mathfrak{a} \neq \mathfrak{a}$ t. q. $s\left(x + \mathfrak{a}\right) = \mathfrak{a}$

$$\Rightarrow \ sx + \mathfrak{a} = \mathfrak{a}$$

$$\Rightarrow \ sx \in \mathfrak{a}$$

$$\Rightarrow \; x \in (\mathfrak{a} : s) \subseteq \bigcup_{s \in \mathbf{S}} (\mathfrak{a} : s)$$

$$\Rightarrow \; x \in \bigcup_{s \in \mathbf{S}} (\mathfrak{a} : s) = \mathfrak{a}$$

$$\Rightarrow \; x \in \mathfrak{a}$$

$$\Rightarrow \; x + \mathfrak{a} = \mathfrak{a}, \; (\rightarrow\leftarrow).$$

$\therefore$ $\mathbf{S}$ no tiene divisores de cero en $\mathbf{A}/\mathfrak{a}$.

"$\Leftarrow$"

Sea $\mathfrak{a}$ un ideal de $\mathbf{A}$ y suponga que ningún elemento de $\mathbf{S}$ es divisor de cero en $\mathbf{A}/\mathfrak{a}$.

Se prueba que $\mathfrak{a} = \mathfrak{a}^{ec}$.

Sea $x \in \mathfrak{a}^{ec}$.

$$x \in \mathfrak{a}^{ec} \;\Rightarrow\; x \in \bigcup_{s \in \mathbf{S}} (\mathfrak{a} : s)$$

$$\Rightarrow \; x \in (\mathfrak{a} : s), \text{ para algún } s \in \mathbf{S}$$

$$\Rightarrow \; xs \in \mathfrak{a}$$

$$\Rightarrow \; xs + \mathfrak{a} = \mathfrak{a}$$

$$\Rightarrow \quad s(x+\mathfrak{a})=\mathfrak{a}, \quad (\ \mathbf{S} \text{ no contiene divisores de cero en } \mathbf{A}/\mathfrak{a}\ )$$

$$\Rightarrow \quad x+\mathfrak{a}=\mathfrak{a}$$

$$\Rightarrow \quad x\in\mathfrak{a}.$$

De donde $\mathfrak{a}^{ec}\subseteq\mathfrak{a}$. Recíprocamente, $\mathfrak{a}^{ec}\supseteq\mathfrak{a}$ por el inciso (iii) de la proposición 1.3.3 por tanto $\mathfrak{a}=\mathfrak{a}^{ec}=\left(\mathfrak{a}^{e}\right)^{c}$, entonces $\mathfrak{a}\in\mathbf{C}$.

$$\therefore \left(\text{Ningún elemento de } \mathbf{S} \text{ es divisor de cero en } \mathbf{A}/\mathfrak{a}\ \right)\Rightarrow\left(\ \mathfrak{a}\in\mathbf{C}\right). \ \blacksquare$$

Proposición 1.7.4: Los ideales primos de $\mathbf{S}^{-1}\mathbf{A}$ están en correspondencia biyectiva con los ideales primos de $\mathbf{A}$ que no cortan a $\mathbf{S}$.

Demostración:

Considere los siguientes conjuntos:

$\mathfrak{F}=\{\mathfrak{p}\mid \mathfrak{p}$ es un ideal primo en $\mathbf{A}$ y $\mathfrak{p}\cap\mathbf{S}=\varnothing\}$ y $\mathfrak{I}=\{\mathfrak{q}\mid \mathfrak{q}$ es un ideal primo en $\mathbf{S}^{-1}\mathbf{A}\}$.

Se define la aplicación de $\mathfrak{F}$ en $\mathfrak{I}$ como sigue:

$$\begin{aligned} \tau : \mathfrak{F} &\longrightarrow \mathfrak{I} \\ \mathfrak{p} &\rightarrow \tau(\mathfrak{p})=\mathbf{S}^{-1}\mathfrak{p}. \end{aligned}$$

Se verifica que la aplicación τ satisface lo siguiente:

(1) τ es cerrada, (de primo a primo).

(2) τ están bien definida.

(3) τ es inyectiva.

(4) τ es sobreyectiva.

Demostración (1):

Sea $\mathfrak{p}$ un ideal primo de $\mathbf{A}$ tal que $\mathfrak{p} \cap \mathbf{S} = \varnothing$. Se demuestra que el ideal $\mathbf{S}^{-1}\mathfrak{p}$ es un ideal primo en $\mathbf{S}^{-1}\mathbf{A}$.

Como $\mathfrak{p} \cap \mathbf{S} = \varnothing$, entoces por la proposición 1.7.3, inciso (ii) $\mathbf{S}^{-1}\mathfrak{p} \neq \mathbf{S}^{-1}\mathbf{A}$. Por tanto $\mathbf{S}^{-1}\mathfrak{p}$ es un ideal propio.

Sea $\dfrac{a}{s}, \dfrac{a'}{s'} \in \mathbf{S}^{-1}\mathbf{A}$ t. q. $\left(\dfrac{a}{s}\right)\left(\dfrac{a'}{s'}\right) \in \mathbf{S}^{-1}\mathfrak{p}$.

$$\left(\frac{a}{s}\right)\left(\frac{a'}{s'}\right) \in \mathbf{S}^{-1}\mathfrak{p} \;\Rightarrow\; \frac{aa'}{ss'} \in \mathbf{S}^{-1}\mathfrak{p}$$

$$\Rightarrow\; \exists\; b \in \mathfrak{p} \text{ y } t \in \mathbf{S} \quad \text{t. q.} \quad \frac{aa'}{ss'} = \frac{b}{t}$$

$$\Rightarrow\; (aa', ss') \equiv (b, t)$$

$$\Rightarrow \ \exists \ u \in \mathbf{S} \ \text{ t. q. } \ u\left(aa't - bss'\right) = 0$$

$$\Rightarrow \ u\left(aa't\right) = u\left(bss'\right)$$

$$\Rightarrow \ aa'\left(ut\right) = b\left(uss'\right)$$

$$\Rightarrow \ aa'\left(ut\right) \in \mathfrak{p}, \quad \left(\mathfrak{p} \text{ es ideal en } \mathbf{A},\ b \in \mathfrak{p} \ \text{ y } \ uss' \in \mathbf{A}\right)$$

$$\Rightarrow \ aa' \in \mathfrak{p} \quad \vee \quad ut \in \mathfrak{p}$$

$$\Rightarrow \ aa' \in \mathfrak{p}, \quad \left(\mathfrak{p} \text{ no corta a } \mathbf{S};\text{ es decir } \mathfrak{p} \cap \mathbf{S} = \varnothing\right)$$

$$\Rightarrow \ a \in \mathfrak{p} \quad \vee \quad a' \in \mathfrak{p}$$

$$\Rightarrow \ \frac{a}{s} \in \mathbf{S}^{-1}\,\mathfrak{p} \ \vee \ \frac{a'}{s'} \in \mathbf{S}^{-1}\,\mathfrak{p}.$$

Luego, $\mathbf{S}^{-1}\,\mathfrak{p}$ es un ideal primo de $\mathbf{S}^{-1}\,\mathbf{A}$.

$\therefore$ La aplicación τ es cerrada.

Demostración (2):

Sean $\mathfrak{p}_1, \mathfrak{p}_2 \in \mathfrak{F}$ ideales primos en $\mathbf{A}$, tal que $\mathfrak{p}_1 = \mathfrak{p}_2$. Se demuestra que $\mathbf{S}^{-1}\,\mathfrak{p}_1 = \mathbf{S}^{-1}\,\mathfrak{p}_2$.

$$\mathbf{S}^{-1}\,\mathfrak{p}_1 = \left\{ \frac{a}{s} \in \mathbf{S}^{-1}\,\mathbf{A} \mid \ a \in \mathfrak{p}_1 \ \text{ y } \ s \in \mathbf{S} \right\}$$

$$=\left\{\frac{a}{s}\in \mathbf{S}^{-1}\,\mathbf{A} \mid a\in \mathfrak{p}_2 \quad \text{y} \quad s\in \mathbf{S}\right\}$$

$$=\mathbf{S}^{-1}\,\mathfrak{p}_2.$$

$\therefore$ τ están bien definida.

Demostración (3):

Sean $\mathfrak{p}_1, \mathfrak{p}_2 \in \mathfrak{F}$ ideales primos en $\mathbf{A}$, tal que $\mathbf{S}^{-1}\,\mathfrak{p}_1 = \mathbf{S}^{-1}\,\mathfrak{p}_2$. Se demuestra que $\mathfrak{p}_1 = \mathfrak{p}_2$.

Dado $a \in \mathfrak{p}_1$.

$$a\in \mathfrak{p}_1 \quad \Rightarrow \quad \frac{a}{1}\in \mathbf{S}^{-1}\,\mathfrak{p}_1 = \mathbf{S}^{-1}\,\mathfrak{p}_2$$

$$\Rightarrow \quad \exists \quad b\in \mathfrak{p}_2 \ \text{ y } \ s\in \mathbf{S} \quad \text{t. q. } \ \frac{a}{1}=\frac{b}{s}$$

$$\Rightarrow \quad (a,1)\equiv(b,s)$$

$$\Rightarrow \ \exists \ u\in \mathbf{S} \quad u\left(as-b\cdot 1\right)=0$$

$$\Rightarrow \ uas = bu$$

$$\Rightarrow \ a(us)\in \mathfrak{p}_2 \ \text{ y } \ us\in \mathbf{S}, \quad (\mathfrak{p}_2 \text{ es ideal y } \mathbf{S} \text{ sistema multiplicativo })$$

$$\Rightarrow \ a\in \mathfrak{p}_2 \quad \text{ó} \quad us\in \mathfrak{p}_2, \quad (\mathfrak{p}_2 \text{ es ideal primo})$$

$$\Rightarrow \ a\in \mathfrak{p}_2, \quad (\mathfrak{p}_2 \cap \mathbf{S} = \varnothing\ ).$$

La otra inclusión se prueba de manera análoga. Luego $\mathfrak{p}_1 = \mathfrak{p}_2$.

$\therefore$ La aplicación τ es inyectiva.

Demostración (4):

Sea $\mathfrak{q}$ un ideal primo en $\mathbf{S}^{-1}\mathbf{A}$. Se demuestra que existe $\mathfrak{p} \in \mathfrak{F}$ tal que $\mathbf{S}^{-1}\mathfrak{p} = \mathfrak{q}$.

Si $\mathfrak{q}$ un ideal primo de $\mathbf{S}^{-1}\mathbf{A}$, entonces por la proposición 1.7.1, existe un ideal $\mathfrak{a}$ en $\mathbf{A}$, tal que;

$$\mathfrak{a}^e = \mathbf{S}^{-1}\mathfrak{a} = \mathfrak{q}.$$

Verifíquese que $\mathfrak{a} \in \mathfrak{F}$. Para ello se prueba que se satisface lo siguiente:

(i) $\mathfrak{a} \cap \mathbf{S} = \varnothing$.

(ii) $\mathfrak{a} \neq (1)$.

(iii) Si existen $x, y \in \mathbf{A}$ tal que $xy \in \mathfrak{a}$, entonces $x \in \mathfrak{a}$ ó $y \in \mathfrak{a}$.

Demostración (i): Supóngase que $\mathfrak{a} \cap \mathbf{S} \neq \varnothing$.

$$\mathfrak{a} \cap \mathbf{S} \neq \varnothing \quad \Rightarrow \quad \mathfrak{a}^e = \mathbf{S}^{-1}\mathbf{A}, \quad \big(\text{Proposición 7.7.3 (ii)}\big)$$

$$\Rightarrow \quad \mathfrak{q} = \mathbf{S}^{-1}\mathbf{A}, \quad (\rightarrow\leftarrow).$$

$\therefore$ $\mathfrak{a} \cap \mathbf{S} = \varnothing$.

Demostración (ii):

Supóngase que $\mathfrak{a} = (1)$.

$\mathfrak{a} = (1) \;\Rightarrow\; \exists\; x \in \mathfrak{a} \;$ t. q. $\; x = 1$

$\Rightarrow\; 1 \in \mathfrak{a}\;$ y $\;1 \in \mathbf{S}$

$\Rightarrow\; 1 \in \mathfrak{a} \cap \mathbf{S} = \varnothing, \;(\to\leftarrow).$

$\therefore\;\; \mathfrak{a} \neq (1).$

Demostración (ii):

Sea $x, y \in \mathbf{A}$ t. q. $xy \in \mathfrak{a}$.

$$xy \in \mathfrak{a} \;\Rightarrow\; \frac{xy}{1} = \left(\frac{x}{1}\right)\left(\frac{y}{1}\right) \in \mathbf{S}^{-1}\mathfrak{a} = \mathfrak{q}$$

$$\Rightarrow\; \frac{x}{1} \in \mathbf{S}^{-1}\mathfrak{a} \;\text{ ó }\; \frac{y}{1} \in \mathbf{S}^{-1}\mathfrak{a}$$

$$\Rightarrow\; x \in \mathfrak{a} \;\text{ ó }\; y \in \mathfrak{a}.$$

Luego $\mathfrak{a}$ es un ideal primo en $\mathbf{A}$ que verifica $\mathfrak{a} \cap \mathbf{S} = \varnothing$. De donde $\mathfrak{a} \in \mathfrak{F}$.

$\therefore\; \tau$ La aplicación es sobreyectiva.■

Observación: Si $\mathfrak{q}$ es un ideal primo en $\mathbf{S}^{-1}\mathbf{A}$, entonces de la definición 1.3.2 observación (2), $\mathfrak{q}^c$ es un ideal primo de $\mathbf{A}$.

Corolario 1.7.5: Si $\mathfrak{p}$ es un ideal primo de $\mathbf{A}$, los ideales primos del anillo local $\mathbf{A}_\mathfrak{p}$ están en correspondencia biyectiva con los ideales primos de $\mathbf{A}$ contenidos en $\mathfrak{p}$.

Demostración:

Sean $\mathfrak{a}$, $\mathfrak{p}$ ideales primos en $\mathbf{A}$, en virtud de la proposición 1.6.1 $\mathbf{S}=\mathbf{A}-\mathfrak{p}$ es un sistema multiplicativo de $\mathbf{A}$. Se demuestra que $\mathfrak{a}$ no corta a $\mathbf{S}$ si y sólo si $\mathfrak{a}\subseteq\mathfrak{p}$; es decir:

$$\mathfrak{a}\cap\mathbf{S}=\varnothing \Leftrightarrow \mathfrak{a}\subseteq\mathfrak{p}.$$

$"\Rightarrow"$.

Suponga que $\mathfrak{a}\cap\mathbf{S}=\varnothing$.

Sea $x\in\mathfrak{a}$.

$$\begin{aligned} x\in\mathfrak{a} \quad &\Rightarrow \quad x\notin\mathbf{S}=\mathbf{A}-\mathfrak{p}, \quad (\mathfrak{a}\text{ no corta a }\mathbf{S}) \\ &\Rightarrow \quad x\in\mathfrak{p} \\ &\Rightarrow \quad \mathfrak{a}\subseteq\mathfrak{p}. \end{aligned}$$

$$\therefore \quad \text{Si } \mathfrak{a}\cap\mathbf{S}=\varnothing, \text{ entonces } \mathfrak{a}\subseteq\mathfrak{p}.$$

$"\Leftarrow"$.

Suponga que $\mathfrak{a} \subseteq \mathfrak{p}$ y $\mathfrak{a}$ corta a $\mathbf{S}$, es decir; $\mathfrak{a} \cap \mathbf{S} \neq \emptyset$.

$$\begin{aligned}
\mathfrak{a} \cap \mathbf{S} \neq \emptyset \quad &\Rightarrow \exists \; x \in \mathfrak{a} \cap \mathbf{S} \\
&\Rightarrow x \in \mathfrak{a} \;\text{ y }\; x \in \mathbf{S} \\
&\Rightarrow x \in \mathfrak{a} \;\text{ y }\; x \notin \mathfrak{p} \\
&\Rightarrow \mathfrak{a} \not\subseteq \mathfrak{p}, \quad (\rightarrow\leftarrow).
\end{aligned}$$

$$\therefore \text{ Si } \mathfrak{a} \subseteq \mathfrak{p}, \text{ entonces } \mathfrak{a} \cap \mathbf{S} = \emptyset.$$

Por la proposición 1.7.4, los ideales primos de $\mathbf{A}_{\mathfrak{p}} = \mathbf{S}^{-1}\mathbf{A}$ están en correspondencia biyectiva con los ideales primos de $\mathbf{A}$ que no cortan a $\mathbf{S}$, es decir; con los ideales primos de $\mathbf{A}$ contenidos en $\mathfrak{p}$. Luego los ideales primos del anillo local $\mathbf{A}_{\mathfrak{p}}$ están en correspondencia biyectiva con los ideales primos de $\mathbf{A}$ contenidos en $\mathfrak{p}$. ■

Nota: Si $\mathfrak{p}$ es un ideal primo de un anillo $\mathbf{A}$, el localizado $\mathbf{A}_{\mathfrak{p}}$ tiene un único ideal maximal, ver proposición 1.6.2. Por tanto es un **anillo local,** y existe una biyección entre ideales primos de $\mathbf{A}_{\mathfrak{p}}$ y los ideales primos de $\mathbf{A}$ contenidos en $\mathfrak{p}$. En consecuencia, si $\mathfrak{p}$ es un ideal primo minimal (**no contiene a ningún otro ideal primo**) de $\mathbf{A}$, entonces $\mathbf{A}_{\mathfrak{p}}$ es un anillo con un único ideal primo.

Proposición 1.7.6: Sea $\mathbf{A}$ un anillo y $\mathbf{S}$ un sistema multiplicativo de $\mathbf{A}$, entonces $\mathbf{S}^{-1}$ satisface las siguientes operaciones de ideales:

(i) $\mathbf{S}^{-1}(\mathfrak{a}+\mathfrak{b})=\mathbf{S}^{-1}(\mathfrak{a})+\mathbf{S}^{-1}(\mathfrak{b})$.

(ii) $\mathbf{S}^{-1}(\mathfrak{a}\cap\mathfrak{b})=\mathbf{S}^{-1}(\mathfrak{a})\cap\mathbf{S}^{-1}(\mathfrak{b})$.

(iii) $\mathbf{S}^{-1}(\mathfrak{a}\mathfrak{b})=\mathbf{S}^{-1}(\mathfrak{a})\ \ \mathbf{S}^{-1}(\mathfrak{b})$.

(iv) $\mathbf{S}^{-1}(r(\mathfrak{a}))=r(\mathbf{S}^{-1}(\mathfrak{a}))$.

Demostración (i):

Se demuestra que $\mathbf{S}^{-1}(\mathfrak{a}+\mathfrak{b})=\mathbf{S}^{-1}(\mathfrak{a})+\mathbf{S}^{-1}(\mathfrak{b})$.

Del inciso (i) de la proposición 1.3.4,

$$(\mathfrak{a}+\mathfrak{b})^e=\mathfrak{a}^e+\mathfrak{b}^e.$$

Luego por la proposición 1.7.2:

$$\mathbf{S}^{-1}(\mathfrak{a}+\mathfrak{b})=(\mathfrak{a}+\mathfrak{b})^e=\mathfrak{a}^e+\mathfrak{b}^e=\mathbf{S}^{-1}(\mathfrak{a})+\mathbf{S}^{-1}(\mathfrak{b}).$$

$\therefore$ $\mathbf{S}^{-1}$ conmuta con sumas finitas de ideales.

Demostración (ii):

Se demuestra que $\mathbf{S}^{-1}(\mathfrak{a}\cap\mathfrak{b})=\mathbf{S}^{-1}(\mathfrak{a})\cap\mathbf{S}^{-1}(\mathfrak{b})$.

Del inciso (ii) de la proposición 1.3.4;

$$(\mathfrak{a}\cap\mathfrak{b})^e\subseteq\mathfrak{a}^e\cap\mathfrak{b}^e.$$

Entonces por la proposición 1.7.2,

$$\mathbf{S}^{-1}(\mathfrak{a}\cap\mathfrak{b})=(\mathfrak{a}\cap\mathfrak{b})^e\subseteq\mathfrak{a}^e\cap\mathfrak{b}^e=\mathbf{S}^{-1}(\mathfrak{a})\cap\mathbf{S}^{-1}(\mathfrak{b}).$$

Por transitividad,

$$\mathbf{S}^{-1}(\mathfrak{a}\cap\mathfrak{b})\subseteq\mathbf{S}^{-1}(\mathfrak{a})\cap\mathbf{S}^{-1}(\mathfrak{b}).$$

Para la otra inclusión, sea $x\in\mathbf{S}^{-1}\mathfrak{a}\cap\mathbf{S}^{-1}\mathfrak{b}$.

$$x\in\mathbf{S}^{-1}\mathfrak{a}\cap\mathbf{S}^{-1}\mathfrak{b}\;\Rightarrow\; x\in\mathbf{S}^{-1}\mathfrak{a}\;\text{ y }\; x\in\mathbf{S}^{-1}\mathfrak{b}$$

$$\Rightarrow\; x=\frac{a}{s}\;\text{ y }\; x=\frac{b}{t},\quad\text{donde } a\in\mathfrak{a},\; b\in\mathfrak{b}\;\text{ y }\; s,t\in\mathbf{S}$$

$$\Rightarrow\;\frac{a}{s}=\frac{b}{t}$$

$$\Rightarrow\;(a,s)\equiv(b,t)$$

$$\Rightarrow \quad \exists \quad s' \in \mathbf{S} \quad \text{t. q.} \quad s'(at - bs) = 0$$

$$\Rightarrow \; a(s't) = b(s's)$$

$$\Rightarrow \; a(s't) \in \mathfrak{a} \quad \text{y} \quad a(s't) \in \mathfrak{b}$$

$$\Rightarrow \; a(s't) \in \mathfrak{a} \cap \mathfrak{b} \quad \text{y} \quad s(s't) \in \mathbf{S}$$

$$\Rightarrow \; \frac{a(s't)}{s(s't)} \in \mathbf{S}^{-1}(\mathfrak{a} \cap \mathfrak{b})$$

$$\Rightarrow \; x = \frac{a}{s} = \left(\frac{a}{s}\right)\left(\frac{s't}{s't}\right) \in \mathbf{S}^{-1}(\mathfrak{a} \cap \mathfrak{b})$$

$$\Rightarrow \; x \in \mathbf{S}^{-1}(\mathfrak{a} \cap \mathfrak{b}). \qquad \qquad \therefore \; \mathbf{S}^{-1}(\mathfrak{a}) \cap \mathbf{S}^{-1}(\mathfrak{b}) \subseteq \mathbf{S}^{-1}(\mathfrak{a} \cap \mathfrak{b}).$$

De donde $\mathbf{S}^{-1}(\mathfrak{a} \cap \mathfrak{b}) = \mathbf{S}^{-1}(\mathfrak{a}) \cap \mathbf{S}^{-1}(\mathfrak{b})$.

$\therefore$ $\mathbf{S}^{-1}$ conmuta con intersecciones finitas de ideales.

Demostración (iii):

Se verifica que $\mathbf{S}^{-1}(\mathfrak{a}\mathfrak{b}) = \mathbf{S}^{-1}(\mathfrak{a}) \; \mathbf{S}^{-1}(\mathfrak{b})$.

Del inciso (iii) de la definición 1.3.4,

$$(\mathfrak{a}\mathfrak{b})^e = \mathfrak{a}^e \mathfrak{b}^e.$$

Por la proposición 1.7.2,

$$\mathbf{S}^{-1}(\mathfrak{a}\mathfrak{b}) = (\mathfrak{a}\mathfrak{b})^e = \mathfrak{a}^e\mathfrak{b}^e = \mathbf{S}^{-1}(\mathfrak{a})\mathbf{S}^{-1}(\mathfrak{b}).$$

Por transitividad,

$$\mathbf{S}^{-1}(\mathfrak{a}\mathfrak{b}) = \mathbf{S}^{-1}(\mathfrak{a})\mathbf{S}^{-1}(\mathfrak{b}).$$

$\therefore$ $\mathbf{S}^{-1}$ conmuta con productos finitos de ideales.

Demostración (iv):

Se demuestra que $\mathbf{S}^{-1}(r(\mathfrak{a})) = r(\mathbf{S}^{-1}\mathfrak{a})$.

Del inciso (iv) de la proposición 1.3.4,

$$(r(\mathfrak{a}))^e \subseteq r(\mathfrak{a}^e).$$

Luego por la proposición 1.7.2;

$$\mathbf{S}^{-1}(r(\mathfrak{a})) = (r(\mathfrak{a}))^e \subseteq r(\mathfrak{a}^e) = r(\mathbf{S}^{-1}\mathfrak{a}).$$

Por transitividad:

$$\mathbf{S}^{-1}(r(\mathfrak{a})) \subseteq r(\mathbf{S}^{-1}\mathfrak{a}).$$

Para la otra inclusión se toma $\frac{a}{s} \in r\left(\mathbf{S}^{-1}\mathfrak{a}\right)$.

$$\frac{a}{s} \in r\left(\mathbf{S}^{-1}\mathfrak{a}\right) \;\Rightarrow\; \exists \;\; n \in \mathbb{N} \;\; \text{t. q.} \;\; \left(\frac{a}{s}\right)^n \in \mathbf{S}^{-1}\mathfrak{a}$$

$$\Rightarrow \; \exists \;\; b \in \mathfrak{a} \;\; \text{y} \;\; t \in \mathbf{S} \;\; \text{t. q.} \;\; \frac{a^n}{s^n} = \frac{b}{t}$$

$$\Rightarrow \; \left(a^n, s^n\right) \equiv (b, t)$$

$$\Rightarrow \; \exists \;\; u \in \mathbf{S} \;\; \text{t. q.} \;\; u\left(a^n t - b s^n\right) = 0$$

$$\Rightarrow \; u a^n t = u s^n b$$

$$\Rightarrow \; u^{n-1} t^{n-1}\left(u a^n t\right) = u^{n-1} t^{n-1}\left(u s^n b\right)$$

$$\Rightarrow \; u^n a^n t^n = \left(u^n t^{n-1} s^n\right) b$$

$$\Rightarrow \; (u\,a\,t)^n \in \mathfrak{a}, \quad \left(\mathfrak{a} \text{ ideal en } \mathbf{A} \text{ y } b \in \mathfrak{a}\right)$$

$$\Rightarrow \; uat \in r(\mathfrak{a}) \;\; \text{y} \;\; ust \in \mathbf{S}$$

$$\Rightarrow \; \frac{uat}{ust} \in \mathbf{S}^{-1}\left(r(\mathfrak{a})\right)$$

$$\Rightarrow\ x=\frac{a}{s}=\left(\frac{ut}{ut}\right)\left(\frac{a}{s}\right)=\frac{uat}{ust}\ \in \mathbf{S}^{-1}\left(r\left(\mathfrak{a}\right)\right)$$

$$\Rightarrow x\in \mathbf{S}^{-1}\left(r\left(\mathfrak{a}\right)\right).$$

Luego $r\left(\mathbf{S}^{-1}\mathfrak{a}\right)\subseteq \mathbf{S}^{-1}\left(r\left(\mathfrak{a}\right)\right)$, entonces $r\left(\mathbf{S}^{-1}\mathfrak{a}\right)=\mathbf{S}^{-1}\left(r\left(\mathfrak{a}\right)\right)$.

$\therefore$ $\mathbf{S}^{-1}$ conmuta con radicales. ■

Corolario 1.7.7: Sea $\mathbf{A}$ un anillo y $\mathbf{S}$ un sistema multiplicativo de $\mathbf{A}$. Si $\mathfrak{R}_{\mathbf{A}}$ es el nilradical de $\mathbf{A}$, el nilradical de $\mathbf{S}^{-1}\mathbf{A}$ es $\mathbf{S}^{-1}\mathfrak{R}_{\mathbf{A}}$.

Demostración:

Se denota por $\mathfrak{R}_{\mathbf{S}^{-1}\mathbf{A}}$ al nilradical de $\mathbf{S}^{-1}\mathbf{A}$ y se demuestra que $\mathbf{S}^{-1}\mathfrak{R}_{\mathbf{A}}=\mathfrak{R}_{\mathbf{S}^{-1}\mathbf{A}}$.

Se verifica lo siguiente:

(1) $\mathbf{S}^{-1}\mathfrak{R}_{\mathbf{A}}\subseteq \mathfrak{R}_{\mathbf{S}^{-1}\mathbf{A}}$.

(2) $\mathfrak{R}_{\mathbf{S}^{-1}\mathbf{A}}\subseteq \mathbf{S}^{-1}\mathfrak{R}_{\mathbf{A}}$.

Demostración (1):

En la proposición 1.2.10 se definió $\mathfrak{R}_{\mathbf{A}}=\left\{x\in \mathbf{A}\ \mid\ x^{n}=0 \text{ para algún } n\in \mathbb{N}\right\}$.

Sea $\dfrac{a}{s} \in \mathbf{S}^{-1}\,\mathfrak{R}_{\mathbf{A}}$.

$$\frac{a}{s} \in \mathbf{S}^{-1}\,\mathfrak{R}_{\mathbf{A}} \;\Rightarrow\; a \in \mathfrak{R}_{\mathbf{A}} \text{ y } s \in \mathbf{S}$$

$$\Rightarrow \exists\; n \in \mathbb{N} \quad \text{t. q.} \quad a^n = 0$$

$$\Rightarrow \left(\frac{a}{s}\right)^n = \frac{a^n}{s^n} = \frac{0}{s^n} = \frac{0}{1}$$

$$\Rightarrow \left(\frac{a}{s}\right)^n = \frac{0}{1} \quad \text{para algún } n \in \mathbb{N}$$

$$\Rightarrow \frac{a}{s} \in \mathfrak{R}_{\mathbf{S}^{-1}\mathbf{A}}.$$

$$\therefore \quad \mathbf{S}^{-1}\,\mathfrak{R}_{\mathbf{A}} \subseteq \mathfrak{R}_{\mathbf{S}^{-1}\mathbf{A}}.$$

Demostración (2):

Sea $\dfrac{a}{s} \in \mathfrak{R}_{\mathbf{S}^{-1}\mathbf{A}}$, donde $a \in \mathbf{A}$ y $s \in \mathbf{S}$.

$$\frac{a}{s} \in \mathfrak{R}_{\mathbf{S}^{-1}\mathbf{A}} \;\Rightarrow\; \exists\; n \in \mathbb{N} \;\text{ t. q. }\; \left(\frac{a}{s}\right)^n = \frac{0}{1}$$

$$\Rightarrow \left(a^n,\, s^n\right) \equiv \left(0,\, 1\right) \;\text{ para algún }\; n \in \mathbb{N}$$

$$\Rightarrow\ \exists\ t \in \mathbf{S}\ \text{ t. q. }\ t\left(a^n \cdot 1 - 0 \cdot s^n\right) = 0 \text{ para algún } n \in \mathbb{N}$$

$$\Rightarrow\ ta^n = 0 \text{ para algún } n \in \mathbb{N}$$

$$\Rightarrow\ (at)^n = 0 \text{ para algún } n \in \mathbb{N}$$

$$\Rightarrow\ at \in \mathfrak{R}_{\mathbf{A}} \quad y \quad ts \in \mathbf{S}$$

$$\Rightarrow\ \frac{ta}{st} \in \mathbf{S}^{-1}\mathfrak{R}_{\mathbf{A}}$$

$$\Rightarrow\ \frac{a}{s} = \left(\frac{t}{t}\right)\left(\frac{a}{s}\right) = \left(\frac{ta}{ts}\right) \in \mathbf{S}^{-1}\mathfrak{R}_{\mathbf{A}}$$

$$\Rightarrow \frac{a}{s} \in \mathbf{S}^{-1}\mathfrak{R}_{\mathbf{A}}.$$

$$\therefore\ \mathbf{S}^{-1}\mathfrak{R}_{\mathbf{A}} \supseteq \mathfrak{R}_{\mathbf{S}^{-1}\mathbf{A}}.$$

Luego $\mathbf{S}^{-1}\mathfrak{R}_{\mathbf{A}} = \mathfrak{R}_{\mathbf{S}^{-1}\mathbf{A}}$. Así se concluye que si $\mathfrak{R}_{\mathbf{A}}$ es el nilradical de $\mathbf{A}$, el nilradical de $\mathbf{S}^{-1}\mathbf{A}$ es $\mathbf{S}^{-1}\mathfrak{R}_{\mathbf{A}}$. ■

Proposición 1.7.8: Sea $f : \mathbf{A} \to \mathbf{B}$ un homomorfismo de anillos, siendo cada ideal de $\mathbf{B}$ extendido de un ideal de $\mathbf{A}$ y $\mathfrak{p}$ un ideal primo de $\mathbf{A}$. Entonces $\mathfrak{p}$ es la contracción de un ideal primo de $\mathbf{B}$ si y sólo si $\mathfrak{p}^{ec} = \mathfrak{p}$.

Demostración:

Se demuestra que $\left(\mathfrak{p} \text{ es la contracción de un ideal primo de } \mathbf{B}\right) \Leftrightarrow \left(\mathfrak{p}^{ec} = \mathfrak{p}\right)$.

"$\Rightarrow$" Suponga que $\mathfrak{p} = \mathfrak{q}^c$ y $\mathfrak{q}$ un ideal primo de $\mathbf{B}$.

Si $\mathfrak{q}$ es un ideal en $\mathbf{B}$, entonces por hipótesis existe un ideal $\mathfrak{a} \subseteq \mathbf{A}$ tal que $\mathfrak{a}^e = \mathfrak{q}$.

Ahora, sustituyendo lo anterior y de la proposición 1.3.3 (v),

$$\mathfrak{p}^e = \left(\mathfrak{q}^c\right)^e = \left(\left(\mathfrak{a}^e\right)^c\right)^e = \mathfrak{a}^{ece} = \mathfrak{a}^e = \mathfrak{q}.$$

Tomando contracción a lo anterior;

$$\left(\mathfrak{p}^e\right)^c = \mathfrak{q}^c = \mathfrak{p}.$$

$$\therefore \quad \mathfrak{p} = \mathfrak{q}^c \quad \Rightarrow \quad \mathfrak{p}^{ec} = \mathfrak{p}.$$

"$\Leftarrow$" Se supone que $\mathfrak{p}^{ec} = \mathfrak{p}$. Se demuestra que $\mathfrak{p}^e$ es un ideal primo de $\mathbf{B}$.

Sean $\mathfrak{b}_1, \mathfrak{b}_2$ ideales de $\mathbf{B}$ tal que $\mathfrak{b}_1\mathfrak{b}_2 \subseteq \mathfrak{p}^e$.

Si $\mathfrak{b}_1, \mathfrak{b}_2$ son ideales en $\mathbf{B}$, entonces existen $\mathfrak{a}_1, \mathfrak{a}_2$ ideales en $\mathbf{A}$ tal que:

$$\mathfrak{a}_1^e = \mathfrak{b}_1 \quad \text{y} \quad \mathfrak{a}_2^e = \mathfrak{b}_2.$$

Por la proposición 1.3.3 (iii),

$$\mathfrak{a}_1\mathfrak{a}_2 \subseteq (\mathfrak{a}_1\mathfrak{a}_2)^{ec} = \left((\mathfrak{a}_1\mathfrak{a}_2)^e\right)^c$$

$$= \left(\mathfrak{a}_1^e\mathfrak{a}_2^e\right)^c, \quad \left(\text{Proposición 1.3.4 (iii)}\right)$$

$$= (\mathfrak{b}_1\mathfrak{b}_2)^c$$

$$\subseteq \left(\mathfrak{p}^e\right)^c = \mathfrak{p}^{ec} = \mathfrak{p}, \quad \left(\text{Proposición 1.3.3 (ii)}\right).$$

Luego $\mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{p}$, por hipótesis, $\mathfrak{p}$ es primo en $\mathbf{A}$, entonces por la proposición 1.2.19, resulta

$$\mathfrak{a}_1 \subseteq \mathfrak{p} \quad \text{ó} \quad \mathfrak{a}_2 \subseteq \mathfrak{p}.$$

Tomando extensiones y por la proposición 1.3.3. (i):

$$\mathfrak{b}_1 = \mathfrak{a}_1^e \subseteq \mathfrak{p}^e \quad \text{ó} \quad \mathfrak{b}_2 = \mathfrak{a}_2^e \subseteq \mathfrak{p}^e.$$

Entonces por la proposición 1.2.19, $\mathfrak{p}^e$ es un ideal primo en $\mathbf{B}$.

$$\therefore \ \left(\mathfrak{p}^{ec} = \mathfrak{p}\right) \Rightarrow \left(\mathfrak{p} \text{ es la contracción de un ideal primo de } \mathbf{B}\right).$$

Proposición 1.7.9: Sea $\mathbf{A}$ un anillo. $\mathbf{S}$ un sistema multiplicativo de $\mathbf{A}$ y $\psi : \mathbf{A} \to \mathbf{S}^{-1}\mathbf{A}$ el correspondiente homomorfismo de localización. Si $\mathfrak{a}$ es un ideal finitamente generado en $\mathbf{A}$, entonces $\mathbf{S}^{-1}\mathfrak{a}$ es un ideal finitamente generado en $\mathbf{S}^{-1}\mathbf{A}$.

Demostración:

Sea $\{a_1, \ldots, a_n\}$ un conjunto finito de generadores de $\mathfrak{a}$. Dado $\frac{x}{s} \in \mathbf{S}^{-1}\mathfrak{a}$.

$$\frac{x}{s} \in \mathbf{S}^{-1}\mathfrak{a} \Rightarrow x \in \mathfrak{a} \text{ y } s \in \mathbf{S}$$

$$\Rightarrow \exists \quad a_1', \ldots, a_n' \in \mathbf{A} \quad \text{t. q. } x = a_1'a_1 + \cdots + a_n'a_n$$

$$\Rightarrow \frac{x}{s} = \frac{a_1'a_1 + \cdots + a_n'a_n}{s}$$

$$= \left(\frac{s}{s}\right)\left(\frac{a_1'a_1 + \cdots + a_n'a_n}{s}\right), \qquad \left(\frac{s}{s} \text{ la unidad en } \mathbf{S}^{-1}\mathbf{A}\right)$$

$$= \frac{sa_1'a_1 + \cdots + sa_n'a_n}{ss}$$

$$= \left(\frac{a_1}{1}\right)\left(\frac{a_1'}{s}\right) + \cdots + \left(\frac{a_n}{1}\right)\left(\frac{a_n'}{s}\right).$$

Luego $\left\{\frac{a_1}{1}, \ldots, \frac{a_n}{1}\right\}$ es un conjunto finito de generadores de $\mathbf{S}^{-1}\mathfrak{a}$. ■

Proposición 1.7.10: Sea $\mathbf{A}$ un anillo. $\mathbf{S} \subseteq \mathbf{A}$ un sistema multiplicativo, $\mathfrak{a} \subseteq \mathbf{A}$ un ideal tal que $\mathfrak{a} \cap \mathbf{S} = \varnothing$ y $\pi : \mathbf{A} \to \mathbf{A}/\mathfrak{a}$ la proyección canónica; se verifica lo siguiente:

(i) $\pi(\mathbf{S})$ es un sistema multiplicativo de $\mathbf{A}/\mathfrak{a}$.

(ii) Existe un isomorfismo de anillos $\mathbf{S}^{-1}\mathbf{A}/\mathbf{S}^{-1}\mathfrak{a} \cong \pi(\mathbf{S})^{-1}(\mathbf{A}/\mathfrak{a})$.

Demostración (i):

Se define la imagen directa de $\mathbf{S}$ en $\mathbf{A}/\mathfrak{a}$. La cual se denota por:

$$\overline{\mathbf{S}} = \pi(\mathbf{S}) = \{x + \mathfrak{a} \in \mathbf{A}/\mathfrak{a} \;\mid\; x \in \mathbf{S}\}.$$

Se verifica que $\overline{\mathbf{S}}$ satisface las condiciones de la definición 1.5.1.

(1) $1 + \mathfrak{a} \in \overline{\mathbf{S}}$.

$\mathbf{A}/\mathfrak{a}$ es un anillo con unidad $\Rightarrow 1 + \mathfrak{a} \in \mathbf{A}/\mathfrak{a}$

$\Rightarrow \exists\; 1 \in \mathbf{A}$ t. q. $1 \in \mathbf{S}$ y $1 + \mathfrak{a} = \pi(1)$

$\Rightarrow 1 + \mathfrak{a} \in \overline{\mathbf{S}}$.

$$\therefore\; 1 + \mathfrak{a} \in \overline{\mathbf{S}}.$$

(2) Sea $x + \mathfrak{a},\; y + \mathfrak{a} \in \overline{\mathbf{S}}$.

$$x+\mathfrak{a},\ \ y+\mathfrak{a}\in\overline{\mathbf{S}}\ \ \Rightarrow\ \ \exists\ \ x,y\in\mathbf{S}\ \ \text{t. q.}\ \ x+\mathfrak{a}=\pi(x)\ \ \text{y}\ \ y+\mathfrak{a}=\pi(y)$$

$$\Rightarrow\ \ \pi(x)\pi(y)=(x+\mathfrak{a})(y+\mathfrak{a})$$

$$\Rightarrow\ \ \pi(xy)=(x+\mathfrak{a})(y+\mathfrak{a}),\ \ \text{donde}\ \ xy\in\mathbf{S}$$

$$\Rightarrow\ \ (x+\mathfrak{a})(y+\mathfrak{a})\in\overline{\mathbf{S}}.$$

$$\therefore\ \ (x+\mathfrak{a})(y+\mathfrak{a})\in\overline{\mathbf{S}}.$$

Luego $\overline{\mathbf{S}}$ es un sistema multiplicativo en $\mathbf{A}/\mathfrak{a}$. Además $\mathfrak{a}\notin\overline{\mathbf{S}}$ pues en caso contrario si $\mathfrak{a}\in\overline{\mathbf{S}}$, entonces existe $y\in\mathbf{S}$ tal que $\mathfrak{a}=y+\mathfrak{a}$ de donde $y\in\mathfrak{a}$, por tanto $y\in\mathfrak{a}\cap\mathbf{S}=\varnothing$ $(\rightarrow\leftarrow)$.

Demostración (ii):

Ahora se demuestra, que existe un isomorfismo de anillos $\mathbf{S}^{-1}\mathbf{A}/\mathbf{S}^{-1}\mathfrak{a}\cong\overline{\mathbf{S}}^{-1}(\mathbf{A}/\mathfrak{a})$.

Se tienen los siguientes homomorfismos,

$$\mathbf{A}\xrightarrow{\ \pi\ }\mathbf{A}/\mathfrak{a}\xrightarrow{\ \psi^*\ }\overline{\mathbf{S}}^{-1}(\mathbf{A}/\mathfrak{a}).$$

Donde $\psi^*:\ \mathbf{A}/\mathfrak{a}\longrightarrow\overline{\mathbf{S}}^{-1}(\mathbf{A}/\mathfrak{a})$ el correspondiente homomorfismo de localización de $\mathbf{A}/\mathfrak{a}$ en $\overline{\mathbf{S}}^{-1}(\mathbf{A}/\mathfrak{a})$. Considere el homomorfismo g definido como sigue:

$$
\begin{aligned}
g = \psi^* \circ \pi : \mathbf{A} &\longrightarrow \overline{\mathbf{S}}^{-1}\left(\mathbf{A}/\mathfrak{a}\right) \\
x \quad &\to \quad g(x) = \psi^*\left(\pi(x)\right) = \frac{\pi(x)}{1+\mathfrak{a}} = \frac{x+\mathfrak{a}}{1+\mathfrak{a}}.
\end{aligned}
$$

Se demuestra que para todo s en $\mathbf{S}$, $g(s)$ es una unidad en $\overline{\mathbf{S}}^{-1}\left(\mathbf{A}/\mathfrak{a}\right)$.

Sea $s \in \mathbf{S}$.

$$s \in \mathbf{S} \quad \Rightarrow \quad g(s) = \frac{\pi(s)}{1+\mathfrak{a}} \quad \text{y} \quad \frac{1+\mathfrak{a}}{\pi(s)} \in \overline{\mathbf{S}}^{-1}\left(\mathbf{A}/\mathfrak{a}\right)$$

$$\Rightarrow \quad g(s)\left(\frac{1+\mathfrak{a}}{\pi(s)}\right) = \left(\frac{\pi(s)}{1+\mathfrak{a}}\right)\left(\frac{1+\mathfrak{a}}{\pi(s)}\right) = \frac{\pi(s)}{\pi(s)} = \frac{1+\mathfrak{a}}{1+\mathfrak{a}}$$

$$\Rightarrow \quad g(s) \;\text{ es unidad en }\; \overline{\mathbf{S}}^{-1}\left(\mathbf{A}/\mathfrak{a}\right) \quad \forall s \in \mathbf{S}.$$

Luego por la propiedad universal de la proposición 1.5.7, existe un único homomorfismo de anillos $g' : \mathbf{S}^{-1}\mathbf{A} \to \overline{\mathbf{S}}^{-1}\left(\mathbf{A}/\mathfrak{a}\right)$ tal que $g' \circ \psi = g = \psi^* \circ \pi$.

Gráficamente:

$$
\begin{tikzcd}
\mathbf{A} \arrow[rr, "\psi"] \arrow[dr, "\psi^* \circ \pi = g"'] & & \mathbf{S}^{-1}\mathbf{A} \arrow[dl, "g'"] \\
& \overline{\mathbf{S}}^{-1}\left(\mathbf{A}/\mathfrak{a}\right) &
\end{tikzcd}
\qquad g' \circ \psi = g.
$$

Se define el homomorfismo g' como:

$$g' : \mathbf{S}^{-1}\,\mathbf{A} \longrightarrow \overline{\mathbf{S}}^{-1}\left(\mathbf{A}/\mathfrak{a}\right)$$

$$\frac{a}{s} \quad \rightarrow \quad g'\left(\frac{a}{s}\right) = g(a)\left[g(s)\right]^{-1} = \left(\frac{\pi(a)}{1+\mathfrak{a}}\right)\left[\frac{\pi(s)}{1+\mathfrak{a}}\right]^{-1} = \frac{\pi(a)}{\pi(s)} = \frac{a+\mathfrak{a}}{s+\mathfrak{a}}.$$

Ahora se verifica que $g' : \mathbf{S}^{-1}\,\mathbf{A} \longrightarrow \overline{\mathbf{S}}^{-1}\left(\mathbf{A}/\mathfrak{a}\right)$ satisface lo siguiente:

(1) $\quad \mathbf{ker}\left(g'\right) = \mathbf{S}^{-1}\,\mathfrak{a}$.

(2) $\quad g'$ es sobreyectiva.

Demostración (1):

$$\mathbf{ker}\left(g'\right) = \left\{\frac{a}{s} \in \mathbf{S}^{-1}\,\mathbf{A} \;\middle|\; g'\left(\frac{a}{s}\right) = \frac{\mathfrak{a}}{1+\mathfrak{a}}\right\}$$

$$= \left\{\frac{a}{s} \in \mathbf{S}^{-1}\,\mathbf{A} \;\middle|\; \frac{a+\mathfrak{a}}{s+\mathfrak{a}} = \frac{\mathfrak{a}}{1+\mathfrak{a}}\right\}$$

$$= \left\{\frac{a}{s} \in \mathbf{S}^{-1}\,\mathbf{A} \;\middle|\; \exists \;\; t+\mathfrak{a} \in \overline{\mathbf{S}} \;\text{ t. q. }\; (a+\mathfrak{a})(t+\mathfrak{a}) = \mathfrak{a}\right\}$$

$$= \left\{\frac{a}{s} \in \mathbf{S}^{-1}\,\mathbf{A} \;\middle|\; at+\mathfrak{a} = \mathfrak{a}\right\}$$

$$= \left\{\frac{a}{s} \in \mathbf{S}^{-1}\,\mathbf{A} \;\middle|\; at \in \mathfrak{a} \;\text{ y }\; st \in \mathbf{S}\right\}$$

$$= \left\{\frac{a}{s} \in \mathbf{S}^{-1}\,\mathbf{A} \;\middle|\; \frac{at}{st} \in \mathbf{S}^{-1}\,\mathfrak{a}\right\}$$

$$= \left\{ \frac{a}{s} \in \mathbf{S}^{-1}\,\mathbf{A} \;\mid\; \frac{a}{s} = \left(\frac{a}{s}\right)\left(\frac{t}{t}\right) \in \mathbf{S}^{-1}\,\mathfrak{a} \right\}$$

$$= \mathbf{S}^{-1}\,\mathfrak{a}.$$

Demostración (2):

Sea $\dfrac{x+\mathfrak{a}}{s+\mathfrak{a}} \in \overline{\mathbf{S}}^{-1}\left(\mathbf{A}/\mathfrak{a}\right)$.

$$\frac{x+\mathfrak{a}}{s+\mathfrak{a}} \in \overline{\mathbf{S}}^{-1}\left(\mathbf{A}/\mathfrak{a}\right) \;\Rightarrow\; x+\mathfrak{a} \in \mathbf{A}/\mathfrak{a} \;\text{ y }\; s+\mathfrak{a} \in \overline{\mathbf{S}}$$

$$\Rightarrow\; \exists\; x, s \in \mathbf{A},\; \text{con }\; s \in \mathbf{S} \;\text{ t. q. }\; x+\mathfrak{a} = \pi(x) \;\text{ y }\; s+\mathfrak{a} = \pi(s)$$

$$\Rightarrow\; \frac{x+\mathfrak{a}}{s+\mathfrak{a}} = \frac{\pi(x)}{\pi(s)} = g'\left(\frac{x}{s}\right)$$

$$\Rightarrow\; \frac{x+\mathfrak{a}}{s+\mathfrak{a}} \in \mathbf{Im}(g')$$

$\Rightarrow\; g'$ es sobreyectiva.

Como consecuencia de la proposición 1.1.13, existe un isomorfismo de anillos:

$$\mathbf{S}^{-1}\mathbf{A}/\mathbf{S}^{-1}\,\mathfrak{a} \cong \mathbf{Im}(g') \cong \overline{\mathbf{S}}^{-1}\left(\mathbf{A}/\mathfrak{a}\right). \;\blacksquare$$

Una demostración alternativa, para verificar que la aplicación τ definida en la demostración de la proposición 1.7.4 es cerrada, utilizando la demostración anterior está dada a continuación.

Sea $\mathfrak{a}$ un ideal primo en $\mathbf{A}$ tal que $\mathfrak{a} \cap \mathbf{S} = \varnothing$. Por el inciso (i) de la proposición 1.2.3, si $\mathfrak{a}$ es un ideal primo en $\mathbf{A}$, entonces $\mathbf{A}/\mathfrak{a}$ es un dominio de integridad. Considere $\overline{\mathbf{S}}$ como la imagen directa de $\mathbf{S}$ en $\mathbf{A}/\mathfrak{a}$ vía la proyección canónica por la proposición anterior se tiene

$$\mathbf{S}^{-1}\,\mathbf{A}\big/\mathbf{S}^{-1}\,\mathfrak{a} \cong \overline{\mathbf{S}}^{-1}\left(\mathbf{A}/\mathfrak{a}\right) \neq \{\mathbf{0}\}.$$

Se demuestra que;

$$\mathbf{S}^{-1}\left(\mathbf{A}/\mathfrak{a}\right) \cong \overline{\mathbf{S}}^{-1}\left(\mathbf{A}/\mathfrak{a}\right).$$

Se define una aplicación h como:

$$\begin{array}{rcl} h:\mathbf{S}^{-1}\left(\mathbf{A}/\mathfrak{a}\right) & \longrightarrow & \overline{\mathbf{S}}^{-1}\left(\mathbf{A}/\mathfrak{a}\right) \\ \dfrac{a+\mathfrak{a}}{s} & \to & h\left(\dfrac{a+\mathfrak{a}}{s}\right) = \dfrac{a+\mathfrak{a}}{s+\mathfrak{a}}. \end{array}$$

Se demuestra que la aplicación $h:\mathbf{S}^{-1}\left(\mathbf{A}/\mathfrak{a}\right) \longrightarrow \overline{\mathbf{S}}^{-1}\left(\mathbf{A}/\mathfrak{a}\right)$ satisface:

(1) La aplicación h está bien definida.

(2) La aplicación h es inyectiva.

(3) La aplicación h es sobreyectiva.

Demostración (1):

Sea $\dfrac{a_1+\mathfrak{a}}{s_1}, \dfrac{a_2+\mathfrak{a}}{s_2} \in \mathbf{S}^{-1}(\mathbf{A}/\mathfrak{a})$ t. q. $\dfrac{a_1+\mathfrak{a}}{s_1} = \dfrac{a_2+\mathfrak{a}}{s_2}$.

$$\frac{a_1+\mathfrak{a}}{s_1} = \frac{a_2+\mathfrak{a}}{s_2} \iff \exists\ s_3 \in \mathbf{S} \text{ t. q. } s_3\left\{(a_1+\mathfrak{a})s_2 - (a_2+\mathfrak{a})s_1\right\} = \mathfrak{a}$$

$$\iff s_3\left\{(a_1s_2+\mathfrak{a}) - (s_1a_2+\mathfrak{a})\right\} = \mathfrak{a}$$

$$\iff s_3\left\{(a_1s_2 - s_1a_2) + \mathfrak{a}\right\} = \mathfrak{a}$$

$$\iff s_3(a_1s_2 - s_1a_2) + \mathfrak{a} = \mathfrak{a}$$

$$\iff (s_3+\mathfrak{a})\left\{(s_2a_1 - s_1a_2) + \mathfrak{a}\right\} = \mathfrak{a}, \quad \text{donde} \quad s_3+\mathfrak{a} \in \overline{\mathbf{S}}$$

$$\iff (s_3+\mathfrak{a})\left\{(a_1+\mathfrak{a})(s_2+\mathfrak{a}) - (a_2+\mathfrak{a})(s_1+\mathfrak{a})\right\} = \mathfrak{a}$$

$$\iff \frac{a_1+\mathfrak{a}}{s_1+\mathfrak{a}} = \frac{a_2+\mathfrak{a}}{s_2+\mathfrak{a}}$$

$$\iff h\left(\frac{a_1+\mathfrak{a}}{s_1}\right) = h\left(\frac{a_2+\mathfrak{a}}{s_2}\right).$$

De donde h está bien definida y es inyectiva. Y por su definición h es sobreyectiva. Entonces;

$$\mathbf{S}^{-1}\left(\mathbf{A}/\mathfrak{a}\right) \cong \overline{\mathbf{S}}^{-1}\left(\mathbf{A}/\mathfrak{a}\right) \cong \mathbf{S}^{-1}\mathbf{A}\big/\mathbf{S}^{-1}\mathfrak{a}.$$

Denote por $\mathbf{k}_{\mathbf{A}/\mathfrak{a}}$ al cuerpo de fracciones del dominio $\mathbf{A}/\mathfrak{a}$. Se considera la aplicación $\xi : \mathbf{A}/\mathfrak{a} \to \mathbf{k}_{\mathbf{A}/\mathfrak{a}}$. Para todo $\overline{s} = s + \mathfrak{a} \in \mathbf{S}^*$, donde $\mathbf{S}^* = \left(\mathbf{A}/\mathfrak{a}\right) - \left\{\mathfrak{a}\right\}$, $\xi\left(\overline{s}\right)$ es una unidad en $\mathbf{k}_{\mathbf{A}/\mathfrak{a}}$. Luego por la **propiedad universal del anillo de fracciones**, existe un homomorfismo $\eta : \overline{\mathbf{S}}^{-1}\left(\mathbf{A}/\mathfrak{a}\right) \to \mathbf{k}_{\mathbf{A}/\mathfrak{a}}$ inyectivo.

Observe el siguiente diagrama:

$$\begin{tikzcd}
\mathbf{A}/\mathfrak{a} \arrow[rr, "\psi^*"] \arrow[dr, "\xi"'] & & \overline{\mathbf{S}}^{-1}\left(\mathbf{A}/\mathfrak{a}\right) \cong \mathbf{S}^{-1}\mathbf{A}\big/\mathbf{S}^{-1}\mathfrak{a} \arrow[dl, "\eta"] \\
& \mathbf{k}_{\mathbf{A}/\mathfrak{a}} &
\end{tikzcd}$$

Luego $\mathbf{S}^{-1}\mathbf{A}\big/\mathbf{S}^{-1}\mathfrak{a}$ está contenido en el cuerpo de fracciones $\mathbf{k}_{\mathbf{A}/\mathfrak{a}}$; por tanto $\mathbf{S}^{-1}\mathbf{A}\big/\mathbf{S}^{-1}\mathfrak{a}$ es un dominio de integridad y por la proposición 1.2.3, inciso (i); $\mathbf{S}^{-1}\mathfrak{a}$ es un ideal primo en $\mathbf{S}^{-1}\mathbf{A}$. ■

CAPITULO II: IDEALES EN ANILLOS DE EXTENSION Y DESCOMPOSICION.

En este capítulo se estudia uno de los elementos importantes del álgebra conmutativa; la descomposición de ideales, (es decir, ideales que se pueden escribir como una intersección finita de ciertos ideales; los ideales **primarios**). Se definen los elementos enteros y las extensiones de anillos, estando especialmente interesados en aquellos anillos $\mathbf{B}$ tal que todos sus elementos son enteros sobre un subanillo $\mathbf{A}$, de $\mathbf{B}$. Luego se examinan algunos resultados fundamentales que relacionan cadenas de ideales primos en anillos de extensión (**los teoremas del Ascenso y del Descenso de Cohen-Seidenberg**).

Sección 1: Descomposición primaria de ideales.

2.1: Ideales primarios.

En seguida se definen los ideales primarios y se estudia la relación entre los ideales primarios del anillo $\mathbf{A}$ y primarios de $\mathbf{S}^{-1}\mathbf{A}$.

Definición 2.1.1: Un ideal $\mathfrak{q} \neq (1)$ en un anillo $\mathbf{A}$, es **primario** si para $a, b \in \mathbf{A}$;

$$ab \in \mathfrak{q} \text{ y } \left(a \notin \mathfrak{q} \text{ ó } b \notin \mathfrak{q} \right) \Rightarrow \left(b^n \in \mathfrak{q} \text{ ó } a^n \in \mathfrak{q} \right) \text{ para algún } n \in \mathbb{N}.$$

Proposición 2.1.2: Sea $\mathbf{A}$ un anillo y $\mathfrak{q}$ un ideal propio de $\mathbf{A}$. Son equivalentes los siguientes enunciados:

(i) $\mathfrak{q}$ es un ideal primario.

(ii) Cada divisor de cero de $\mathbf{A}/\mathfrak{q}$ es un elemento nilpotente.

Demostración:

$(i) \Rightarrow (ii)$.

Sea $x+\mathfrak{q} \in \mathbf{A}/\mathfrak{q}$ un divisor de cero.

$x+\mathfrak{q}$ divide a cero $\Rightarrow \exists\, y+\mathfrak{q} \in \mathbf{A}/\mathfrak{q}$, $y+\mathfrak{q} \neq \mathfrak{q}$ t. q. $(y+\mathfrak{q})(x+\mathfrak{q}) = \mathfrak{q}$

$\Rightarrow \mathfrak{q} = (y+\mathfrak{q})(x+\mathfrak{q}) = yx+\mathfrak{q}$

$\Rightarrow yx \in \mathfrak{q}$

$\Rightarrow x^n \in \mathfrak{q}$, para algún $n \in \mathbb{N}$, ($y \notin \mathfrak{q}$ y $\mathfrak{q}$ es primario)

$\Rightarrow x^n + \mathfrak{q} = \mathfrak{q}$

$\Rightarrow (x+\mathfrak{q})^n = \mathfrak{q}$

$\Rightarrow x+\mathfrak{q}$ es nilpotente.

$\therefore$ Todo divisor de cero en $\mathbf{A}/\mathfrak{q}$ es nilpotente.

$(ii) \Rightarrow (i)$.

Sea $x, y \in \mathbf{A}$ tal que $xy \in \mathfrak{q}$. Se supone que $y \notin \mathfrak{q}$. Si $y \notin \mathfrak{q}$, entonces $y + \mathfrak{q} \neq \mathfrak{q}$.

$$xy \in \mathfrak{q} \Rightarrow xy + \mathfrak{q} = \mathfrak{q}$$

$$\Rightarrow (x+\mathfrak{q})(y+\mathfrak{q}) = \mathfrak{q}$$

$\Rightarrow$ $x + \mathfrak{q}$ es divisor de cero en $\mathbf{A}/\mathfrak{q}$

$\Rightarrow$ $x + \mathfrak{q}$ es un elemento nilpotente, (Hipotesis)

$\Rightarrow$ $\exists\ n \in \mathbb{N}$ t. q. $(x+\mathfrak{q})^n = \mathfrak{q}$

$$\Rightarrow x^n + \mathfrak{q} = \mathfrak{q}$$

$$\Rightarrow x^n \in \mathfrak{q}.$$

$\therefore$ $\mathfrak{q}$ es primario.

Proposición 2.1.3: Se verifica lo siguiente:

(i) Sea $\mathbf{A}$ un anillo y $\mathfrak{p}$ un ideal primo, entonces $\mathfrak{p}$ es un ideal primario.

(ii) Sea $f : \mathbf{A} \to \mathbf{B}$ un homomorfismo de anillos, la contracción de un ideal primario es primario.

Demostración (i):

Sea $x, y \in \mathbf{A}$ t. q. $xy \in \mathfrak{p}$. Se supone que $x \notin \mathfrak{p}$.

$$xy \in \mathfrak{p} \Rightarrow x \in \mathfrak{p} \text{ ó } y \in \mathfrak{p}$$

$$\Rightarrow y \in \mathfrak{p} = r(\mathfrak{p})$$

$$\Rightarrow \exists \ n \in \mathbb{N} \text{ t. q. } y^n \in \mathfrak{p}.$$

$\therefore$ Si $\mathfrak{p}$ es un ideal primo, entonces $\mathfrak{p}$ es un ideal primario.

Demostración (ii):

Sea $\mathfrak{q}$ un ideal primario en $\mathbf{B}$. Se prueba que $\mathfrak{q}^c$ un ideal primario en $\mathbf{A}$.

Sea $x, y \in \mathbf{A}$ t. q. $xy \in \mathfrak{q}^c$.

$$xy \in \mathfrak{q}^c \Rightarrow f(xy) \in \mathfrak{q}$$

$$\Rightarrow f(x)f(y) \in \mathfrak{q}$$

$$\Rightarrow f(x) \in \mathfrak{q} \text{ ó } (f(y))^n \in \mathfrak{q} \text{ para algún } n \in \mathbb{N}$$

$$\Rightarrow f(x) \in \mathfrak{q} \text{ ó } f(y^n) \in \mathfrak{q} \text{ para algún } n \in \mathbb{N}$$

$$\Rightarrow x \in \mathfrak{q}^c \text{ ó } y^n \in \mathfrak{q}^c \text{ para algún } n \in \mathbb{N}.$$

$\therefore$ La contracción de un ideal primario es primaria. ■

Proposición 2.1.4: Sea $\mathfrak{q}$ un ideal primario en un anillo $\mathbf{A}$, se verifica que:

(i) $r(\mathfrak{q})$ es un ideal primo.

(ii) $r(\mathfrak{q})$ es el menor ideal primo que contiene a $\mathfrak{q}$.

Demostración (i):

Sean $x, y \in \mathbf{A}$, t. q. $x\,y \in r(\mathfrak{q})$.

$$xy \in r(\mathfrak{q}) \Rightarrow \exists \ n \in \mathbb{N} \text{ t. q. } (xy)^n \in \mathfrak{q}$$

$$\Rightarrow x^n y^n \in \mathfrak{q}$$

$$\Rightarrow \exists \ k \in \mathbb{N} \text{ t. q. } x^n \in \mathfrak{q} \text{ ó } (y^n)^k \in \mathfrak{q}$$

$$\Rightarrow x \in r(\mathfrak{q}) \text{ ó } y^n \in r(\mathfrak{q})$$

$$\Rightarrow x \in r(\mathfrak{q}) \text{ ó } y \in r(r(\mathfrak{q}))$$

$$\Rightarrow x \in r(\mathfrak{q}) \text{ ó } y \in r(\mathfrak{q}).$$

Lo que demuestra que $r(\mathfrak{q})$ es un ideal primo.

$\therefore$ Si $\mathfrak{q}$ es primario, entonces $r(\mathfrak{q})$ es primo.

Demostración (ii):

Ahora se demuestra que $r(\mathfrak{q})$ es el menor ideal primo que contiene a $\mathfrak{q}$. Sea $\mathfrak{p}$ un ideal primo en $\mathbf{A}$ tal que $\mathfrak{q} \subseteq \mathfrak{p}$. Se quiere ver que $r(\mathfrak{q}) \subseteq \mathfrak{p}$.

Sea $x \in r(\mathfrak{q})$.

$$x \in r(\mathfrak{q}) \Rightarrow \exists\ n \in \mathbb{N} \quad \text{t. q.} \quad x^n \in \mathfrak{q}$$

$$\Rightarrow x^n \in \mathfrak{p}, \quad (\mathfrak{q} \subseteq \mathfrak{p})$$

$$\Rightarrow x \in r(\mathfrak{p})$$

$$\Rightarrow x \in \mathfrak{p}, \quad (\text{Proposición 1.2.15 (v)}).$$

Así $r(\mathfrak{q}) \subseteq \mathfrak{p}$, y por la proposición 1.2.15 (i), si $\mathfrak{q} \subseteq r(\mathfrak{q})$, entonces $\mathfrak{q} \subseteq r(\mathfrak{q}) \subseteq \mathfrak{p}$.

$\therefore\ r(\mathfrak{q})$ es el menor ideal primo que contiene a $\mathfrak{q}$. ■

En vista de la proposición anterior se da la siguiente definición.

Definición 2.1.5: Sea $\mathfrak{q}$ un ideal primario en un anillo $\mathbf{A}$. Se dice que $\mathfrak{q}$ es un ideal primario correspondiente al ideal primo $\mathfrak{p}$ ó que $\mathfrak{q}$ es $\mathfrak{p}-$primario, si $r(\mathfrak{q}) = \mathfrak{p}$.

En general, determinar si un ideal es primario es difícil, pero el siguiente caso particular nos será de mucha utilidad.

Proposición 2.1.6: Sea $\mathbf{A}$ un anillo y $\mathfrak{q}$ un ideal propio. Si $r(\mathfrak{q})$ es un ideal maximal, entonces $\mathfrak{q}$ es un ideal primario.

Demostración:

Sean $x, y \in \mathbf{A}$ t. q. $xy \in \mathfrak{q}$. Se supone que $y^m \notin \mathfrak{q} \quad \forall\ m \in \mathbb{N}$.

$$y^m \notin \mathfrak{q} \quad \forall\ m \in \mathbb{N} \quad \Rightarrow\ y \notin r(\mathfrak{q}) \ \text{ y } \ r(\mathfrak{q}) \subseteq r(\mathfrak{q}) + (y)$$

$$\Rightarrow\ r(\mathfrak{q}) + (y) = (1) \quad \text{ó} \quad r(\mathfrak{q}) + (y) = r(\mathfrak{q}),\ \left(r(\mathfrak{q}) \text{ ideal max}\right).$$

Suponga $r(\mathfrak{q}) + (y) = r(\mathfrak{q})$.

$$r(\mathfrak{q}) + (y) = r(\mathfrak{q}) \quad \Rightarrow \quad (y) \subseteq r(\mathfrak{q})$$

$$\Rightarrow\ y \in r(\mathfrak{q}),\ (\rightarrow\leftarrow). \qquad\qquad \therefore\ r(\mathfrak{q}) + (y) = (1).$$

$$r(\mathfrak{q}) + (y) = (1) \quad \Rightarrow \quad \exists\ \ s \in r(\mathfrak{q}) \ \text{ y } \ t \in \mathbf{A} \ \text{ t. q. } \ s + yt = 1$$

$$\Rightarrow\ \exists\ m \in \mathbb{N} \ \text{ t. q. } \ s^m \in \mathfrak{q}.$$

Elevando $s + yt = 1$ a la m y por el teorema del binomio se obtiene:

$$1 = (s + yt)^m = s^m + ms^{m-1}yt + \cdot \cdot \cdot + (yt)^m.$$

Multiplicando por x a ambos lados,

$$x = x\left(s^m\right) + x\left(ms^{m-1}yt\right) + \ \cdot \ \cdot \ \cdot \ + x\left(yt\right)^m.$$

Asociando xy se tiene,

$$x = x\left(s^m\right) + \left(xy\right)\left(ms^{m-1}t\right) + \ \cdot \ \cdot \ \cdot \ + \left(xy\right)\left(y^{m-1}t^m\right).$$

Donde todos los sumandos de la derecha están en $\mathfrak{q}$, por tanto $x \in \mathfrak{q}$.

$\therefore$ $\mathfrak{q}$ es un ideal primario.■

Corolario 2.1.7: Sea $\mathbf{A}$ un anillo.

(i) Las potencias de un ideal maximal $\mathfrak{m}$ en un anillo $\mathbf{A}$ son $\mathfrak{m}-$primarios.

(ii) Si $\mathfrak{m}^n \subseteq \mathfrak{q} \subseteq \mathfrak{m}$ para algún $n \in \mathbb{N}$, entonces $\mathfrak{q}$ es un ideal $\mathfrak{m}$-primario.

Demostración (i):

Sea $\mathfrak{a} = \mathfrak{m}^n$, donde $n \in \mathbb{N}$, la potencia de un ideal maximal $\mathfrak{m}$. Se demuestra que $\mathfrak{a}$ es un ideal $\mathfrak{m}-$primario, es decir, $r\left(\mathfrak{a}\right) = \mathfrak{m}$.

$\mathfrak{a} = \mathfrak{m}^n \ \Rightarrow \ r\left(\mathfrak{a}\right) = r\left(\mathfrak{m}^n\right)$, $\quad$ (Proposición 1.2.15 (ii))

$\Rightarrow \ r\left(\mathfrak{a}\right) = \mathfrak{m}$, $\quad$ (Proposición 1.2.15 (v))

$\Rightarrow$ $\mathfrak{a}$ es $\mathfrak{m}$-primario. $\quad$ $\therefore$ $\mathfrak{a}$ es un ideal $\mathfrak{m}-$primario.

Demostración (ii):

$$\mathfrak{m}^n \subseteq \mathfrak{q} \subseteq \mathfrak{m} \;\Rightarrow\; r\left(\mathfrak{m}^n\right) \subseteq r(\mathfrak{q}) \subseteq r(\mathfrak{m}), \qquad (\text{ Proposición 1.2.15 (ii) })$$

$$\Rightarrow\; \mathfrak{m} \subseteq r(\mathfrak{q}) \subseteq \mathfrak{m}, \quad (\text{Proposición 1.2.15. } (v))$$

$$\Rightarrow\; r(\mathfrak{q}) = \mathfrak{m}.$$

Luego $\mathfrak{q}$ es un ideal $\mathfrak{m}$-primario por la definición 2.1.5.■

Lema 2.1.8: Sea $\mathbf{A}$ un anillo y $\{\mathfrak{q}_\alpha \mid \alpha \in \Lambda\}$ una familia de ideales $\mathfrak{p}-$primario, entonces $\bigcap\limits_{\alpha \in \Lambda} \mathfrak{q}_\alpha$ es un ideal $\mathfrak{p}-$primario.

Demostración:

Sea $\mathfrak{q} = \bigcap\limits_{\alpha \in \Lambda} \mathfrak{q}_\alpha$.

Se demuestra lo siguiente:

(1) $r(\mathfrak{q}) = \mathfrak{p}$.

(2) $\mathfrak{q}$ es primario.

(1) $\mathfrak{q}_\alpha$ son $\mathfrak{p}-$primario $\forall \alpha \in \Lambda \;\Rightarrow\; r(\mathfrak{q}_\alpha) = \mathfrak{p} \;\; \forall \alpha \in \Lambda.$

$$\mathfrak{q}=\bigcap_{\alpha\in\Lambda}\mathfrak{q}_{\alpha} \Rightarrow r(\mathfrak{q})=r\left(\bigcap_{\alpha\in\Lambda}\mathfrak{q}_{\alpha}\right), \quad \text{(Proposición 1.2.15 (ii))}$$

$$=\bigcap_{\alpha\in\Lambda} r(\mathfrak{q}_{\alpha})$$

$$=\bigcap_{\alpha\in\Lambda}\mathfrak{p}$$

$$=\mathfrak{p}. \qquad \therefore\ r(\mathfrak{q})=\mathfrak{p}.$$

(2) Sea $x, y\in\mathbf{A}$, tal que $xy\in\mathfrak{q}$. Suponiendo que $x\notin\mathfrak{q}$.

$$xy\in\mathfrak{q} \ \text{ y } \ x\notin\mathfrak{q} \Rightarrow xy\in\mathfrak{q}_{\beta} \ \text{ y } \ x\notin\mathfrak{q}_{\beta} \ \text{ para algún } \beta\in\Lambda$$

$$\Rightarrow \exists\ n\in\mathbb{N} \ \text{ t. q. } \ y^{n}\in\mathfrak{q}_{\beta}$$

$$\Rightarrow y\in r(\mathfrak{q}_{\beta})=\mathfrak{p}$$

$$\Rightarrow y\in\mathfrak{p}=r(\mathfrak{q}), \quad (\text{por lo demostrado en } (1))$$

$$\Rightarrow y\in r(\mathfrak{q})$$

$$\Rightarrow y^{m}\in\mathfrak{q} \ \text{ para algún } m\in\mathbb{N}.$$

Luego $\mathfrak{q}$ es un ideal primario.

$\therefore$ La intersección de ideales $\mathfrak{p}-$primarios es $\mathfrak{p}-$primaria. ■

Lema 2.1.9: Sea $\mathfrak{q}$ un ideal $\mathfrak{p}$-primario, x un elemento de $\mathbf{A}$. Entonces se verifica lo siguiente:

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

(ii) Si $x \notin \mathfrak{q}$, entonces $(\mathfrak{q} : x)$ es $\mathfrak{p}-$primario.

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

Demostración (i):

Se quiere probar: Si $x \in \mathfrak{q}$, entonces $(\mathfrak{q} : x) = (1)$.

$x \in \mathfrak{q} \quad \Rightarrow \quad xy \in \mathfrak{q} \qquad \forall \quad y \in (1) = \mathbf{A}$

$\Rightarrow \quad y \in (\mathfrak{q} : x) \qquad \forall \quad y \in \mathbf{A}$

$\Rightarrow \quad (1) \subseteq (\mathfrak{q} : x) \subseteq (1)$

$\Rightarrow \quad (\mathfrak{q} : x) = (1)$. $\qquad \therefore$ Si $x \in \mathfrak{q}$, entonces $(\mathfrak{q} : x) = (1)$.

Demostración (ii):

Para el inciso (ii) se prueba que si $x \notin \mathfrak{q}$, entonces $(\mathfrak{q} : x)$ es $\mathfrak{p}-$primario, para ello se ve las partes siguientes:

(1) $(\mathfrak{q} : x)$ es primario.

(2) $r((\mathfrak{q} : x)) = \mathfrak{p}$.

(1) Sea $m, n \in \mathbf{A}$ tal que $mn \in (\mathfrak{q} : x)$. Se supone que $n \notin (\mathfrak{q} : x)$.

$$\begin{aligned} mn \in (\mathfrak{q} : x) \ \text{ y } \ n \notin (\mathfrak{q} : x) &\Rightarrow (mn)x \in \mathfrak{q} \ \text{ y } \ nx \notin \mathfrak{q} \\ &\Rightarrow m(nx) \in \mathfrak{q} \\ &\Rightarrow nx \in \mathfrak{q} \ \text{ ó } \ m^k \in \mathfrak{q} \ \text{ para algún } k \in \mathbb{N}. \\ &\Rightarrow m^k \in \mathfrak{q} \ \text{ para algún } k \in \mathbb{N}. \\ &\Rightarrow xm^k \in \mathfrak{q}, \qquad (\ \forall\, x \in \mathbf{A} \text{ en particular para } x \notin \mathfrak{q}\ ) \\ &\Rightarrow m^k \in (\mathfrak{q} : x) \ \text{ para algún } k \in \mathbb{N}. \end{aligned}$$

Luego $(\mathfrak{q} : x)$ es ideal primario.

(2) Para la segunda parte, se comprueba la igualdad siguiente:

$$\begin{aligned} r((\mathfrak{q} : x)) &= \left\{ y \in \mathbf{A} \mid y^n \in (\mathfrak{q} : x), \text{ para algún } n \in \mathbb{N} \right\} \\ &= \left\{ y \in \mathbf{A} \mid y^n x \in \mathfrak{q}, \text{ para algún } n \in \mathbb{N} \right\} \\ &= \left\{ y \in \mathbf{A} \mid \left(y^n\right)^k \in \mathfrak{q}, \text{ para algunos } n, k \in \mathbb{N} \right\} \\ &= \left\{ y \in \mathbf{A} \mid y^n \in r(\mathfrak{q}), \text{ para algún } n \in \mathbb{N} \right\} \end{aligned}$$

$$= \left\{ y \in \mathbf{A} \mid y \in r\left(r(\mathfrak{q})\right) \right\}$$

$$= \left\{ y \in \mathbf{A} \mid y \in r(\mathfrak{q}) \right\}$$

$$= r(\mathfrak{q})$$

$$= \mathfrak{p}.$$

Luego $r\left((\mathfrak{q} : x)\right) = \mathfrak{p}$, entonces $(\mathfrak{q} : x)$ es $\mathfrak{p}$-primario.

$\therefore$ Si $x \notin \mathfrak{q}$, entonces $(\mathfrak{q} : x)$ es $\mathfrak{p}-$primario. ■

Demostración (iii):

Se demuestra que si $x \notin \mathfrak{p}$, entonces $(\mathfrak{q} : x) = \mathfrak{q}$.

$$\begin{aligned}
(\mathfrak{q} : x) &= \left\{ y \in \mathbf{A} \mid yx \in \mathfrak{q} \right\} \\
&= \left\{ y \in \mathbf{A} \mid y \in \mathfrak{q} \quad \text{ó} \quad x^n \in \mathfrak{q}, \text{ para algún } n \in \mathbb{N} \right\} \\
&= \left\{ y \in \mathbf{A} \mid y \in \mathfrak{q} \quad \text{ó} \quad x \in r(\mathfrak{q}) \right\} \\
&= \left\{ y \in \mathbf{A} \mid y \in \mathfrak{q} \quad \text{ó} \quad x \in \mathfrak{p} \right\} \\
&= \mathfrak{q}.
\end{aligned}$$

$\therefore$ Si $x \notin \mathfrak{p}$, entonces $(\mathfrak{q} : x) = \mathfrak{q}$. ■

A continuación se investiga el comportamiento de los ideales primarios respecto al proceso de localización.

Proposición 2.1.10: Sea $\mathbf{A}$ un anillo y $\mathbf{S}$ un sistema multiplicativo de $\mathbf{A}$. Si $\mathfrak{q}$ es un ideal $\mathfrak{p}-$primario de $\mathbf{A}$ se verifica:

(i) Si $\mathbf{S}\cap\mathfrak{p}\neq\varnothing$, entonces $\mathbf{S}^{-1}\mathfrak{q}=\mathbf{S}^{-1}\mathbf{A}$.

(ii) Si $\mathbf{S}\cap\mathfrak{p}=\varnothing$, entonces $\mathbf{S}^{-1}\mathfrak{q}$ es $\mathbf{S}^{-1}\mathfrak{p}-$primario y $\left(\mathbf{S}^{-1}\mathfrak{q}\right)^{c}=\mathfrak{q}$.

Demostración (i): Se supone que $\mathbf{S}\cap\mathfrak{p}\neq\varnothing$.

$$\mathbf{S}\cap\mathfrak{p}\neq\varnothing \;\Rightarrow\; \exists\;\; x\in\mathbf{S}\cap\mathfrak{p}$$

$$\Rightarrow\; x\in\mathbf{S}\;\text{ y }\; x\in\mathfrak{p}=r(\mathfrak{q})$$

$$\Rightarrow\; \exists\;\; n\in\mathbb{N}\quad \text{t. q.}\quad x^{n}\in\mathbf{S}\quad\text{y}\quad x^{n}\in\mathfrak{q}$$

$$\Rightarrow\; x^{n}\in\mathbf{S}\cap\mathfrak{q}$$

$$\Rightarrow\; \mathfrak{q}\cap\mathbf{S}\neq\varnothing$$

$$\Rightarrow\; \mathbf{S}^{-1}\mathfrak{q}=(1_{\mathbf{S}^{-1}\mathbf{A}})=\mathbf{S}^{-1}\mathbf{A},\qquad \big(\text{ Proposición 1.7.3 (ii)}\big).$$

$$\therefore\; \text{Si }\; \mathbf{S}\cap\mathfrak{p}\neq\varnothing,\; \text{entonces }\; \mathbf{S}^{-1}\mathfrak{q}=\mathbf{S}^{-1}\mathbf{A}.$$

Demostración (ii):

Demostrar que $\mathbf{S}^{-1}\mathfrak{q}$ es $\mathbf{S}^{-1}\mathfrak{p}-$primario, significa verificar lo siguiente:

(1) $\mathbf{S}^{-1}\mathfrak{q}$ es primario.

(2) $r\left(\mathbf{S}^{-1}\mathfrak{q}\right)=\mathbf{S}^{-1}\mathfrak{p}$.

(1) Sea $\dfrac{x}{s}, \dfrac{y}{t} \in \mathbf{S}^{-1}\mathbf{A}$ tal que $\dfrac{x}{s}\dfrac{y}{t} \in \mathbf{S}^{-1}\mathfrak{q}$.

$$\frac{x}{s}\frac{y}{t} \in \mathbf{S}^{-1}\mathfrak{q} \quad \Rightarrow \frac{xy}{st} \in \mathbf{S}^{-1}\mathfrak{q}$$

$$\Rightarrow xy \in \mathfrak{q} \text{ y } st \in \mathbf{S}$$

$$\Rightarrow x \in \mathfrak{q} \text{ ó } y^n \in \mathfrak{q} \text{ para algún } n \in \mathbb{N}$$

$$\Rightarrow x \in \mathfrak{q} \text{ ó } y \in r(\mathfrak{q})$$

$$\Rightarrow \frac{x}{s} \in \mathbf{S}^{-1}\mathfrak{q} \text{ ó } \frac{y}{t} \in \mathbf{S}^{-1}\left(r(\mathfrak{q})\right)=r\left(\mathbf{S}^{-1}\mathfrak{q}\right), \text{ (Prop. 1.7.6 (iv))}$$

$$\Rightarrow \frac{x}{s} \in \mathbf{S}^{-1}\mathfrak{q} \text{ ó } \left(\frac{y}{t}\right)^k \in \mathbf{S}^{-1}\mathfrak{q}, \text{ para algún } k \in \mathbb{N}.$$

$\therefore$ $\mathbf{S}^{-1}\mathfrak{q}$ es un ideal primario.

(2) En consecuencia de la proposición 1.7.6, inciso (iv),

$$r\left(\mathbf{S}^{-1}\mathfrak{q}\right)=\mathbf{S}^{-1}\left(r\left(\mathfrak{q}\right)\right)=\mathbf{S}^{-1}\mathfrak{p}.$$

$$\therefore\ \mathbf{S}^{-1}\mathfrak{q} \text{ es un ideal } \mathbf{S}^{-1}\mathfrak{p}-\text{primario.}$$

Ahora se ve la segunda parte de (ii); es decir, probar que $\left(\mathbf{S}^{-1}\mathfrak{q}\right)^c=\mathfrak{q}.$

Por la proposición 1.3.2, inciso (iii);

$$\mathfrak{q}\subseteq\mathfrak{q}^{ec}=\left(\mathfrak{q}^e\right)^c=\left(\mathbf{S}^{-1}\mathfrak{q}\right)^c \quad\Rightarrow\quad \mathfrak{q}\subseteq\left(\mathbf{S}^{-1}\mathfrak{q}\right)^c.$$

$$\therefore\ \mathfrak{q}\subseteq\left(\mathbf{S}^{-1}\mathfrak{q}\right)^c.$$

Sea $x\in\left(\mathbf{S}^{-1}\mathfrak{q}\right)^c=\mathfrak{q}^{ec}$.

$$x\in\left(\mathbf{S}^{-1}\mathfrak{q}\right)^c \ \Rightarrow\ x\in\mathfrak{q}^{ec}=\bigcup_{s\in\mathbf{S}}\left(\mathfrak{q}:s\right), \quad \left(\text{Proposición 1.7.3 (i)}\right)$$

$$\Rightarrow\ x\in\left(\mathfrak{q}:s\right) \text{ para algún } s\in\mathbf{S}$$

$$\Rightarrow\ xs\in\mathfrak{q}$$

$$\Rightarrow\ x\in\mathfrak{q} \text{ ó } s^n\in\mathfrak{q} \text{ para algún } n\in\mathbb{N}$$

$$\Rightarrow\ x\in\mathfrak{q}\ \text{ ó }\ s\in r(\mathfrak{q})=\mathfrak{p}$$

$$\Rightarrow\ x\in\mathfrak{q},\quad (\mathbf{S}\cap\mathfrak{p}=\varnothing).$$

$$\therefore\ \left(\mathbf{S}^{-1}\mathfrak{q}\right)^{c}\subseteq\mathfrak{q}.$$

Luego $\mathfrak{q}\subseteq\left(\mathbf{S}^{-1}\mathfrak{q}\right)^{c}$ y $\left(\mathbf{S}^{-1}\mathfrak{q}\right)^{c}\subseteq\mathfrak{q}$, entonces $\left(\mathbf{S}^{-1}\mathfrak{q}\right)^{c}=\mathfrak{q}$. ■

Observación: De acuerdo con inciso (ii), de la proposición 2.1.10 se tiene:

1. Existe una correspondencia biyectiva entre los ideales $\mathbf{S}^{-1}\mathfrak{p}$ – primarios de $\mathbf{S}^{-1}\mathbf{A}$ y los ideales $\mathfrak{p}$ – primarios de $\mathbf{A}$, donde $\mathfrak{p}$ no cortan a $\mathbf{S}$.

2. En particular, si $\mathbf{S}=\mathbf{A}-\mathfrak{p}$, entonces $\left(\mathbf{S}^{-1}\mathfrak{q}\right)^{c}=\mathfrak{q}$. Por tanto para que dos ideales $\mathfrak{p}$ – primarios coincidan es suficiente que coincidan al localizar en $\mathfrak{p}$.

Nota: Para cada ideal $\mathfrak{a}$ y todo sistema multiplicativo $\mathbf{S}$ de $\mathbf{A}$, la contracción en $\mathbf{A}$ del ideal $\mathbf{S}^{-1}\mathfrak{a}$ se indica por $\mathbf{S}(\mathfrak{a})=\left(\mathbf{S}^{-1}\mathfrak{a}\right)^{c}$.

2.2: Teoremas de unicidad.

A continuación se examinan presentaciones de un ideal como una intersección finita de ideales primarios, la cual no es necesariamente única.

Definición 2.2.1: Si $\mathfrak{a}$ es un ideal propio de $\mathbf{A}$, una **descomposición primaria** de $\mathfrak{a}$ es una expresión de la forma:

$$\mathfrak{a}=\bigcap_{i=1}^{n}\mathfrak{q}_i,$$

con $\mathfrak{q}_i$ ideales primarios, $\forall\ i=1\ ,\ .\ .\ .\ ,\ n.$

Definición 2.2.2: Una descomposición primaria. Se llama **minimal** si se verifican las condiciones siguientes:

(i) $r\left(\mathfrak{q}_i\right)\neq r\left(\mathfrak{q}_j\right)\ \ \left(1\leq i,\ j\leq n\right),$ para $i\neq j.$

(ii) $\bigcap_{j\neq i}\mathfrak{q}_j\not\subseteq\mathfrak{q}_i$ para $\left(1\leq i,\ j\leq n\right).$

Definición 2.2.3: Un ideal se llama **descomponible** si tiene una descomposición primaria.

En general una descomposición primaria tal, puede no existir; en esta sección sólo se tendrá en cuenta ideales que tienen una descomposición primaria.

Si un ideal en un anillo puede descomponerse como intersección finita de ideales primarios, se puede obtener una descomposición primaria que satisfaga la propiedad (ii) de la definición 2.2.2, simplemente eliminando las componentes redundantes $\mathfrak{q}_i$ si los hubiera. En consecuencia del lema 2.1.8, para satisfacer la condición (i) de la definición 2.2.2 de una descomposición minimal, cuando hay varios ideales $\mathfrak{p}-$primario, se toma la intersección de todos ellos y se obtiene un nuevo ideal $\mathfrak{p}-$primario, así se obtiene una descomposición primaria en la que todos los ideales tienen radicales diferentes. **Véase la siguiente proposición**.

Teorema 2.2.4: Sea $\mathfrak{a}$ un ideal en un anillo $\mathbf{A}$. Si $\mathfrak{a}$ es descomponible, entonces $\mathfrak{a}$ tiene una descomposición primaria minimal.

Demostración:

Sea $\mathfrak{a}$ un ideal descomponible en un anillo $\mathbf{A}$ y $\mathfrak{a}=\bigcap_{j=1}^{n}\mathfrak{q}_j$ una descomposición primaria (donde cada $\mathfrak{q}_j$ es primario). Se verifica las siguientes condiciones:

(1) $\bigcap_{j\neq i}\mathfrak{q}_j \not\subseteq \mathfrak{q}_i$ para $(1\leq i,\ j\leq h\leq n)$.

(2) $r(\mathfrak{q}_i)\neq r(\mathfrak{q}_j)$ $(1\leq i,\ j\leq h\leq n)$, para $i\neq j$.

Demostración (1):

Suponga que existe $\mathfrak{q}_i$ $(1\leq i\leq n)$ tal que $\bigcap_{\substack{j=1\\ j\neq i}}^{n}\mathfrak{q}_j\subseteq\mathfrak{q}_i$. Entonces $\mathfrak{a}=\bigcap_{\substack{j=1\\ j\neq i}}^{n}\mathfrak{q}_j$ es también una descomposición primaria. Reordenando los índices,

$$\mathfrak{a}=\bigcap_{j=1}^{s}\mathfrak{q}_j,\quad \text{donde } (s\leq n).$$

De nuevo suponga que existe $\mathfrak{q}_t\left(1 \le t \le s\right)$ tal que $\bigcap_{j=1}^{s}\mathfrak{q}_j \subseteq \mathfrak{q}_t$. Entonces $\mathfrak{a} = \bigcap_{\substack{j=1 \\ j\neq t}}^{s}\mathfrak{q}_j$ es también una descomposición primaria. Reescribiendo los índices se tiene:

$$\mathfrak{a} = \bigcap_{j=1}^{r}\mathfrak{q}_j, \quad \text{donde } \left(r \le s \le n\right).$$

Sucesivamente eliminando todas las componentes $\mathfrak{q}_i$ que resulten redundantes (y cambiando los índices) se tiene que $\mathfrak{a} = \bigcap_{j=1}^{k}\mathfrak{q}_j$, donde $\left(k \le r \le s \le n\right)$ y ningún $\mathfrak{q}_i$ contiene la intersección de los otros $\mathfrak{q}_j$ con $j \neq i$.

Luego se ha obtenido una descomposición primaria que satisface la condición (ii) de la definición 2.2.2.

Demostración (2):

Sea $\left\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\right\}$ los ideales primos distintos en el conjunto $\left\{r\left(\mathfrak{q}_1\right), \ldots, r\left(\mathfrak{q}_k\right)\right\}$, donde $\left(r \le k\right)$. Haciendo, $\mathfrak{q}'_i = \bigcap_{1\le j\le k}\left\{\mathfrak{q}_j \mid r\left(\mathfrak{q}_j\right) = \mathfrak{p}_i, \text{ donde } 1 \le i \le r\right\}$.

Del lema 2.1.8 cada $\mathfrak{q}'_i$ es $\mathfrak{p}_i -$primario. Se supone que existe $\mathfrak{q}'_i$ $\left(1 \le i \le r\right)$ tal que $\bigcap_{\substack{j=1 \\ j\neq i}}^{r}\mathfrak{q}'_j \subseteq \mathfrak{q}'_i$, entonces

$$\mathfrak{q}'_i \supseteq \bigcap_{\substack{j=1\\ j\neq i}}^{r} \mathfrak{q}'_j = \mathfrak{q}'_1 \cap \mathfrak{q}'_2 \cap \ \cdot \ \cdot \ \cdot \cap \mathfrak{q}'_{i-1} \cap \mathfrak{q}'_{i+1} \cap \ \cdot \ \cdot \ \cdot \cap \mathfrak{q}'_r$$

$$= \left[\bigcap_{1\leq j\leq k} \left\{ \mathfrak{q}_j \ \mid \ r\left(\mathfrak{q}_j\right) = \mathfrak{p}_1 \right\} \right] \cap \left[\bigcap_{1\leq j\leq k} \left\{ \mathfrak{q}_j \ \mid \ r\left(\mathfrak{q}_j\right) = \mathfrak{p}_2 \right\} \right] \cap \cdot \ \cdot \ \cdot$$

$$\cdot \ \cdot \ \cdot \cap \left[\bigcap_{1\leq j\leq k} \left\{ \mathfrak{q}_j \ \mid \ r\left(\mathfrak{q}_j\right) = \mathfrak{p}_{i-1} \right\} \right] \cap \left[\bigcap_{1\leq j\leq k} \left\{ \mathfrak{q}_j \ \mid \ r\left(\mathfrak{q}_j\right) = \mathfrak{p}_{i+1} \right\} \right] \cap \cdot \ \cdot \ \cdot$$

$$\cdot \ \cdot \ \cdot \ \cap \left[\bigcap_{1\leq j\leq k} \left\{ \mathfrak{q}_j \ \mid \ r\left(\mathfrak{q}_j\right) = \mathfrak{p}_r \right\} \right]$$

$$= \bigcap_{j=1}^{k} \left\{ \mathfrak{q}_j \ \mid \ r\left(\mathfrak{q}_j\right) \neq \mathfrak{p}_i \right\}.$$

Por la definición de $\mathfrak{q}'_i$ existe $\mathfrak{q}_t$ para $1 \leq t \leq k$ tal que $r\left(\mathfrak{q}_t\right) = \mathfrak{p}_i$, entonces,

$$\mathfrak{q}_t \supseteq \mathfrak{q}'_i \supseteq \bigcap_{\substack{j=1\\ j\neq i}}^{r} \mathfrak{q}'_j = \bigcap_{j=1}^{k} \left\{ \mathfrak{q}_j \ \mid \ r\left(\mathfrak{q}_j\right) \neq \mathfrak{p}_i \right\} \supseteq \bigcap_{\substack{j=1\\ j\neq t}}^{k} \mathfrak{q}_j.$$

De donde por transitividad,

$$\mathfrak{q}_t \supseteq \bigcap_{\substack{j=1\\ j\neq t}}^{k} \mathfrak{q}_j.$$

Que es una contradicción por lo hecho en (1). Luego;

$$\mathfrak{a}=\bigcap_{i=1}^{k}\mathfrak{q}_i=\mathfrak{q}_1\cap\mathfrak{q}_2\cap\ \cdot\ \cdot\ \cdot\cap\mathfrak{q}_k$$

$$=\left[\bigcap_{j=1}^{k}\left\{\mathfrak{q}_j\ \mid\ r\left(\mathfrak{q}_j\right)=\mathfrak{p}_1\right\}\right]\cap\left[\bigcap_{j=1}^{k}\left\{\mathfrak{q}_j\ \mid\ r\left(\mathfrak{q}_j\right)=\mathfrak{p}_2\right\}\right]\cap\cdot\ \cdot\ \cdot$$

$$\cdot\ \cdot\ \cdot\cap\left[\bigcap_{j=1}^{k}\left\{\mathfrak{q}_j\ \mid\ r\left(\mathfrak{q}_j\right)=\mathfrak{p}_{r-1}\right\}\right]\cap\left[\bigcap_{j=1}^{k}\left\{\mathfrak{q}_j\ \mid\ r\left(\mathfrak{q}_j\right)=\mathfrak{p}_r\right\}\right]$$

$$=\mathfrak{q}_1'\cap\mathfrak{q}_2'\cap\ \cdot\ \cdot\ \cdot\cap\mathfrak{q}_{r-1}'\cap\mathfrak{q}_r'$$

$$=\bigcap_{i=1}^{r}\mathfrak{q}_i'.$$

Es una descomposición primaria que verifica las condiciones (i) y (ii) de la definición 2.2.2. Entonces toda descomposición primaria se puede llevar a una descomposición primaria minimal.

$\therefore$ Todo ideal descomponible admite una descomposición primaria minimal.■

Teorema 2.2.5: (1º Teorema de unicidad). Sea $\mathfrak{a}$ un ideal descomponible y sea $\mathfrak{a}=\bigcap_{i=1}^{n}\mathfrak{q}_i$ una descomposición primaria minimal de $\mathfrak{a}$. Sea $\mathfrak{p}_i=r\left(\mathfrak{q}_i\right)$ $\left(1\le i\le n\right)$. Entonces los $\mathfrak{p}_i$ son todos los ideales primos que se pueden escribir de la forma $r\left(\mathfrak{a}:x\right)$ para $x\in\mathbf{A}$. Como consecuencia son independientes de la descomposición primaria considerada.

Demostración:

Se demuestra que los ideales $\mathfrak{p}_i \ (1 \leq i \leq n)$, son exactamente los ideales primos que se pueden escribir en la forma $r(\mathfrak{a} : x)$, para algún $x \in \mathbf{A}$.

Sea $x \in \mathbf{A}$.

$$(\mathfrak{a} : x) = \left(\bigcap_{i=1}^{n} \mathfrak{q}_i : x \right)$$

$$= \bigcap_{i=1}^{n} (\mathfrak{q}_i : x), \qquad (\text{ Proposición } 1.1.11 \ (\text{ii}))$$

$$= \left\{ \bigcap_{\{j \mid x \in \mathfrak{q}_j\}} (\mathfrak{q}_j : x) \right\} \cap \left\{ \bigcap_{\{j \mid x \notin \mathfrak{q}_j\}} (\mathfrak{q}_j : x) \right\}$$

$$= \mathbf{(1)} \cap \left\{ \bigcap_{\{j \mid x \notin \mathfrak{q}_j\}} (\mathfrak{q}_j : x) \right\}, \qquad (\text{ Lema } 2.1.9 \ (\text{i}))$$

$$= \bigcap_{\{j \mid x \notin \mathfrak{q}_j\}} (\mathfrak{q}_j : x).$$

Tomando radicales de ambos lados,

$$r(\mathfrak{a} : x) = r\left(\bigcap_{\{j \mid x \notin \mathfrak{q}_j\}} (\mathfrak{q}_j : x) \right)$$

$$= \bigcap_{\{j \mid x \notin \mathfrak{q}_j\}} r(\mathfrak{q}_j : x), \qquad (\text{Proposición } 1.2.15 \ (\text{iii}))$$

$$= \bigcap_{\{j \mid x \notin \mathfrak{q}_j\}} \mathfrak{p}_j, \qquad (\text{Lema } 2.1.9 \ (\text{ii})).$$

Sea $\mathfrak{p}$ un ideal primo en $\mathbf{A}$ tal que $\mathfrak{p} = r(\mathfrak{a} : x)$, para algún $x \in \mathbf{A}$. Si $\mathfrak{p} = r(\mathfrak{a} : x)$, entonces $\mathfrak{p} = \bigcap_{\{j \mid x \notin \mathfrak{q}_j\}} \mathfrak{p}_j$, por el inciso (ii) de la proposición 1.2.9 se tiene que $\mathfrak{p} = \mathfrak{p}_j$ para algún j $(1 \le j \le n)$.

Recíprocamente, como la descomposición primaria es minimal, entonces para cualquier i $(1 \le i \le n)$, existe $x_i \in \bigcap_{j \ne i} \mathfrak{q}_j$ tal que $x_i \notin \mathfrak{q}_i$.

$$r(\mathfrak{a} : x_i) = r\left(\bigcap_{i=1}^{n} \mathfrak{q}_i : x_i\right)$$

$$= r\left(\bigcap_{j \ne i} \mathfrak{q}_j \cap \mathfrak{q}_i : x\right)$$

$$= r\left(\left(\bigcap_{j \ne i} \mathfrak{q}_j : x_i\right) \cap (\mathfrak{q}_i : x_i)\right)$$

$$= r\big((1) \cap (\mathfrak{q}_i : x_i)\big), \qquad (\text{ Lema } 2.1.9 \ (\text{i}) \ )$$

$= r\left(\left(\mathfrak{q}_i : x_i\right)\right)$

$= \mathfrak{p}_i, \quad$ (Lema 2.1.9 **(ii)**).

Así para cada índice i existe un elemento $x_i \in \mathbf{A}$ tal que $\mathfrak{p}_i = r\left(\mathfrak{a} : x_i\right)$ y $\left(\mathfrak{a} : x_i\right)$ es $\mathfrak{p}_i$ – primario. ■

Corolario 2.2.6: Sea $\mathfrak{a}$ un ideal descomponible y $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$ una descomposición primaria minimal de $\mathfrak{a}$. Si $\mathfrak{p}_i = r\left(\mathfrak{q}_i\right)$ $\left(1 \le i \le n\right)$, entonces los $\mathfrak{p}_i$ son precisamente los ideales primos asociados a $\mathbf{0}$ en $\mathbf{A}/\mathfrak{a}$.

Demostración:

Por el primer **teorema de unicidad,** $\mathfrak{p}$ es un ideal primo asociado a $\mathfrak{a}$ en $\mathbf{A}$, sí y sólo si existe $x \in \mathbf{A}$ tal que $\mathfrak{p} = r\left(\mathfrak{a} : x\right)$. Luego por la definición 1.1.10, observación (3):

$$\mathfrak{p} = r\left(\mathfrak{a} : x\right) = r\left(\operatorname{Ann}\left(\overline{x}\right)\right) = r\left(\mathbf{0} : \overline{x}\right).$$

Que es equivalente a decir que $\mathfrak{p}$ es un ideal primo asociado a $\mathbf{0}$ en $\mathbf{A}/\mathfrak{a}$. ■

Observación: En consecuencia del corolario anterior, el 1º **Teorema de unicidad** equivale a decir, que los $\mathfrak{p}_i$ son los ideales primos que se presentan como radicales de anuladores de elementos del cociente.

Definición 2.2.7: Sea $\mathfrak{a}$ un ideal y $\mathfrak{a}=\bigcap_{i=1}^{n}\mathfrak{q}_i$ una descomposición primaria minimal.

- Los ideales primos $\mathfrak{p}_i=r(\mathfrak{q}_i)$ $(1\le i\le n)$ se llaman primos **asociados** o **pertenecientes** a $\mathfrak{a}$.
- Los elementos minimales (**con respecto a la inclusión**) del conjunto $\{\mathfrak{p}_1,\ \mathfrak{p}_2,\ .\ .\ .\ ,\ \mathfrak{p}_n\}$ de primos asociados, se llaman primos **minimales** o **aislados**. Los demás se llaman primos **inmersos**.

Se usa la notación $\operatorname{Ass}(\mathfrak{a})$, para referirnos a los primos **asociados** ó **pertenecientes** a $\mathfrak{a}$ y $\operatorname{MinAss}(\mathfrak{a})$ para referirnos a los primos minimales **asociados** ó **pertenecientes** a $\mathfrak{a}$.

Las siguientes dos proposiciones dan aplicaciones de la descomposición primaria, para hallar los ideales primos minimales que contienen a un ideal descomponible, el conjunto de los divisores de cero y el de elementos nilpotentes de un anillo.

Proposición 2.2.8: Sea $\mathbf{A}$ un anillo y $\mathfrak{a}$ un ideal con una descomposición primaria minimal. Para cada ideal primo $\mathfrak{p}\supseteq\mathfrak{a}$, existe un ideal primo minimal $\mathfrak{q}$ asociado a $\mathfrak{a}$, tal que $\mathfrak{p}\supseteq\mathfrak{q}\supseteq\mathfrak{a}$. Además los ideales primos minimales sobre $\mathfrak{a}$ son exactamente los elementos minimales de $\operatorname{Ass}(\mathfrak{a})$.

Demostración:

Se demuestra lo siguiente:

(1) Para cada ideal primo $\mathfrak{p}$ con $\mathfrak{p} \supseteq \mathfrak{a}$, existe un ideal primo $\mathfrak{q} \in \text{MinAss}(\mathfrak{a})$ tal que $\mathfrak{p} \supseteq \mathfrak{q}$

(2) Los ideales primos minimales sobre $\mathfrak{a}$ son exactamente los elementos $\text{MinAss}(\mathfrak{a})$.

Demostración (1)**:**

Se tiene $\mathfrak{a}$ un ideal, con una descomposición primaria minimal y un ideal primo $\mathfrak{p}$ tal que $\mathfrak{p} \supseteq \mathfrak{a}$. De acuerdo con la proposición 1.2.17. Si $\mathfrak{p} \supseteq \mathfrak{a}$. entonces existe $\overline{\mathfrak{p}}$, un ideal primo minimal sobre $\mathfrak{a}$ tal que $\mathfrak{p} \supseteq \overline{\mathfrak{p}} \supseteq \mathfrak{a}$.

Rescribiendo todo esto, se obtiene,

$$\overline{\mathfrak{p}} \supseteq \mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i, \text{ donde } \mathfrak{q}_i \text{ es ideal } \mathfrak{p}_i - \text{primario } \forall i = 1, \ . \ . \ . \ , n.$$

Tomando radicales a la expresión anterior;

$$\overline{\mathfrak{p}} = r(\overline{\mathfrak{p}}) \supseteq r(\mathfrak{a}) = r\left(\bigcap_{i=1}^{n} \mathfrak{q}_i\right) = \bigcap_{i=1}^{n} r(\mathfrak{q}_i) = \bigcap_{i=1}^{n} \mathfrak{p}_i.$$

Por transitividad,

$$\overline{\mathfrak{p}} \supseteq \bigcap_{i=1}^{n} \mathfrak{p}_i.$$

Por tanto del inciso (ii) de la proposición 1.2.9,

$$\overline{\mathfrak{p}} \supseteq \mathfrak{p}_i \quad \text{para algún} \quad (1 \leq i \leq n).$$

De la minimalidad de $\overline{\mathfrak{p}}$ se tiene,

$$\overline{\mathfrak{p}} = \mathfrak{p}_i \quad \text{para algún} \quad (1 \leq i \leq n).$$

Luego $\mathfrak{p} \supseteq \mathfrak{p}_i$ es un ideal primo minimal perteneciente a $\mathfrak{a}$.

$$\therefore\ \mathfrak{p} \supseteq \mathfrak{a}, \text{ existe un ideal primo } \mathfrak{q} \in \text{MinAss}(\mathfrak{a}) \text{ tal que } \mathfrak{p} \supseteq \mathfrak{q}.$$

Demostración (2)**:**

En la segunda parte se demuestra que $\{\text{Ideales primos minimales sobre } \mathfrak{a}\} = \text{MinAss}(\mathfrak{a})$.

Sea $\mathfrak{p}$ un ideal primo minimal sobre $\mathfrak{a}$.

$$\begin{aligned} \mathfrak{p} \text{ es primo minimal sobre } \mathfrak{a} \quad &\Rightarrow \quad \mathfrak{p} \supseteq \mathfrak{a} \\ &\Rightarrow \quad \exists \ \mathfrak{p}_j \in \text{MinAss}(\mathfrak{a}) \text{ t. q. } \mathfrak{p} \supseteq \mathfrak{p}_j \supseteq \mathfrak{a}, \quad (\text{Parte (1)}) \\ &\Rightarrow \quad \mathfrak{p} = \mathfrak{p}_j, \quad (\text{Por la minimalidad de } \mathfrak{p}) \\ &\Rightarrow \quad \mathfrak{p} \in \text{MinAss}(\mathfrak{a}). \end{aligned}$$

$$\therefore\ \{ \text{ Ideales primos minimales sobre } \mathfrak{a} \ \} \subseteq \text{MinAss}(\mathfrak{a}).$$

Sea $\mathfrak{p}_j \in \mathrm{MinAss}(\mathfrak{a})$, se supone que $\mathfrak{p}_j \supseteq \mathfrak{p}$ tal que $\mathfrak{p}$ es un ideal primo $\mathfrak{p} \supseteq \mathfrak{a}$.

$\mathfrak{a} \subseteq \mathfrak{p} \;\Rightarrow\; \exists\; \mathfrak{p}_i \in \mathrm{MinAss}(\mathfrak{a})$ t. q. $\mathfrak{p}_i \subseteq \mathfrak{p}$, $\big(\text{Parte } (1)\big)$

$\Rightarrow \mathfrak{p}_i \subseteq \mathfrak{p} \subseteq \mathfrak{p}_j$

$\Rightarrow \mathfrak{p}_i \subseteq \mathfrak{p}_j$

$\Rightarrow \mathfrak{p}_i = \mathfrak{p}_j$, $\big(\text{Por la minimalidad de } \mathfrak{p}_j\big)$

$\Rightarrow \mathfrak{p}_j = \mathfrak{p}$

$\Rightarrow \mathfrak{p}_j \in \{$ Ideales primos minimales sobre $\mathfrak{a}\}$.

$\therefore$ $\mathrm{MinAss}(\mathbf{a}) \subseteq \{$ Ideales primos minimales sobre $\mathfrak{a}\}$.

Luego, $\mathrm{MinAss}(\mathfrak{a}) = \{$ Ideales primos minimales sobre $\mathfrak{a}\}$.■

Proposición 2.2.9: Sea $\mathbf{A}$ un anillo y $\mathbf{0} = \bigcap_{i=1}^{n} \mathfrak{q}_i$ una descomposición primaria minimal del ideal $\mathbf{0}$, si $r(\mathfrak{q}_i) = \mathfrak{p}_i$ $(1 \le i \le n)$, entonces:

$$\{\text{Divisores de cero en } \mathbf{A}\} = \bigcup_{i=1}^{n} \mathfrak{p}_i .$$

Demostración:

Se demuestra que el conjunto $\mathbf{D}$ de los divisores de cero de $\mathbf{A}$ es la unión de ideales primos asociados al ideal cero; es decir:

$$\mathbf{D}=\bigcup_{i=1}^{n}\mathfrak{p}_i, \quad \text{donde} \quad \mathfrak{p}_i = r(\mathfrak{q}_i) \ \ (1\le i\le n).$$

En consecuencia de la proposición 1.2.18,

$$\mathbf{D}=\bigcup_{x\neq 0} r(\operatorname{Ann}(x))=\bigcup_{x\neq 0} r(\mathbf{0}:x).$$

Sea $a\in\mathbf{D}$.

$$a\in\mathbf{D} \ \Rightarrow \ \exists \ b\in\mathbf{A},\ b\neq 0 \ \text{ t. q. } \ ab=0$$

$$\Rightarrow \ ab\in\bigcap_{i=1}^{n}\mathfrak{q}_i=\mathbf{0}$$

$$\Rightarrow \ ab\in\mathfrak{q}_i \quad \forall \ i=1,\ .\ .\ .\ ,\ n$$

$$\Rightarrow \ b\in\mathfrak{q}_i \quad \text{ó} \quad a^n\in\mathfrak{q}_i, \quad \text{para algún} \quad n\in\mathbb{N},\ \ \forall\ i=1,\ .\ .\ .\ ,\ n.$$

Se supone que $b\in\mathfrak{q}_i$.

$$b\in\mathfrak{q}_i \quad \forall \ i=1,\ .\ .\ .\ ,\ n \quad \Rightarrow \ b\in\bigcap_{i=1}^{n}\mathfrak{q}_i=\mathbf{0}$$

$$\Rightarrow \ b=0, \quad (\rightarrow\leftarrow)$$

$$\Rightarrow \ b\notin\mathfrak{q}_i \quad \text{para algún } (1\le i\le n).$$

De donde se concluye que $a^n \in \mathfrak{q}_i$, para algún $n \in \mathbb{N}$.

$$a^n \in \mathfrak{q}_i \quad \text{para algún } n \in \mathbb{N} \quad \Rightarrow \quad a \in r(\mathfrak{q}_i) = \mathfrak{p}_i$$

$$\Rightarrow \quad a \in \bigcup_{i=1}^{n} \mathfrak{p}_i.$$

$$\therefore \quad \mathbf{D} \subseteq \bigcup_{i=1}^{n} \mathfrak{p}_i.$$

Sea $a \in \bigcup_{i=1}^{n} \mathfrak{p}_i$.

$$a \in \bigcup_{i=1}^{n} \mathfrak{p}_i \quad \Rightarrow \quad a \in \mathfrak{p}_i = r(\mathfrak{q}_i), \quad \text{para algún } (1 \le i \le n)$$

$$\Rightarrow \quad \exists \; n \in \mathbb{N} \;\text{ t. q. }\; a^n \in \mathfrak{q}_i$$

$$\Rightarrow \quad a^n b \in \mathfrak{q}_i \quad \forall \quad b \neq 0 \in \bigcap_{j \neq i} \mathfrak{q}_i$$

$$\Rightarrow \quad a^n b \in \mathfrak{q}_i \quad \text{y} \quad a^n b \in \bigcap_{j \neq i} \mathfrak{q}_i$$

$$\Rightarrow \quad a^n b \in \bigcap_{i=1}^{n} \mathfrak{q}_i = \mathbf{0}$$

$$\Rightarrow \quad a^n \in (\mathbf{0} : b)$$

$$\Rightarrow \quad a \in r(\mathbf{0} : b) \subseteq \bigcup_{x \neq 0} r(\mathbf{0} : x) = \mathbf{D}. \qquad \therefore \; \bigcup_{i=1}^{n} \mathfrak{p}_i \subseteq \mathbf{D}.$$

Luego, $\mathbf{D}=\bigcup_{i=1}^{n}\mathfrak{p}_i$, ya que se han probado ambos contenidos.

$\therefore$ Si el cero es descomponible, entonces el conjunto de divisores de cero de $\mathbf{A}$ es la unión de ideales primos asociados al ideal $\mathbf{0}$. ■

Proposición 2.2.10: Sea $\mathbf{A}$ un anillo y $\mathfrak{a}=\bigcap_{i=1}^{n}\mathfrak{q}_i$ una descomposición primaria minimal. Sea $r(\mathfrak{q}_i)=\mathfrak{p}_i$ para cada índice $(1\le i\le n)$, entonces:

$$\bigcup_{i=1}^{n}\mathfrak{p}_i=\left\{\, x\in\mathbf{A} \;\mid\; (\mathfrak{a}:x)\neq\mathfrak{a} \,\right\}.$$

Demostración:

Se demuestra primero que si $\mathfrak{a}$ es descomponible en $\mathbf{A}$, entonces $\mathbf{0}$ es descomponible en $\mathbf{A}/\mathfrak{a}$.

Sea $\pi:\mathbf{A}\to\mathbf{A}/\mathfrak{a}$, $a\to\overline{a}$ la proyección canónica. Por definición; π es un homomorfismo sobreyectivo, de acuerdo con la proposición 1.3.5, $\pi(\mathfrak{q}_i)$ es un ideal en $\mathbf{A}/\mathfrak{a}$, para todo $i=1,\ldots,n$. Denote por $\pi(\mathfrak{q}_i)=\overline{\mathfrak{q}}_i$.

Se prueba que $\bigcap_{i=1}^{n}\overline{\mathfrak{q}}_i=\mathbf{0}$, donde $\overline{\mathfrak{q}}_i$ es la imagen de $\mathfrak{q}_i$ en $\mathbf{A}/\mathfrak{a}$, es una descomposición primaria del ideal $\mathbf{0}$ en $\mathbf{A}/\mathfrak{a}$.

Para ello se verifica:

(1) $\bigcap_{i=1}^{n} \overline{\mathfrak{q}}_i = \mathbf{0}.$

(2) $\overline{\mathfrak{q}}_i$ es primario $\forall\ i = 1, \ldots, n$.

Demostración (1):

$$\bigcap_{i=1}^{n} \overline{\mathfrak{q}}_i = \left\{ x + \mathfrak{a} \in \mathbf{A}/\mathfrak{a} \ \mid \ x + \mathfrak{a} \in \overline{\mathfrak{q}}_i \quad \forall\ i = 1, \ldots, n \right\}$$

$$= \left\{ x + \mathfrak{a} \in \mathbf{A}/\mathfrak{a} \ \mid \ x \in \mathfrak{q}_i \quad \forall\ i = 1, \ldots, n \right\}$$

$$= \left\{ x + \mathfrak{a} \in \mathbf{A}/\mathfrak{a} \ \mid \ x \in \bigcap_{i=1}^{n} \mathfrak{q}_i = \mathfrak{a} \right\}$$

$$= \left\{ x + \mathfrak{a} \in \mathbf{A}/\mathfrak{a} \ \mid \ x \in \mathfrak{a} \right\} = \mathbf{0}.$$

Demostración (2):

Sean $(x+\mathfrak{a}),\ (y+\mathfrak{a}) \in \mathbf{A}/\mathfrak{a}$ t. q. $(x+\mathfrak{a})(y+\mathfrak{a}) \in \overline{\mathfrak{q}}_i$.

$$(x+\mathfrak{a})(y+\mathfrak{a}) \in \overline{\mathfrak{q}}_i \ \Rightarrow \ xy + \mathfrak{a} \in \overline{\mathfrak{q}}_i$$

$$\Rightarrow \ xy \in \mathfrak{q}_i$$

$$\Rightarrow \;\; x \in \mathfrak{q}_i \;\; \text{ó} \;\; y^n \in \mathfrak{q}_i, \text{ para algún } n \in \mathbb{N}.$$

$$\Rightarrow \;\; x + \mathfrak{a} \in \overline{\mathfrak{q}}_i \;\; \text{ó} \;\; y^n + \mathfrak{a} \in \overline{\mathfrak{q}}_i, \text{ para algún } n \in \mathbb{N}.$$

$$\Rightarrow \;\; x + \mathfrak{a} \in \overline{\mathfrak{q}}_i \;\; \text{ó} \;\; (y + \mathfrak{a})^n \in \overline{\mathfrak{q}}_i, \text{ para algún } n \in \mathbb{N}.$$

Luego $\overline{\mathfrak{q}}_i$ es primario en $\mathbf{A}/\mathfrak{a}$ $\forall\, i = 1, \ldots, n$. Por tanto cada descomposición primaria de $\mathfrak{a} = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \cdots \cap \mathfrak{q}_n$ define una descomposición primaria $\mathbf{0} = \overline{\mathfrak{q}}_1 \cap \overline{\mathfrak{q}}_2 \cap \cdots \cap \overline{\mathfrak{q}}_n$ del ideal cero en el anillo $\mathbf{A}/\mathfrak{a}$.

Ahora pasando al cociente $\mathbf{A}/\mathfrak{a}$ se supone que $\mathfrak{a} = \mathbf{0}$. Observe el conjunto:

$$\{ x \in \mathbf{A} \mid (\mathfrak{a} : x) \neq \mathfrak{a} \} = \{ x \in \mathbf{A} \mid \exists\; r \in (\mathfrak{a} : x) \;\text{ t. q. }\; r \notin \mathfrak{a} \}$$

$$= \{ x \in \mathbf{A} \mid \exists\;\; rx \in \mathfrak{a} \;\text{ t. q. }\; r \notin \mathfrak{a} \}$$

$$= \{ x \in \mathbf{A} \mid \exists\;\; rx + \mathfrak{a} = \mathfrak{a} \;\text{ t. q. }\; r + \mathfrak{a} \neq \mathfrak{a} \}$$

$$= \{ x \in \mathbf{A} \mid \exists\;\; (x + \mathfrak{a})(r + \mathfrak{a}) = \mathfrak{a} \;\text{ t. q. }\; r + \mathfrak{a} \neq \mathfrak{a} \}$$

$$= \{ \text{Divisores de cero en } \mathbf{A}/\mathfrak{a} \}$$

$$= \bigcup_{i=1}^{n} \mathfrak{p}_i, \qquad (\text{Proposición 2.2.9, Corolario 2.2.6}).$$

De donde,

$$\bigcup_{i=1}^{n} \mathfrak{p}_i = \{\, x \in \mathbf{A} \;\mid\; (\mathfrak{a} : x) \neq \mathfrak{a} \,\}.$$

Observación: Si el ideal cero es descomponible en $\mathbf{A}$. Entonces:

- $\mathbf{D_A} = \{$ Divisores de cero de $\mathbf{A}\}$

  $= \bigcup \{\, \mathfrak{p} \mid \mathfrak{p}$ es un ideal pirmo asociado al ideal $\mathbf{0}\,\}$.

- $\mathbf{R_A} = \{$ Elementos nilpotentes de $\mathbf{A}\}$

  $= r(\mathbf{0})$, $\quad$ (Proposición 1.2.13 observación (1))

  $= \bigcap \{\, \mathfrak{p} \mid \mathfrak{p}$ es un ideal primo minimal sobre el ideal $\mathbf{0}\,\}$

  $= \bigcap \{\, \mathfrak{p} \mid \mathfrak{p}$ es un ideal primo minimal asociado a ideal $\mathbf{0}\,\}$.

Proposición 2.2.11: Sea $\mathbf{A}$ un anillo y $\mathfrak{a}$ un ideal en $\mathbf{A}$. Los siguientes enunciados son equivalentes:

(i) $\operatorname{Ass}(\mathfrak{a}) = \{\mathfrak{p}\}$.

(ii) $\mathfrak{a}$ es primario.

Demostración: $(\mathrm{i}) \Rightarrow (\mathrm{ii})$. $\left(\operatorname{Ass}(\mathfrak{a}) = \{\mathfrak{p}\}\right) \;\Rightarrow\; (\mathfrak{a}$ es primario$)$.

Pasando al anillo cociente, se supone que $\mathfrak{a}=\mathbf{0}$ y $\operatorname{Ass}(\mathbf{0})$ es el conjunto de primos asociados a $\mathbf{0}$ en $\mathbf{A}/\mathfrak{a}$. De la observación anterior se tiene:

- $\mathbf{D}_{\mathbf{A}/\mathfrak{a}} = \bigcup_{\mathfrak{p}\in\operatorname{Ass}(\mathbf{0})} \mathfrak{p} = \mathfrak{p}.$

- $\mathbf{R}_{\mathbf{A}/\mathfrak{a}} = \bigcap_{\mathfrak{p}\in\operatorname{Ass}(\mathbf{0})} \mathfrak{p} = \mathfrak{p}.$

Luego todo divisor de cero en $\mathbf{A}/\mathfrak{a}$ es un elemento nilpotente. De acuerdo con la proposición 2.1.2, $\mathfrak{a}$ es un ideal primario.

$(\text{ii})\Rightarrow(\text{i})$. $(\mathfrak{a}\text{ es primario}) \Rightarrow (\operatorname{Ass}(\mathfrak{a})=\{\mathfrak{p}\})$.

Sea $\operatorname{Ass}(\mathfrak{a})=\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$, el conjunto de primos asociados a $\mathfrak{a}$.

$(\mathfrak{a}\text{ es primario}) \Rightarrow$ (Cada divisor de cero en $\mathbf{A}/\mathfrak{a}$ es nilpotente), (proposicion 2.1.2)

$$\Rightarrow \mathbf{D}_{\mathbf{A}/\mathfrak{a}} = \mathbf{R}_{\mathbf{A}/\mathfrak{a}}$$

$$\Rightarrow \bigcup_{i=1}^{n}\mathfrak{p}_i = \bigcap_{i=1}^{n}\mathfrak{p}_i$$

$$\Rightarrow \mathfrak{p}_i = \mathfrak{p}_j, \text{ para } j=1, \ldots, n \text{ con } j\neq i$$

$$\Rightarrow \operatorname{Ass}(\mathfrak{a})=\{\mathfrak{p}_i\}.$$

Luego si $\mathfrak{a}$ es un ideal primario en $\mathbf{A}$, entonces $\operatorname{Ass}(\mathfrak{a}) = \{\mathfrak{p}_i\}$. ■

Proposición 2.2.12: Sea $\mathbf{A}$ un anillo, $\mathbf{S}$ un sistema multiplicativo de $\mathbf{A}$, $\mathfrak{a}$ un ideal de $\mathbf{A}$ con una descomposición primaria minimal $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$. Sea $r(\mathfrak{q}_i) = \mathfrak{p}_i$ $(1 \leq i \leq n)$. Se supone que $\mathfrak{p}_j \cap \mathbf{S} = \varnothing$ para $j = 1, \ . \ . \ . \ , m$ y $\mathfrak{p}_j \cap \mathbf{S} \neq \varnothing$ para $j = m+1, \ . \ . \ . \ , n$, entonces:

$$\mathbf{S}^{-1}\mathfrak{a} = \bigcap_{i=1}^{m} \mathbf{S}^{-1}\mathfrak{q}_i \qquad \text{y} \qquad \mathbf{S}(\mathfrak{a}) = \bigcap_{i=1}^{m} \mathfrak{q}_i$$

son descomposiciones primarias minimales.

Demostración:

$$\begin{aligned}
\mathbf{S}^{-1}\mathfrak{a} &= \mathbf{S}^{-1}\left(\bigcap_{i=1}^{n} \mathfrak{q}_i\right) = \bigcap_{i=1}^{n} \mathbf{S}^{-1}\mathfrak{q}_i \\
&= \left[\bigcap_{i=1}^{m} \mathbf{S}^{-1}\mathfrak{q}_i\right] \cap \left[\bigcap_{i=m+1}^{n} \mathbf{S}^{-1}\mathfrak{q}_i\right] \\
&= \left[\bigcap_{i=1}^{m} \mathbf{S}^{-1}\mathfrak{q}_i\right] \cap \mathbf{S}^{-1}\mathbf{A}, \qquad (\text{Proposición 2.1.10 (i)}) \\
&= \bigcap_{i=1}^{m} \mathbf{S}^{-1}\mathfrak{q}_i.
\end{aligned}$$

De donde $\mathbf{S}^{-1}\mathfrak{a}=\bigcap_{i=1}^{m}\mathbf{S}^{-1}\mathfrak{q}_i$ y por el inciso (ii) de la proposición 2.1.10, $\mathbf{S}^{-1}\mathfrak{q}_i$ es $\mathbf{S}^{-1}\mathfrak{q}_i-$primario $\forall\ i=1,\ .\ .\ .\ ,\ m.$

Haciendo la contracción de $\mathbf{S}^{-1}\mathfrak{a}$ y las proposiciones 1.3.4, (v) y 2.1.10 se tiene:

$$\mathbf{S}(\mathfrak{a})=\left(\mathbf{S}^{-1}\mathfrak{a}\right)^c=\left(\bigcap_{i=1}^{m}\mathbf{S}^{-1}\mathfrak{q}_i\right)^c$$

$$=\bigcap_{i=1}^{m}\left(\mathbf{S}^{-1}\mathfrak{q}_i\right)^c, \qquad \left(\text{Proposición 1.3.4 }(\text{v})\right)$$

$$=\bigcap_{i=1}^{m}\mathfrak{q}_i, \qquad \left(\text{Proposición 2.1.10 }(\text{ii})\right).$$

Así $\mathbf{S}(\mathfrak{a})=\bigcap_{i=1}^{m}\mathfrak{q}_i$, donde $\mathfrak{q}_i$ es $\mathfrak{p}_i-$primario $\forall\ i=1,\ .\ .\ .\ ,\ m.$ Ahora se demuestra que $\mathbf{S}^{-1}\mathfrak{a}=\bigcap_{i=1}^{m}\mathbf{S}^{-1}\mathfrak{q}_i$ y $\mathbf{S}(\mathfrak{a})=\bigcap_{i=1}^{m}\mathfrak{q}_i$ son descomposiciones primarias minimales. Para $\mathbf{S}^{-1}(\mathfrak{a})=\bigcap_{i=1}^{m}\mathbf{S}^{-1}\mathfrak{q}_i$ se verifica que:

(1) $\quad r\left(\mathbf{S}^{-1}\mathfrak{q}_i\right)\neq r\left(\mathbf{S}^{-1}\mathfrak{q}_j\right)$ para $i\neq j \quad \left(1\leq i,\ j\leq m\right)$.

(2) $\quad \bigcap_{\substack{j=1\\ j\neq i}}^{m}\mathbf{S}^{-1}\mathfrak{q}_j\not\subseteq\mathbf{S}^{-1}\mathfrak{q}_i$ para $\left(1\leq i,\ j\leq m\right)$.

Demostración (1)**:**

Se supone que $r\left(\mathbf{S}^{-1}\mathfrak{q}_i\right)=r\left(\mathbf{S}^{-1}\mathfrak{q}_j\right)$.

$$r\left(\mathbf{S}^{-1}\mathfrak{q}_i\right)=r\left(\mathbf{S}^{-1}\mathfrak{q}_j\right) \;\Rightarrow\; \mathbf{S}^{-1}\left(r\left(\mathfrak{q}_i\right)\right)=\mathbf{S}^{-1}\left(r\left(\mathfrak{q}_j\right)\right)$$

$$\Rightarrow\; \left[\mathbf{S}^{-1}\left(r\left(\mathfrak{q}_i\right)\right)\right]^c=\left[\mathbf{S}^{-1}\left(r\left(\mathfrak{q}_j\right)\right)\right]^c$$

$$\Rightarrow\; r\left(\mathfrak{q}_i\right)=r\left(\mathfrak{q}_j\right) \quad i\neq j,\ \left(\text{Proposición 2.1.10 (ii)}\right) \quad (\rightarrow\leftarrow).$$

$\therefore\ \left\{r\left(\mathbf{S}^{-1}\mathfrak{q}_1\right),\ .\ .\ .\ .\ ,\ r\left(\mathbf{S}^{-1}\mathfrak{q}_m\right)\right\}$ es un conjunto de ideales primos distintos en $\mathbf{S}^{-1}\mathbf{A}$.

Demostración (2)**:**

Se supone que $\bigcap_{\substack{j=1\\ j\neq i}}^{m}\mathbf{S}^{-1}\mathfrak{q}_j\subseteq\mathbf{S}^{-1}\mathfrak{q}_i$ para algún $(1\leq i\leq m)$.

$$\mathbf{S}^{-1}\mathfrak{q}_i\supseteq\bigcap_{\substack{j=1\\ j\neq i}}^{m}\mathbf{S}^{-1}\mathfrak{q}_j \;\Rightarrow\; \left(\mathbf{S}^{-1}\mathfrak{q}_i\right)^c\supseteq\left(\bigcap_{\substack{j=1\\ j\neq i}}^{m}\mathbf{S}^{-1}\mathfrak{q}_j\right)^c=\bigcap_{\substack{j=1\\ j\neq i}}^{m}\left(\mathbf{S}^{-1}\mathfrak{q}_j\right)^c, \quad \left(\text{Proposición 1.3.4 (v)}\right)$$

$$\Rightarrow\; \mathfrak{q}_i\supseteq\bigcap_{\substack{j=1\\ j\neq i}}^{m}\mathfrak{q}_j, \qquad \left(\text{Proposición 2.1.10 (ii)}\right)$$

$$\Rightarrow \ \mathfrak{q}_i \supseteq \bigcap_{\substack{j=1\\ j\neq i}}^{m} \mathfrak{q}_j \supseteq \bigcap_{\substack{j=1\\ j\neq i}}^{n} \mathfrak{q}_j$$

$$\Rightarrow \ \mathfrak{q}_i \supseteq \bigcap_{\substack{j=1\\ j\neq i}}^{n} \mathfrak{q}_j, \quad (\rightarrow\leftarrow).$$

$$\therefore \ \bigcap_{\substack{j=1\\ j\neq i}}^{m} \mathbf{S}^{-1}\mathfrak{q}_j \not\subseteq \mathbf{S}^{-1}\mathfrak{q}_i \quad (1 \leq i,\ j \leq m).$$

Para $\mathbf{S}(\mathfrak{a}) = \bigcap_{\substack{j=1\\ j\neq i}}^{m} \mathfrak{q}_i$ se verifica lo siguiente:

(1) $\quad r(\mathfrak{q}_i) \neq r(\mathfrak{q}_j)$ para $i \neq j (1 \leq i,\ j \leq m)$.

(2) $\quad \bigcap_{\substack{j=1\\ j\neq i}}^{m} \mathfrak{q}_j \not\subseteq \mathfrak{q}_i$ para $(1 \leq i,\ j \leq m)$.

Demostración (1)**:**

$r(\mathfrak{q}_i) \neq r(\mathfrak{q}_j)$ para $i \neq j (1 \leq i, j \leq m)$ pues $\bigcap_{j=1}^{n} \mathfrak{q}_j = \mathfrak{a}$ es una descomposición primaria minimal del ideal $\mathfrak{a}$.

$$\therefore \ \{\mathfrak{q}_1, \ldots, \mathfrak{q}_m\} \text{ es un conjunto de ideales primos distintos en } \mathbf{A}.$$

Demostración (2)**:**

Se supone que $\bigcap_{\substack{j=1 \\ j\neq i}}^{m} \mathfrak{q}_j \subseteq \mathfrak{q}_i$, para algún $(1 \leq i \leq m)$.

$$\bigcap_{\substack{j=1 \\ j\neq i}}^{m} \mathfrak{q}_j \subseteq \mathfrak{q}_i \;\Rightarrow\; \bigcap_{\substack{j=1 \\ j\neq i}}^{n} \mathfrak{q}_j \subseteq \bigcap_{\substack{j=1 \\ j\neq i}}^{m} \mathfrak{q}_j \subseteq \mathfrak{q}_i$$

$$\Rightarrow\; \bigcap_{\substack{j=1 \\ j\neq i}}^{n} \mathfrak{q}_j \subseteq \mathfrak{q}_i, \quad (\rightarrow\leftarrow).$$

$$\therefore\; \bigcap_{\substack{j=1 \\ j\neq i}}^{m} \mathfrak{q}_j \not\subseteq \mathfrak{q}_i.$$

Luego $\mathbf{S}^{-1}\mathfrak{a} = \bigcap_{i=1}^{m} \mathbf{S}^{-1}\mathfrak{q}_i$ y $\mathbf{S}(\mathfrak{a}) = \bigcap_{j=1}^{m} \mathbf{S}^{-1}\mathfrak{q}_i$, son descomposiciones primarias minimales.■

Definición 2.2.13: Un conjunto Σ de ideales primos pertenecientes a $\mathfrak{a}$ se dice que es **genéricamente estable,** si se satisface la siguiente condición:

- Si $\mathfrak{p}'$ es un ideal primo perteneciente a $\mathfrak{a}$ y $\mathfrak{p}' \subseteq \mathfrak{p}$ para algún $\mathfrak{p} \in \Sigma$, entonces $\mathfrak{p}' \in \Sigma$.

Observación:

Cualquier conjunto de primos minimales asociados a $\mathfrak{a}$, es un conjunto genéricamente estable.

Proposición 2.2.14: Sea $\mathfrak{a}$ un ideal de $\mathbf{A}$, Σ un conjunto genéricamente estable de ideales primos pertenecientes a $\mathfrak{a}$ y sea $\mathbf{S} = \mathbf{A} - \bigcup\limits_{\mathfrak{p}\in\Sigma} \mathfrak{p}$. Se verifica lo siguiente:

(i) $\mathbf{S}$ es un sistema multiplicativo de $\mathbf{A}$.

(ii) $\mathfrak{p}' \in \Sigma \;\Rightarrow\; \mathfrak{p}' \cap \mathbf{S} = \varnothing$.

(iii) $\mathfrak{p}' \notin \Sigma \;\Rightarrow\; \mathfrak{p}' \not\subseteq \bigcup\limits_{\mathfrak{p}\in\Sigma} \mathfrak{p} \;\Rightarrow\; \mathfrak{p}' \cap \mathbf{S} \neq \varnothing$.

Demostración (i):

Observe primero el siguiente conjunto:

$$\mathbf{A} - \mathbf{S} = \mathbf{A} - \left(\mathbf{A} - \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p} \right) = \mathbf{A} - \left(\mathbf{A} \cap \left(\bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p} \right)^{C} \right)$$

$$= \mathbf{A} \cap \left(\mathbf{A} \cap \left(\bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p} \right)^{C} \right)^{C}$$

$$= \mathbf{A} \cap \left(\mathbf{A}^{C} \cup \left(\bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p} \right) \right)$$

$$= \left(\mathbf{A} \cap \mathbf{A}^{C} \right) \cup \left(\mathbf{A} \cap \left(\bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p} \right) \right)$$

$$= \mathbf{A} \cap \left(\bigcup_{\mathfrak{p} \in \Sigma} \mathfrak{p} \right) = \bigcup_{\mathfrak{p} \in \Sigma} \mathfrak{p}.$$

$$= \bigcup_{\mathfrak{p} \in \Sigma} \mathfrak{p}.$$

Ahora se demuestra que $\mathbf{S}$ es un sistema multiplicativo de $\mathbf{A}$.

(1) $1 \in \mathbf{S}$. Se supone que $1 \notin \mathbf{S}$.

$$1 \notin \mathbf{S} \;\Rightarrow\; 1 \in \mathbf{A} - \mathbf{S} = \bigcup_{\mathfrak{p} \in \Sigma} \mathfrak{p} \;\Rightarrow\; 1 \in \mathfrak{p} \text{ para algún } \mathfrak{p} \in \Sigma, \quad (\rightarrow\leftarrow). \quad \therefore\; 1 \in \mathbf{S}.$$

(2) Sean $s, t \in \mathbf{S}$, se verifica que $s\,t \in \mathbf{S}$.

$$s,\ t \in \mathbf{S} \;\Rightarrow\; s, t \notin \mathbf{A} - \mathbf{S} = \bigcup_{\mathfrak{p} \in \Sigma} \mathfrak{p}$$

$$\Rightarrow\; s, t \notin \mathfrak{p} \quad \forall\ \mathfrak{p} \in \Sigma$$

$$\Rightarrow\; s\,t \notin \mathfrak{p} \quad \forall\ \mathfrak{p} \in \Sigma$$

$$\Rightarrow\; s\,t \notin \bigcup_{\mathfrak{p} \in \Sigma} \mathfrak{p} = \mathbf{A} - \mathbf{S}$$

$$\Rightarrow\; s\,t \in \mathbf{S}.$$

Luego si $s, t \in \mathbf{S}$, entonces $s\,t \in \mathbf{S}$. $\therefore$ $\mathbf{S}$ es un sistema multiplicativo de $\mathbf{A}$.

Demostración (ii):

Se quiere demostrar que $\mathfrak{p}' \in \Sigma \;\Rightarrow\; \mathfrak{p}' \cap \mathbf{S} = \varnothing$.

$$\mathfrak{p}' \in \Sigma \;\Rightarrow\; \mathfrak{p}' \subseteq \bigcup_{\mathfrak{p} \in \Sigma} \mathfrak{p}$$

$$\Rightarrow\; \mathbf{A} - \mathfrak{p}' \supseteq \mathbf{A} - \bigcup_{\mathfrak{p} \in \Sigma} \mathfrak{p} = \mathbf{S}, \qquad (\text{Tomando complementos})$$

$$\Rightarrow\; \mathbf{A} - \mathfrak{p}' \supseteq \mathbf{S}$$

$$\Rightarrow\; \mathfrak{p}' \cap (\mathbf{A} - \mathfrak{p}') \supseteq \mathfrak{p}' \cap \mathbf{S}$$

$$\Rightarrow\; \varnothing \supseteq \mathfrak{p}' \cap \mathbf{S} \supseteq \varnothing$$

$$\Rightarrow\; \mathfrak{p}' \cap \mathbf{S} = \varnothing.$$

$$\therefore\; \mathfrak{p}' \in \Sigma \;\Rightarrow\; \mathfrak{p}' \cap \mathbf{S} = \varnothing.$$

Demostración (iii):

(1) $\mathfrak{p}' \notin \Sigma \;\Rightarrow\; \mathfrak{p}' \not\subseteq \bigcup_{\mathfrak{p} \in \Sigma} \mathfrak{p}.$

(2) $\mathfrak{p}' \not\subseteq \bigcup_{\mathfrak{p} \in \Sigma} \mathfrak{p} \;\Rightarrow\; \mathfrak{p}' \cap \mathbf{S} \neq \varnothing.$

(1) Suponiendo $\mathfrak{p}' \subseteq \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p}$.

$$\mathfrak{p}' \subseteq \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p} \;\Rightarrow\; \mathfrak{p}' \subseteq \mathfrak{p} \quad \text{para algún} \quad \mathfrak{p}\in\Sigma, \quad \left(\text{ Proposición 1.2.9 (i) }\right)$$

$$\Rightarrow\; \mathfrak{p}' \in \Sigma, \qquad \left(\text{Definición 2.2.13}\right).$$

$$\therefore\;\; \mathfrak{p}' \notin \Sigma \;\Rightarrow\; \mathfrak{p}' \not\subseteq \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p}.$$

(2) Se supone que $\mathfrak{p}' \cap \mathbf{S} = \varnothing$.

$$\mathfrak{p}' \cap \mathbf{S} = \varnothing \;\Rightarrow\; \forall \;\; x \in \mathfrak{p}' \;\; \text{t. q.} \;\; x \notin \mathbf{S}$$

$$\Rightarrow\; x \in \mathfrak{p}' \;\; \text{y} \;\; x \in \mathbf{A} - \mathbf{S} = \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p}$$

$$\Rightarrow\; x \in \mathfrak{p}' \;\; \text{y} \;\; x \in \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p}$$

$$\Rightarrow\; \mathfrak{p}' \subseteq \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p}.$$

$$\therefore\;\; \mathfrak{p}' \subsetneq \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p} \;\Rightarrow\; \mathfrak{p}' \cap \mathbf{S} \neq \varnothing.$$

Proposición 2.2.15: (2º Teorema de unicidad). Sea $\mathbf{A}$ un anillo, $\mathfrak{a}$ un ideal con una descomposición primaria minimal $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$ y $r(\mathfrak{q}_i) = \mathfrak{p}_i$ $(1 \leq i \leq n)$. Si $\{\mathfrak{p}_{i_1}, \ . \ . \ . \ , \ \mathfrak{p}_{i_m}\}$ es un conjunto genéricamente estable contenido en $\operatorname{Ass}(\mathfrak{a})$, entonces $\mathfrak{q}_{i_1} \cap, \ . \ . \ . \ , \cap \mathfrak{q}_{i_m}$ es independiente de la descomposición primaria.

Demostración:

Sea $\mathbf{S} = \mathbf{A} - (\mathfrak{p}_{i_1} \cup \ . \ . \ . \ \cup \mathfrak{p}_{i_m})$ donde $(1 \leq m \leq n)$. En consecuencia de la proposición 2.2.13, $\mathbf{S}$ es un sistema multiplicativo de $\mathbf{A}$, además $\mathbf{S} \cap \mathfrak{p}_j = \varnothing$ para $j = 1, \ldots, m$.

Por la proposición 2.2.12,

$$\mathbf{S}(\mathfrak{a}) = \left(\mathbf{S}^{-1}\mathfrak{a}\right)^c = \mathfrak{q}_{i_1} \cap, \ . \ . \ . \ , \cap \mathfrak{q}_{i_m}.$$

Si $\mathfrak{a} = \bigcap_{i=1}^{s} \mathfrak{q}'_i$ es otra descomposición primaria minimal del ideal $\mathfrak{a}$. Aplicando lo anterior;

$$\mathbf{S}(\mathfrak{a}) = \left(\mathbf{S}^{-1}\mathfrak{a}\right)^c = \mathfrak{q}'_{i_1} \cap, \ . \ . \ . \ , \cap \mathfrak{q}'_{i_m}.$$

Por tanto, la intersección $\mathfrak{q}_{i_1} \cap, \ . \ . \ . \ , \cap \mathfrak{q}_{i_m}$, no depende de la descomposición primaria de $\mathfrak{a}$ considerada, puesto que en **1º teorema de unicidad** los $\mathfrak{p}_i$ sólo dependen de $\mathfrak{a}$ y no de la descomposición. ■

Definición 2.1.16: Sea $\mathfrak{a}$ un ideal descomponible y $\{\mathfrak{p}_1, \ . \ . \ . \ , \ \mathfrak{p}_n\}$ el conjunto de primos asociados a $\mathfrak{a}$.

- Si $\mathfrak{p}_i$ es un ideal primo **minimal** o **aislado** en el conjunto de primos asociados, entonces $\mathfrak{q}_i$ se llama **componente primaria aislada.**
- Si $\mathfrak{p}_i$ es un ideal primo **inmerso** en el conjunto de primos asociados, entonces $\mathfrak{q}_i$ se llama **componente primaria inmersa.**

Corolario 2.2.17: Sea $\mathbf{A}$ un anillo, $\mathfrak{a}$ un ideal con una descomposición primaria. Las componentes primarias aisladas están determinadas en forma única.

Demostración:

Sea $\mathfrak{p}$ un ideal primo minimal asociado a $\mathfrak{a}$, $\mathfrak{q}_1$ y $\mathfrak{q}_2$ componentes de la descomposición primaria tal que $r(\mathfrak{q}_1) = r(\mathfrak{q}_2) = \mathfrak{p}$.

Considere el conjunto genéricamente estable $\Sigma = \{\mathfrak{p}\}$ y el sistema multiplicativo $\mathbf{S} = \mathbf{A} - \mathfrak{p}$, de la proposición 2.2.15, se obtiene $\mathfrak{q}_1 = \mathfrak{q}_2$.

$\therefore$ Que las componentes primarias aisladas están determinadas en forma única. ■

Sección 2: Cadenas de ideales primos en anillos de extensión.

2.3: Ideales primos y maximales en anillos de extensión.

Esta sección está dedicada a explorar las relaciones entre ideales (**primos y maximales**) en $\mathbf{A}$ y $\mathbf{B}$, donde $\mathbf{B}$ es un anillo de extensión de $\mathbf{A}$. Para ello se introducen algunos conceptos previos sobre dependencia entera.

Definición 2.3.1: Sea $\mathbf{B}$ un anillo y $\mathbf{A}$ un subanillo de $\mathbf{B}$ que contiene $1_{\mathbf{B}}$. Entonces, se dice que, $\mathbf{B}$ es un **anillo de extensión** de $\mathbf{A}$.

Definición 2.3.2: Sea $\mathbf{A} \subseteq \mathbf{B}$ una extensión de anillos. Un elemento $b \in \mathbf{B}$ es **entero** sobre $\mathbf{A}$, si existe un polinomio mónico $f(x) \in \mathbf{A}[x]$ tal que $f(b) = 0$.

Si el polinomio es;

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdot \cdot \cdot + a_1 x + a_0,$$

entonces b cumple la ecuación polinomial,

$$b^n + a_{n-1}b^{n-1} + \cdot \cdot \cdot + a_1 b + a_0 = 0.$$

El elemento $b \in \mathbf{B}$ es entonces una raíz de un polinomio cuyo coeficiente de mayor grado es 1.

Definición 2.3.3: Una extensión de anillos $\mathbf{A} \subseteq \mathbf{B}$ es **entera**, si todo elemento de $\mathbf{B}$ es entero sobre $\mathbf{A}$.

Definición 2.3.4: Sea $\mathbf{A} \subseteq \mathbf{B}$ una extensión de anillos.

$$\tilde{\mathbf{A}} = \{ x \in \mathbf{B} \mid x \text{ es entero sobre } \mathbf{A} \}.$$

El conjunto $\tilde{\mathbf{A}}$ es un subanillo de $\mathbf{B}$ que contiene sólo los elementos de $\mathbf{B}$ enteros sobre $\mathbf{A}$, denominado **clausura entera** de $\mathbf{A}$ en $\mathbf{B}$.

Observación:

1. La definición de $\tilde{\mathbf{A}}$ asegura que $\tilde{\mathbf{A}}$, es entero sobre $\mathbf{A}$ y que contiene todos los subanillos de $\mathbf{B}$ enteros sobre $\mathbf{A}$.
2. Si $\mathbf{B}$ es **entero sobre** $\mathbf{A}$, entonces $\tilde{\mathbf{A}} = \mathbf{B}$.

Definición 2.3.5: Sea $\mathbf{A} \subseteq \mathbf{B}$ una extensión de anillos. El anillo $\mathbf{A}$ es **íntegramente cerrado** en $\mathbf{B}$, si $\mathbf{A} = \tilde{\mathbf{A}}$.

La siguiente proposición muestra que una simple inducción justifica que si se adjunta a un anillo $\mathbf{A}$ un número finito de elementos enteros se obtiene un $\mathbf{A}-$ módulo finitamente generado.

Proposición 2.3.6: Sea $\mathbf{A} \subseteq \mathbf{B}$ una extensión de anillos y $x_1, \ldots, x_n \in \mathbf{B}$ enteros sobre $\mathbf{A}$, entonces el anillo $\mathbf{A}[x_1, \ldots, x_n]$ es un $\mathbf{A}-$módulo finitamente generado.

Demostración:

Se demuestra el caso cuando $n = 1$ y la generalización se obtiene aplicando inducción.

Si $n = 1$ el enunciado del teorema es el siguiente:

$$(x_1 \in \mathbf{B} \text{ es entero sobre } \mathbf{A}) \Rightarrow (\mathbf{A}[x_1] \text{ es un } \mathbf{A}-\text{módulo finitamente generado})$$

Si $x_1 \in \mathbf{B}$ es entero sobre $\mathbf{A}$, entonces existe $a_0, a_1, \ldots, a_{n-1}$ en $\mathbf{A}$ tal que,

$$f(x_1) = x_1^n + a_{n-1}x_1^{n-1} + \cdots + a_1x_1 + a_0 = 0.$$

Todo elemento de $\mathbf{A}[x_1]$ es de la forma $g(x_1)$ con $g(x) \in \mathbf{A}[x]$.

Así:

$$\mathbf{A}[x_1] = \{ g(x_1) \in \mathbf{B} \mid g(x) \in \mathbf{A}[x] \}.$$

Sea $g(x_1) \in \mathbf{A}[x_1]$.

$$(g(x_1) \in \mathbf{A}[x_1]) \Rightarrow (\exists \text{ un polinomio } g(x) \in \mathbf{A}[x]).$$

Del algoritmo de la división,

Si $f(x),\ g(x) \in \mathbf{A}[x]$ y $f(x) \neq 0,$ entonces existen $q(x), r(x) \in \mathbf{A}[x]$ tal que

$$g(x) = f(x)\, q(x) + r(x), \text{ donde } \operatorname{grd}(r(x)) < \operatorname{grd}(f(x)).$$

Así, en $\mathbf{B}$ se obtiene:

$$\mathrm{g}(x_1) = \cancel{f(x_1)} q(x_1) + r(x_1) = r(x_1)$$

$$= a'_m x_1^{\ m} + a'_{m-1} x_1^{\ m-1} + \cdot \cdot \cdot + a'_1 x_1 + a'_0, \quad \text{donde } a'_j \in \mathbf{A}.$$

Luego $\mathrm{g}(x_1)$ es una combinación lineal de $\{ x_1^{\ m}, x_1^{\ m-1}, \ . \ . \ . \ , x_1, 1_{\mathbf{A}} \}$, por tanto $\mathbf{A}[x_1]$ está generado como $\mathbf{A}-$módulo por las potencias de x_1 de orden menor que el $\operatorname{grd}(f(x))$. ■

Nota: Para el lector interesado con elementos que relacionan la dependencia entera y los módulos finitamente generados, puede consultar **[1]**. Páginas 65-67. ■

Proposición 2.3.7: Sea $\mathbf{A} \subseteq \mathbf{B}$ una extensión de anillos. Si $\mathfrak{q}$ es un ideal primo en $\mathbf{B}$, entonces $\mathfrak{q} \cap \mathbf{A}$ es un ideal primo de $\mathbf{A}$.

Demostración:

A continuación se prueba que $\mathfrak{q} \cap \mathbf{A}$ es ideal primo en $\mathbf{A}$. Hágase $\mathbf{S} = \mathbf{A} - (\mathfrak{q} \cap \mathbf{A})$.

Observe los siguientes conjuntos.

$$\mathbf{S} = \mathbf{A} - (q \cap \mathbf{A}) = \mathbf{A} \cap (q \cap \mathbf{A})^{C}$$

$$= \mathbf{A} \cap \left(q^{C} \cup \mathbf{A}^{C}\right)$$

$$= \left(\mathbf{A} \cap q^{C}\right) \cup \left(\mathbf{A} \cap \mathbf{A}^{C}\right)$$

$$= \mathbf{A} \cap q^{C}$$

$$= \mathbf{A} - q.$$

$$\therefore\ \mathbf{S} = \mathbf{A} - q.$$

$$\mathbf{A} - \mathbf{S} = \mathbf{A} - (\mathbf{A} - q) = \mathbf{A} - \left(\mathbf{A} \cap q^{C}\right)$$

$$= \mathbf{A} \cap \left(\mathbf{A} \cap q^{C}\right)^{C}$$

$$= \mathbf{A} \cap \left(\mathbf{A}^{C} \cup \left(q^{C}\right)^{C}\right)$$

$$= \left(\mathbf{A} \cap \mathbf{A}^{C}\right) \cup (\mathbf{A} \cap q)$$

$$= q.$$

$$\therefore\ \mathbf{A} - \mathbf{S} = q.$$

Se demuestra que $\mathbf{S}$ es un sistema multiplicativo de $\mathbf{A}$. Es decir:

(1) $1 \in \mathbf{S}$.

(2) Si $x, y \in \mathbf{S}$, entonces $xy \in \mathbf{S}$.

(1) Se supone que $1 \notin \mathbf{S}$.

$$1 \notin \mathbf{S} = \mathbf{A} - \mathfrak{q} \;\Rightarrow\; 1 \in \mathbf{A} - \mathbf{S} = \mathfrak{q}$$

$$\Rightarrow\; 1 \in \mathfrak{q}$$

$$\Rightarrow\; (1) = \mathfrak{q}, \quad (\rightarrow\leftarrow) \quad (\mathfrak{q} \text{ es ideal primo en } \mathbf{B}). \qquad \therefore\; 1 \in \mathbf{S}.$$

(2) Sean $x, y \in \mathbf{S} = \mathbf{A} - \mathfrak{q}$.

$$x, y \in \mathbf{S} = \mathbf{A} - \mathfrak{q} \;\Rightarrow\; x, y \in \mathbf{A} \;\text{ y }\; x, y \notin \mathfrak{q}$$

$$\Rightarrow\; xy \in \mathbf{A} \;\text{ y }\; xy \notin \mathfrak{q}$$

$$\Rightarrow\; xy \in \mathbf{A} - \mathfrak{q} = \mathbf{S}$$

$$\Rightarrow\; xy \in \mathbf{S}. \qquad \therefore\; xy \in \mathbf{S}.$$

Luego $\mathbf{S}$ es un sistema multiplicativo de $\mathbf{A}$. De acuerdo con la proposición 1.6.1, $\mathfrak{q} \cap \mathbf{A}$ es un ideal primo en $\mathbf{A}$. ■

Definición 2.3.8: Sea $\mathbf{A} \subseteq \mathbf{B}$ una extensión de anillos. El ideal $\mathfrak{p} = \mathfrak{q} \cap \mathbf{A}$ se llama **contracción** de $\mathfrak{q}$ en $\mathbf{A}$ y se dice que $\mathfrak{q}$ está **sobre** $\mathfrak{p}$.

En general la unión de ideales no es un ideal, pero se demuestra que para el caso de una familia totalmente ordenada, la unión satisface las condiciones de la definición 1.1.9, de ideal (**Véase la proposición siguiente**).

Proposición 2.3.9: Sea $\mathfrak{J}$ un conjunto de ideales propios de $\mathbf{A}$, ordenados por la inclusión, si $\mathfrak{L}$ es una cadena de $\mathfrak{J}$, es decir, una familia no vacía $\{\mathfrak{a}_\lambda\}_{\lambda\in\Lambda}$ totalmente ordenada. Se demuestra que la $\bigcup_{\lambda\in\Lambda} \mathfrak{a}_\lambda$, es un ideal propio en $\mathbf{A}$.

Demostración:

Nótese que $\{\mathfrak{a}_\lambda\}_{\lambda\in\Lambda}$ no necesariamente debe ser numerable, pero ayuda a imaginar a $\mathfrak{L}$ cómo;

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdot\ \cdot\ \cdot \subseteq \mathfrak{a}_\alpha \subseteq \mathfrak{a}_{\alpha+1} \subseteq \cdot\ \cdot\ \cdot\ .$$

Sea $\mathfrak{g} = \bigcup_{\lambda\in\Lambda} \mathfrak{a}_\lambda$. Se verifica lo siguiente.

1. Sean $x, y \in \mathfrak{g}$.

$$x, y \in \mathfrak{g} \quad \Rightarrow \quad \exists \ \lambda_1, \lambda_2 \in \Lambda \quad \text{t. q.} \quad x \in \mathfrak{a}_{\lambda_1} \ \text{ y } \ y \in \mathfrak{a}_{\lambda_2}.$$

Suponga que $\mathfrak{a}_{\lambda_1} \subseteq \mathfrak{a}_{\lambda_2}$.

$$\mathfrak{a}_{\lambda_1} \subseteq \mathfrak{a}_{\lambda_2} \;\Rightarrow\; x, y \in \mathfrak{a}_{\lambda_2}$$

$$\Rightarrow x + y \in \mathfrak{a}_{\lambda_2}, \quad \left(\mathfrak{a}_{\lambda_2} \text{ es ideal en } \mathbf{A} \right)$$

$$\Rightarrow x + y \in \bigcup_{\lambda \in \Lambda} \mathfrak{a}_\lambda = \mathfrak{g}.$$

$$\therefore x,\ y \in \mathfrak{g} \;\Rightarrow\; x + y \in \mathfrak{g}.$$

2. Sea $x \in \mathbf{A}$ y $y \in \mathfrak{g}$.

$$y \in \mathfrak{g} \;\Rightarrow\; \exists \;\; \lambda \in \Lambda \;\text{ t. q. }\; y \in \mathfrak{a}_\lambda$$

$$\Rightarrow yx \in \mathfrak{a}_\lambda, \quad \left(\mathfrak{a}_\lambda \text{ es ideal en } \mathbf{A} \right)$$

$$\Rightarrow yx \in \bigcup_{\lambda \in \Lambda} \mathfrak{a}_\lambda = \mathfrak{g}\,.$$

$$\therefore \quad x \in \mathfrak{g} \;\text{ y }\; y \in \mathbf{A} \;\Rightarrow\; yx \in \mathfrak{g}.$$

3. $\mathfrak{g}$ es un ideal propio en $\mathbf{A}$. En efecto si $1 \in \mathfrak{g}$, entonces existe $\lambda \in \Lambda$ tal que $1 \in \mathfrak{a}_\lambda$. Pero esto no es posible por la elección de $\mathfrak{J}$.

Luego $\mathfrak{g}$ verifica las condiciones de la definición de ideal, por tanto $\mathfrak{g}$ es un ideal propio en $\mathbf{A}$.

A continuación se demuestra una propiedad que será de mucha utilidad para el resto de el capitulo.

Proposición 2.3.10: Sea $\mathbf{A}$ un anillo, $\mathbf{S}$ un sistema multiplicativo en $\mathbf{A}$, $\mathfrak{a}$ un ideal de $\mathbf{A}$, tal que $\mathfrak{a} \cap \mathbf{S} = \varnothing$. Entonces existe un ideal primo $\mathfrak{p}$ de $\mathbf{A}$, tal que $\mathfrak{a} \subseteq \mathfrak{p}$, $\mathfrak{p} \cap \mathbf{S} = \varnothing$ y $\mathfrak{p}$ es maximal para la inclusión respecto a los ideales de $\mathbf{A}$ que cumplen estas propiedades.

Demostración: Se define la familia de ideales de $\mathbf{A}$;

$$\mathfrak{J} = \left\{ \mathfrak{b} \subseteq \mathbf{A} \mid \mathfrak{b} \cap \mathbf{S} = \varnothing \quad \text{y} \quad \mathfrak{b} \supseteq \mathfrak{a} \right\}.$$

Este conjunto es no vacío, ya que $\mathfrak{a} \in \mathfrak{J}$. Sea $\{\mathfrak{h}\}_{\mathfrak{h} \in \mathfrak{J}}$ una cadena de elementos en $\mathfrak{J}$, y considérese el conjunto $\mathfrak{F} = \bigcup_{\mathfrak{h} \in \mathfrak{J}} \mathfrak{h}$. De la proposición 2.3.9, $\mathfrak{F}$ es un ideal en $\mathbf{A}$ con la propiedad de que $\mathfrak{a} \subseteq \mathfrak{F}$ y $\mathfrak{F} \cap \mathbf{S} = \varnothing$. Entonces por el lema de Zorn $\mathfrak{J}$ tiene elementos maximales. Dado $\mathfrak{q} \in \mathfrak{J}$ maximal. Se demuestra que $\mathfrak{q}$ es un ideal primo.

Para ello se verifica lo siguiente:

(1) $\mathfrak{q} \neq (1)$.

(2) Si $x, y \in \mathbf{A}$, tal que $xy \in \mathfrak{q}$, entonces $x \in \mathfrak{q}$ ó $y \in \mathfrak{q}$.

Demostración (1):

Supóngase que $\mathfrak{q} = (1)$.

$\mathfrak{q} = (1) \;\Rightarrow\; \exists \;\; x \in \mathfrak{q} \;$ t. q. $\; x = 1$

$\Rightarrow \;\; x \in \mathfrak{q} \;$ y $\; x \in \mathbf{S}, \quad (1 \in \mathbf{S})$

$\Rightarrow \;\; x \in \mathfrak{q} \cap \mathbf{S}$

$\Rightarrow \;\; \mathfrak{q} \cap \mathbf{S} \neq \varnothing, \quad (\rightarrow\leftarrow) \quad (\mathfrak{q} \in \mathfrak{J})$.

Demostración (2):

Supóngase que existe $a_1, a_2 \in \mathbf{A}$ tal que $a_1, a_2 \notin \mathfrak{q}$ y $a_1 a_2 \in \mathfrak{q}$. Considere los ideales $\mathfrak{q} + a_i\,\mathbf{A}$, que satisfacen $\mathfrak{q} \subsetneq \mathfrak{q} + a_i\,\mathbf{A}$ para $i = 1, 2$.

Por la maximalidad de $\mathfrak{q}$,

$$\mathfrak{q} + a_i\,\mathbf{A} \notin \mathfrak{J} \quad \text{para } i = 1, 2.$$

Luego por la definición de $\mathfrak{J}$,

$$\left(\mathfrak{q} + a_i\,\mathbf{A}\right) \cap \mathbf{S} \neq \varnothing \quad \text{para } i = 1, 2.$$

Entonces existe $x, y \in \mathbf{A}$ tal que,

$$x, y \in \left(\mathfrak{q} + a_i\,\mathbf{A}\right) \cap \mathbf{S} \quad \text{para } i = 1, 2.$$

Por definición de intersección resulta:

$$x, y \in \left(\mathfrak{q} + a_i\,\mathbf{A}\right) \quad \text{y} \quad x, y \in \mathbf{S} \quad \text{para } i = 1, 2.$$

Por tanto existen $m_i \in \mathfrak{q}$ y $n_i \in \mathbf{A}$, para $i = 1, 2$ tal que:

$$x = m_1 + a_1 n_1 \qquad y \qquad y = m_2 + a_2 n_2$$

Haciendo el producto de estos elementos,

$$xy = \left(m_1 + a_1 n_1\right)\left(m_2 + a_2 n_2\right)$$

Distribuyendo por ser elementos de $\mathbf{A}$,

$$xy = m_1 m_2 + m_1\left(a_2 n_2\right) + a_1 n_1\left(m_2\right) + a_1 n_1\left(a_2 n_2\right)$$

Asociando por ser elementos de $\mathbf{A}$,

$$xy = m_1 m_2 + m_1\left(a_2 n_2\right) + a_1 n_1\left(m_2\right) + n_1 n_2\left(a_1 a_2\right)$$

Donde todos los sumandos de la derecha están en $\mathfrak{q}$, por tanto $xy \in \mathfrak{q}$. Luego por ser $\mathbf{S}$ un sistema multiplicativo en $\mathbf{A}$, se deduce que $x\,y \in \mathbf{S}$. De donde $xy \in \mathfrak{q} \cap \mathbf{S} = \varnothing$ $(\rightarrow\leftarrow)$. Luego $a_1 \in \mathfrak{q}$ ó $a_2 \in \mathfrak{q}$. En consecuencia $\mathfrak{q}$ es un ideal primo en $\mathbf{A}$ y es maximal entre los que tienen intersección vacía con $\mathbf{S}$. ■

Nota: Hasta este punto se han estudiado los elementos enteros sobre un anillo; para ir más lejos y obtener nuevas propiedades se definen los elementos enteros sobre un ideal.

Definición 2.3.11: Sea $\mathbf{A} \subseteq \mathbf{B}$ una extensión entera de anillos y $\mathfrak{a}$ un ideal de $\mathbf{A}$. Un elemento $x \in \mathbf{B}$ es **entero sobre el ideal** $\mathfrak{a}$, si satisface una ecuación de dependencia entera sobre $\mathbf{A}$:

$$x^n + a_{n-1}x^{n-1} + \cdot \cdot \cdot + a_1 x + a_0 = 0, \quad \text{donde } a_i \in \mathfrak{a}.$$

Definición 2.3.12: Se denomina **clausura entera en B de un ideal** $\mathfrak{a}$ **de A**, al conjunto de todos los elementos de $\mathbf{B}$ enteros sobre $\mathfrak{a}$.

Definición 2.3.13: Sea $\mathbf{A} \subseteq \mathbf{B}$ una extensión de anillos, $\mathfrak{a}$ un ideal de $\mathbf{A}$. Se representa por $\mathfrak{a}\mathbf{B}$, al ideal generado por $\mathfrak{a}$ en $\mathbf{B}$, que está formado por las combinaciones lineales finitas de elementos de $\mathfrak{a}$ con coeficientes en $\mathbf{B}$. Más explícitamente:

$$\mathfrak{a}\mathbf{B} = \left\{ x \in \mathbf{B} \mid x = \sum_{j=1}^{s} b_j a_j, \quad \text{donde } b_j \in \mathbf{B} \quad \text{y} \quad a_j \in \mathfrak{a} \right\}.$$

Lema 2.3.14: Sea $\mathbf{A} \subseteq \mathbf{B}$ una extensión entera de anillos y $\mathfrak{a}$ un ideal de $\mathbf{A}$. Si $\mathbf{C}$ es la clausura entera de $\mathbf{A}$ en $\mathbf{B}$, entonces la clausura entera de $\mathfrak{a}$ en $\mathbf{B}$ es el radical de $\mathfrak{a}\mathbf{C}$ en $\mathbf{C}$.

Demostración:

Denote por $\mathbf{C}'$ la clausura entera de $\mathfrak{a}$ en $\mathbf{B}$. Se demuestra que $\mathbf{C}' = r(\mathfrak{a}\mathbf{C})$ en $\mathbf{C}$.

Verifíquese lo siguiente:

(1) $\mathbf{C}' \subseteq r(\mathfrak{a}\mathbf{C})$.

(2) $\mathbf{C}' \supseteq r(\mathfrak{a}\mathbf{C})$.

Demostración (1):

Sea $x \in \mathbf{C}'$. $(x \in \mathbf{C}') \Rightarrow$ (x es un elemento entero sobre $\mathfrak{a}$).

Si x es entero sobre $\mathfrak{a}$, entonces existen $a_0,\ a_1,\ .\ .\ .\ ,a_{n-1}$ en $\mathfrak{a}$ tal que

$$x^n + a_{n-1}x^{n-1} + \cdot\ \cdot\ \cdot + a_1x + a_0 = 0.$$

Como $\mathfrak{a}$ es ideal en $\mathbf{A}$, por tanto $x \in \mathbf{C}$. Despejando x^n de la expresión anterior

$$x^n = -\sum_{j=0}^{n-1} a_j x^j \in \mathfrak{a}\mathbf{C}, \qquad \text{con } a_j \in \mathfrak{a}.$$

De donde $x \in r(\mathfrak{a}\mathbf{C})$.

$$\therefore \ \mathbf{C}' \subseteq r(\mathfrak{a}\mathbf{C}).$$

Demostración (2):

Sea $x \in r(\mathfrak{a}\mathbf{C})$.

$$x \in r(\mathfrak{a}\mathbf{C}) \ \Rightarrow \ \exists \ n \in \mathbb{N} \ \text{tal que} \ x^n \in \mathfrak{a}\mathbf{C}$$

$$\Rightarrow \ \exists \quad a_j \in \mathfrak{a} \ \text{ y } \ c_j \in \mathbf{C} \ \text{ tal que } \ x^n = \sum_{j=1}^{t} a_j c_j.$$

Cada $a_j \in \mathfrak{a}, (1 \leq j \leq t)$ es entero sobre $\mathfrak{a}$ y por tanto enteros sobre $\mathbf{A}$. De la proposición 2.3.6, el anillo $\mathbf{M} = \mathbf{A}[a_1, \ldots, a_n]$ es un $\mathbf{A}-$módulo finitamente generado.

Denote por $\{m_1, \ldots, m_k\}$ al conjunto de generadores de $\mathbf{M}$ como $\mathbf{A}-$módulo. Por definición de $\mathbf{M}$ y por la elección de x se tiene $x^n \in \mathfrak{a}\mathbf{M}$.

$$x^n \in \mathfrak{a}\mathbf{M} \ \Rightarrow \ x^n m_i \in \mathfrak{a}\mathbf{M} \qquad \forall \quad i = 1, \ldots, k$$

$$\Rightarrow \ \exists \, \alpha_{ij} \in \mathfrak{a} \ \text{ t. q. } \ x^n m_i = \sum_{j=1}^{k} \alpha_{ij} m_j \qquad \forall \ i = 1, \ldots, k$$

$$\Rightarrow \qquad x^n m_i - \sum_{j=1}^{k} \alpha_{ij} m_j = 0 \qquad \forall\ i = 1, \ . \ . \ . \ , k$$

$$\Rightarrow \qquad \sum_{j=1}^{k} \left(x^n\ \delta_{ij} - \alpha_{ij} \right) m_j = 0 \qquad \forall\ i = 1, \ . \ . \ . \ , k, \ \text{ donde } \ \delta_{ij} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}.$$

Escribiendo en forma matricial la expresión anterior

$$\begin{bmatrix} x^n - \alpha_{11} & \alpha_{12} & . \ . \ . & \alpha_{1k} \\ \alpha_{21} & x^n - \alpha_{22} & . \ . \ . & \alpha_{2k} \\ . & . & & . \\ . & . & & . \\ . & . & & . \\ \alpha_{k1} & \alpha_{k2} & . \ . \ . & x^n - \alpha_{kk} \end{bmatrix} \begin{bmatrix} m_1 \\ m_2 \\ . \\ . \\ . \\ m_k \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ . \\ . \\ . \\ 0 \end{bmatrix}.$$

Sea

$$\mathbf{A} = \begin{bmatrix} x^n - \alpha_{11} & \alpha_{12} & . \ . \ . & \alpha_{1k} \\ \alpha_{21} & x^n - \alpha_{22} & . \ . \ . & \alpha_{2k} \\ . & . & & . \\ . & . & & . \\ . & . & & . \\ \alpha_{k1} & \alpha_{k2} & . \ . \ . & x^n - \alpha_{kk} \end{bmatrix}.$$

Multiplicando por la adjunta de $\mathbf{A}$ se obtiene:

$$\operatorname{Adj}(\mathbf{A})\mathbf{A}\begin{bmatrix} m_1 \\ m_2 \\ . \\ . \\ . \\ m_k \end{bmatrix} = \operatorname{Adj}(\mathbf{A})\begin{bmatrix} 0 \\ 0 \\ . \\ . \\ . \\ 0 \end{bmatrix} \Rightarrow \det(\mathbf{A})\begin{bmatrix} m_1 \\ m_2 \\ . \\ . \\ . \\ m_k \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ . \\ . \\ . \\ 0 \end{bmatrix}$$

$$\Rightarrow \det(\mathbf{A})m_1 + \det(\mathbf{A})m_2 + \ . \ . \ . \ + \det(\mathbf{A})m_k = 0$$

$$\Rightarrow \sum_{i=1}^{k} \det(\mathbf{A})m_i = 0$$

$$\Rightarrow \det(\mathbf{A}) = 0$$

$$\Rightarrow (x^n - \alpha_{11})(x^n - \alpha_{22}) \ . \ . \ . \ (x^n - \alpha_{kk}) = 0$$

$$\Rightarrow (x^n)^k + a_{n-1}(x^n)^{k-1} + \ . \ . \ . \ + a_1(x^n) + a_0 = 0,$$

donde $a_j \in \mathfrak{a} \ \forall \ j = n-1, \ . \ . \ . \ , 0$

$$\Rightarrow x^{nk} + a_{n-1}x^{n(k-1)} + \ . \ . \ . \ + a_1 x^n + a_0 = 0$$

$\Rightarrow$ x es entero sobre $\mathfrak{a}$

$\Rightarrow$ $x \in \mathbf{C}'$.

$\therefore \ r(\mathfrak{a}\mathbf{C}) \subseteq \mathbf{C}'$.

Luego la clausura entera de $\mathfrak{a}$ en $\mathbf{B}$ es $r(\mathfrak{a}\mathbf{C})$. ■

Observación: Si $\mathfrak{q}$ es un ideal primo en un anillo de extensión $\mathbf{B}$ de $\mathbf{A}$, entonces la contracción $\mathfrak{q} \cap \mathbf{A}$ de $\mathfrak{q}$ en $\mathbf{A}$ es un ideal primo de $\mathbf{A}$. Véase **proposición 2.3.7**.

El problema del recíproco es: Dado un ideal primo $\mathfrak{p}$ de $\mathbf{A}$, ¿existe un ideal primo $\mathfrak{q}$ de $\mathbf{B}$ que este sobre $\mathfrak{p}$ (esto es, $\mathfrak{q} \cap \mathbf{A} = \mathfrak{p}$)?. Una solución parcial a este problema está dada por el siguiente teorema de **Cohen-Seidenberg**.

Proposición 2.3.15: Sea $\mathbf{A} \subseteq \mathbf{B}$ una extensión entera de anillo y $\mathfrak{p} \subseteq \mathbf{A}$ un ideal primo. Existe un ideal primo $\mathfrak{q} \subseteq \mathbf{B}$ tal que $\mathfrak{q} \cap \mathbf{A} = \mathfrak{p}$.

Demostración:

Considere los siguientes conjuntos:

$$\mathfrak{F} = \{\mathfrak{q} \mid \mathfrak{q} \text{ es u ideal primo en } \mathbf{B}\} \text{ y } \mathfrak{I} = \{\mathfrak{p} \mid \mathfrak{p} \text{ es u ideal primo en } \mathbf{A}\}.$$

Se define una aplicación de $\mathfrak{F}$ en $\mathfrak{I}$:

$$\begin{aligned} \Phi : \mathfrak{F} &\longrightarrow \mathfrak{I} \\ \mathfrak{q} &\rightarrow \Phi(\mathfrak{q}) = \mathfrak{q} \cap \mathbf{A}. \end{aligned}$$

En consecuencia de la proposición 2.3.7, para todo $\mathfrak{q} \in \mathfrak{F}$ se verifica que $\Phi(\mathfrak{q}) = \mathfrak{q} \cap \mathbf{A}$ es un ideal primo en $\mathbf{A}$. Luego la aplicación Φ es cerrada. Se demuestra que Φ es sobreyectiva.

Sea $\mathfrak{p} \in \mathfrak{J}$. Verifíquese que el ideal generado por $\mathfrak{p}$ en $\mathbf{B}$ está sobre $\mathfrak{p}$. $(\mathfrak{p}\mathbf{B} \cap \mathbf{A} = \mathfrak{p})$.

Dado $x \in \mathfrak{p}\mathbf{B} \cap \mathbf{A}$.

$$
\begin{aligned}
x \in \mathfrak{p}\mathbf{B} \cap \mathbf{A} \quad & \Rightarrow \quad x \in \mathfrak{p}\mathbf{B} \quad \text{y} \quad x \in \mathbf{A} \\
& \Rightarrow \quad x \in r(\mathfrak{p}\mathbf{B}) \quad \text{y} \quad x \in \mathbf{A}, \ (\text{Proposición 1.2.15, (i)}) \\
& \Rightarrow \quad x \text{ es entero sobre } \mathfrak{p}, \ (\text{Lema 2.3.14}) \\
& \Rightarrow \quad \exists \ a_0, a_1, \ . \ . \ . \ , a_{n-1} \in \mathfrak{p} \quad \text{t. q. } \ x^n + a_{n-1}x^{n-1} + \cdot \ \cdot \ \cdot + a_1 x + a_0 = 0 \\
& \Rightarrow \quad x^n = \sum_{i=0}^{n-1} a_i \left(-x^i\right) \in \mathfrak{p} \\
& \Rightarrow \quad x \in \mathfrak{p}, \quad (\mathfrak{p} \text{ es primo en } \mathbf{A}) \\
& \Rightarrow \quad \mathfrak{p}\mathbf{B} \cap \mathbf{A} \subseteq \mathfrak{p}.
\end{aligned}
$$

De acuerdo con la proposición 1.3.3, inciso (iii), $\mathfrak{p} \subseteq \mathfrak{p}\mathbf{B} \cap \mathbf{A}$. Habiendo probado ambos contenidos se concluye que $\mathfrak{p}\mathbf{B} \cap \mathbf{A} = \mathfrak{p}$.

Considere el sistema multiplicativo en $\mathbf{A}$ y por tanto en $\mathbf{B}$, definido como; $\mathbf{S} = \mathbf{A} - \mathfrak{p}$.

Se demuestra que el ideal generado por $\mathfrak{p}$ en $\mathbf{B}$ no corta a $\mathbf{S}$. Es decir; $\mathfrak{p}\mathbf{B} \cap \mathbf{S} = \varnothing$.

Supóngase que $\mathfrak{p}\mathbf{B}\cap\mathbf{S}\neq\varnothing$.

$$\mathfrak{p}\mathbf{B}\cap\mathbf{S}\neq\varnothing \;\Rightarrow\; \exists\; x\in\mathfrak{p}\mathbf{B}\cap\mathbf{S}$$

$$\Rightarrow\; x\in\mathfrak{p}\mathbf{B} \quad \text{y} \quad x\in\mathbf{S}$$

$$\Rightarrow\; x\in r(\mathfrak{p}\mathbf{B}) \quad \text{y} \quad x\in\mathbf{S}, \quad (\text{Proposición 1.2.15 (i)})$$

$$\Rightarrow\; x \text{ es entero sobre } \mathfrak{p}, \quad (\text{Lema 2.3.14})$$

$$\Rightarrow\; \exists\;\; a_0, a_1, \ldots, a_{n-1}\in\mathfrak{p} \quad \text{t. q.} \quad x^n + a_{n-1}x^{n-1} + \cdot\;\cdot\;\cdot + a_1x + a_0 = 0$$

$$\Rightarrow\; x^n = \sum_{i=0}^{n-1} a_i\left(-x^i\right)\in\mathfrak{p}, \quad (x\in\mathbf{S}\subseteq\mathbf{A})$$

$$\Rightarrow\; x\in\mathfrak{p} \quad \text{y } x\in\mathbf{S}, \;(\mathfrak{p} \text{ es primo en } \mathbf{A})$$

$$\Rightarrow\; x\in\mathfrak{p}\cap\mathbf{S}=\varnothing, \;(\rightarrow\leftarrow).$$

Luego $\mathfrak{p}\mathbf{B}\cap\mathbf{S}=\varnothing$. De acuerdo con la proposición 2.3.10, existe un ideal primo $\mathfrak{q}$ en $\mathbf{B}$ tal que $\mathfrak{q}\cap\mathbf{S}=\varnothing$ y $\mathfrak{p}\mathbf{B}\subseteq\mathfrak{q}$. Por definición de $\mathbf{S}$, $\mathfrak{q}\subseteq\mathfrak{p}$. Interceptando $\mathbf{A}$, se obtiene;

$$\mathfrak{q}\cap\mathbf{A}\subseteq\mathfrak{p}\cap\mathbf{A}\subseteq\mathfrak{p}.$$

De nuevo interceptando $\mathbf{A}$ en $\mathfrak{p}\mathbf{B}\subseteq\mathfrak{q}$, resulta $\mathfrak{p}\mathbf{B}\cap\mathbf{A}\subseteq\mathfrak{q}\cap\mathbf{A}$.

De la proposición 1.3.3, inciso (iii),

$$\mathfrak{p} \subseteq \mathfrak{p}\mathbf{B} \cap \mathbf{A}.$$

De lo anterior:

$$\mathfrak{p} \subseteq \mathfrak{p}\mathbf{B} \cap \mathbf{A} \subseteq \mathfrak{q} \cap \mathbf{A} \subseteq \mathfrak{p}.$$

Por transitividad se deduce,

$$\mathfrak{p} \subseteq \mathfrak{q} \cap \mathbf{A} \subseteq \mathfrak{p}.$$

Por tanto, $\mathfrak{p} = \mathfrak{q} \cap \mathbf{A} = \Phi(\mathfrak{q})$. Lo que demuestra que Φ es sobreyectiva. De donde si $\mathfrak{p} \subseteq \mathbf{A}$ un ideal primo, entonces existe un ideal primo $\mathfrak{q} \subseteq \mathbf{B}$ tal que $\mathfrak{q} \cap \mathbf{A} = \mathfrak{p}$. ■

Definición 2.3.16: Sea $\mathbf{A}$ un anillo y $\{\mathfrak{a}_0, \mathfrak{a}_1, \ldots, \mathfrak{a}_n, \ldots\}$ un conjunto de ideales en $\mathbf{A}$. Una **cadena ascendente** de ideales es una expresión de la forma:

$$\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \cdots \subseteq \mathfrak{a}_n \subseteq \cdots.$$

Teorema 2.3.17: (Teorema del ascenso). Sea $\mathbf{A} \subseteq \mathbf{B}$ una extensión entera de anillo y $\mathfrak{p}_1 \subseteq \ldots \subseteq \mathfrak{p}_n$ una cadena finita ascendente de ideales primos de $\mathbf{A}$ y $\mathfrak{q}_1 \subseteq \ldots \subseteq \mathfrak{q}_m$ una cadena ascendente de ideales primos de $\mathbf{B}$ verificando $\mathfrak{q}_i \cap \mathbf{A} = \mathfrak{p}_i$, para $1 \leq i \leq m < n$.

$$\mathfrak{p}_1 \subseteq \mathfrak{p}_2 \subseteq \ ... \ \subseteq \mathfrak{p}_m \subseteq \ ... \ \subseteq \mathfrak{p}_n ;$$
$$\mathfrak{q}_1 \subseteq \mathfrak{q}_2 \subseteq \ ... \ \subseteq \mathfrak{q}_m .$$

Entonces la cadena $\mathfrak{q}_1 \subseteq \ ... \ \subseteq \mathfrak{q}_m$ se puede extender a una cadena $\mathfrak{q}_1 \subseteq \ ... \ \subseteq \mathfrak{q}_n$ en la que $\mathfrak{q}_i \cap \mathbf{A} = \mathfrak{p}_i,\ 1 \leq i \leq n.$

Demostración:

Por inducción sobre $m,\ n$ se reduce al caso $m = 1$ y $n = 2.$

Proceso 1: Cuando $m = 1,\ n = 2.$ El enunciado del teorema es:

Si $\mathfrak{p}_1,\ \mathfrak{p}_2$ son ideales primos en $\mathbf{A}$ tal que $\mathfrak{p}_1 \subseteq \mathfrak{p}_2,\ \mathfrak{q}_1$ un ideal primo en $\mathbf{B}$ verificando $\mathfrak{q}_1 \cap \mathbf{A} = \mathfrak{p}_1,$ entonces existe un ideal primo $\mathfrak{q}_2$ en $\mathbf{B}$ tal que $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$ y $\mathfrak{q}_2 \cap \mathbf{A} = \mathfrak{p}_2.$

Se demuestra lo siguiente:

(1) Existe un ideal primo $\mathfrak{q}_2$ en $\mathbf{B}$ tal que $\mathfrak{q}_1 \subseteq \mathfrak{q}_2.$

(2) $\mathfrak{q}_2 \cap \mathbf{A} = \mathfrak{p}_2.$

Demostración (1):

Como $\mathfrak{p}_2$ es primo en $\mathbf{A},\ \mathbf{S} = \mathbf{A} - \mathfrak{p}_2$ es un sistema multiplicativo en $\mathbf{A}.$ Por hipótesis $\mathfrak{q}_1 \cap \mathbf{A} = \mathfrak{p}_1 \subseteq \mathfrak{p}_2.$

Interceptando $\mathbf{S}$ se obtiene:

$$\left(\mathfrak{q}_1 \cap \mathbf{A}\right) \cap \mathbf{S} = \mathfrak{q}_1 \cap \left(\mathbf{A} \cap \mathbf{S}\right) = \mathfrak{q}_1 \cap \mathbf{S} \subseteq \mathfrak{p}_2 \cap \mathbf{S} = \varnothing.$$

De donde se deduce que $\mathfrak{q}_1 \cap \mathbf{S} = \varnothing$. En consecuencia de la proposición 2.3.10, existe un ideal primo $\mathfrak{q}_2$ en $\mathbf{B}$ tal que $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$ y es maximal en el conjunto de todos los ideales $\mathfrak{a}$ en $\mathbf{B}$ que verifican $\mathfrak{q}_1 \subseteq \mathfrak{a}$ y $\mathfrak{a} \cap \mathbf{S} = \varnothing$.

$\therefore$ Existe un ideal primo $\mathfrak{q}_2$ en $\mathbf{B}$ tal que $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$.

Demostración (2):

Ahora se verifica que $\mathfrak{q}_2$ esta sobre $\mathfrak{p}_2$; es decir $\mathfrak{q}_2 \cap \mathbf{A} = \mathfrak{p}_2$.

De nuevo considérese la familia:

$$\Gamma = \left\{ \mathfrak{a} \subseteq \mathbf{B} \mid \mathfrak{a} \cap \mathbf{S} = \varnothing \right\} \quad .$$

Por la maximalidad de $\mathfrak{q}_2$; $\mathfrak{q}_2 \in \Gamma$, entonces,

$$\mathfrak{q}_2 \cap \mathbf{S} = \mathfrak{q}_2 \cap \left(\mathbf{A} - \mathfrak{p}_2\right) = \varnothing.$$

De donde, $\mathfrak{q}_2 \subseteq \mathfrak{p}_2$. Intersectando $\mathbf{A}$ se obtiene:

$$\mathfrak{q}_2 \cap \mathbf{A} \subseteq \mathfrak{p}_2 \cap \mathbf{A} \subseteq \mathfrak{p}_2.$$

Se deduce que $\mathfrak{q}_2 \cap \mathbf{A} \subseteq \mathfrak{p}_2$.

Para la otra inclusión, supóngase $\mathfrak{q}_2 \cap \mathbf{A} \neq \mathfrak{p}_2$, $\left(\mathfrak{q}_2 \cap \mathbf{A} \supsetneq \mathfrak{p}_2\right)$.

$$\mathfrak{q}_2 \cap \mathbf{A} \neq \mathfrak{p}_2 \quad \Rightarrow \quad \mathfrak{p}_2 - \left(\mathfrak{q}_2 \cap \mathbf{A}\right) \neq \varnothing$$

$$\Rightarrow \quad \exists \;\; u \in \mathfrak{p}_2 - \left(\mathfrak{q}_2 \cap \mathbf{A}\right)$$

$$\Rightarrow \quad u \in \mathfrak{p}_2 \quad \text{y} \quad u \notin \left(\mathfrak{q}_2 \cap \mathbf{A}\right)$$

$$\Rightarrow \quad u \in \mathfrak{p}_2 \quad \text{y} \quad \left\{ u \notin \mathfrak{q}_2 \quad \text{ó} \quad u \notin \mathbf{A} \right\}$$

$$\Rightarrow \quad \left\{ u \in \mathfrak{p}_2 \quad \text{y} \quad u \notin \mathfrak{q}_2 \right\} \;\text{ ó }\; \left\{ u \in \mathfrak{p}_2 \quad \text{y} \quad u \notin \mathbf{A} \right\}$$

$$\Rightarrow \quad u \in \mathfrak{p}_2 \quad \text{y} \quad u \notin \mathfrak{q}_2, \quad \left(\mathfrak{p}_2 \text{ es ideal en } \mathbf{A}\right).$$

De lo anterior $u \notin \mathfrak{q}_2$, luego el ideal $\mathfrak{q}_2 + (u) \supsetneq \mathfrak{q}_2$. De donde por la maximalidad de $\mathfrak{q}_2$, $\mathfrak{q}_2 + (u) \notin \Gamma$.

$$\mathfrak{q}_2 + (u) \notin \Gamma \quad \Rightarrow \quad \left(\mathfrak{q}_2 + (u)\right) \cap \mathbf{S} \neq \varnothing$$

$$\Rightarrow \quad \exists \quad s \in \left(\mathfrak{q}_2 + (u)\right) \cap \mathbf{S}$$

$$\Rightarrow \quad s \in \mathfrak{q}_2 + (u) \quad \text{y} \quad s \in \mathbf{S}$$

$$\Rightarrow \quad \exists \quad t \in \mathfrak{q}_2, \;\; y \in \mathbf{B} \quad \text{t. q.} \quad s = t + uy.$$

Como $\mathbf{A} \subseteq \mathbf{B}$, es una extensión entera de anillos, entonces $y \in \mathbf{B}$ es entero sobre $\mathbf{A}$, por tanto existen $a_0, a_1, \ldots, a_{n-1}$ en $\mathbf{A}$ tal que

$$y^n + a_{n-1}y^{n-1} + \cdots + a_1 y + a_0 = 0.$$

Multiplicando por u^n resulta,

$$(yu)^n + a_{n-1}u(yu)^{n-1} + \cdots + a_1 u^{n-1}(yu) + a_0 u^n = 0.$$

De la relación $s - t = uy$ se deduce,

$$(s-t)^n + a_{n-1}u(s-t)^{n-1} + \cdots + a_1 u^{n-1}(s-t) + a_0 u^n = 0.$$

El teorema del binomio implica,

$$\left(\sum_{i=0}^{n}\binom{n}{i}s^{n-i}(-t)^i\right) + a_{n-1}u\left(\sum_{i=0}^{n-1}\binom{n-1}{i}s^{(n-1)-i}(-t)^i\right) + \cdots + a_1 u^{n-1}(s-t) + a_0 u^n = 0.$$

Lo que equivale a,

$$s^n+\left(\underbrace{\sum_{i=1}^{n}\binom{n}{i}s^{n-i}\left(-t\right)^i}_{\alpha_1 t}\right)+a_{n-1}u\left(s^{n-1}+\underbrace{\sum_{i=1}^{n-1}\binom{n\text{-}1}{i}s^{(n-1)-i}\left(-t\right)^i}_{\alpha_2 t}\right)+\ \cdots +a_1u^{n\text{-}1}\left(s-t\right)+a_0u^n=0.$$

Sustituyendo $\alpha_1 t,\ \alpha_2 t$ y distribuyendo,

$$s^n+\alpha_1 t+a_{n-1}us^{n-1}+a_{n-1}u\alpha_2 t+\ \cdot\cdot\cdot\ +a_1u^{n-1}s-a_1u^{n-1}t+a_0u^n=0,\quad \text{con }\ \alpha_1,\ \alpha_2\in\mathbf{A}.$$

Agrupando,

$$\left(s^n+a_{n-1}us^{n-1}+\ \cdot\cdot\cdot\ +a_1u^{n-1}s+a_0u^n\right)+\left(\alpha_1 t+a_{n-1}u\alpha_2 t+\ \cdot\cdot\cdot\ -a_1u^{n-1}t\right)=0\,.$$

Haciendo $v=s^n+a_{n-1}us^{n-1}+\ \cdot\cdot\cdot\ +a_1u^{n-1}s+a_0u^n$. Despejando y factorizando resulta:

$$v=\left(-\alpha_1-a_{n-1}u\alpha_2-\ \cdot\cdot\cdot\ +a_1u^{n-1}\right)t.$$

Como $t\in\mathfrak{q}_2$, entonces $v\in\mathfrak{q}_2$. Además $\mathfrak{q}_2\subseteq\mathfrak{p}_2\subseteq\mathbf{A}$ y $t,v\in\mathfrak{q}_2$, por tanto $t,\ v\in\mathfrak{q}_2\cap\mathbf{A}\subseteq\mathfrak{p}_2$. Despejando s^n de v, se tiene:

$$s^n=v-\alpha_1 t-u\left(a_{n-1}s^{n-1}-\ \cdot\cdot\cdot\ -a_1u^{n-2}s-a_0u^{n-1}\right),$$

donde todos los sumandos de la derecha están en $\mathfrak{p}_2$, por tanto $s^n \in \mathfrak{p}_2$. Por ser $\mathfrak{p}_2$ primo, s debe pertenecer a $\mathfrak{p}_2$, $(\rightarrow\leftarrow)$.■

Nota: La generalización de este teorema se obtiene aplicando reiteradamente el **proceso 1,** con $(m = 1 \text{ y } n = 2)$. Observe las cadenas con $m = 1$ y $n = k \geq 2$:

$$\begin{array}{l} \boxed{\begin{array}{l}\mathfrak{p}_1 \subseteq \mathfrak{p}_2 \\ \mathfrak{q}_1\end{array}} \subseteq \mathfrak{p}_3 \subseteq \ \cdots \ \subseteq \mathfrak{p}_{k-1} \subseteq \mathfrak{p}_k; \\ \overbrace{\mathfrak{q}_1 \cap \mathbf{A} = \mathfrak{p}_1}^{\uparrow}. \end{array}$$

Aplicando el **proceso 1** a lo enmarcado, existe un ideal primo $\mathfrak{q}_2$ en $\mathbf{B}$ tal que $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$ y $\mathfrak{q}_2 \cap \mathbf{A} = \mathfrak{p}_2$.

$$\begin{array}{ll} \begin{array}{l}\mathfrak{p}_1 \subseteq \\ \mathfrak{q}_1 \subseteq\end{array} & \boxed{\begin{array}{l}\mathfrak{p}_2 \subseteq \mathfrak{p}_3 \\ \mathfrak{q}_2\end{array}} \subseteq \ \cdots \ \subseteq \mathfrak{p}_{k-1} \subseteq \mathfrak{p}_k; \\ & \overbrace{\mathfrak{q}_2 \cap \mathbf{A} = \mathfrak{p}_2}^{\uparrow}. \end{array}$$

Aplicando el **proceso 1** a lo enmarcado, existe un ideal primo $\mathfrak{q}_3$ en $\mathbf{B}$ tal que $\mathfrak{q}_2 \subseteq \mathfrak{q}_3$ y $\mathfrak{q}_3 \cap \mathbf{A} = \mathfrak{p}_3$.

$$\begin{array}{ll} \begin{array}{l}\mathfrak{p}_1 \subseteq \mathfrak{p}_2 \subseteq \\ \mathfrak{q}_1 \subseteq \mathfrak{q}_2 \subseteq\end{array} & \boxed{\begin{array}{l}\mathfrak{p}_3 \subseteq \\ \mathfrak{q}_3\end{array}} \ \cdots \ \subseteq \mathfrak{p}_{k-1} \subseteq \mathfrak{p}_k; \\ & \overbrace{\mathfrak{q}_3 \cap \mathbf{A} = \mathfrak{p}_3}^{\uparrow}. \end{array}$$

Sucesivamente, existe un ideal primo $\mathfrak{q}_{k-1}$ en $\mathbf{B}$ tal que $\mathfrak{q}_{k-2} \subseteq \mathfrak{q}_{k-1}$ y $\mathfrak{q}_{k-1} \cap \mathbf{A} = \mathfrak{p}_{k-1}$.

$$\begin{array}{l} \mathfrak{p}_1 \subseteq \mathfrak{p}_2 \subseteq \ . \ . \ . \ \subseteq \mathfrak{p}_{k-2} \subseteq \\ \mathfrak{q}_1 \subseteq \mathfrak{q}_2 \subseteq \ . \ . \ . \ \subseteq \mathfrak{q}_{k-2} \subseteq \end{array} \underbrace{\boxed{\begin{array}{l} \mathfrak{p}_{k-1} \subseteq \mathfrak{p}_k \\ \mathfrak{q}_{k-1} \end{array}}}_{\substack{\uparrow \\ \mathfrak{q}_{k-1} \cap \mathbf{A} = \mathfrak{p}_{k-1}.}} ;$$

Ahora se aplica el **proceso 1** a lo enmarcado, entonces existe un ideal primo $\mathfrak{q}_k$ en $\mathbf{B}$ tal que $\mathfrak{q}_{k-1} \subseteq \mathfrak{q}_k$ y $\mathfrak{q}_k \cap \mathbf{A} = \mathfrak{p}_k$.

$$\begin{array}{l} \mathfrak{p}_1 \subseteq \mathfrak{p}_2 \subseteq \ . \ . \ . \ \subseteq \mathfrak{p}_{k-1} \subseteq \mathfrak{p}_k; \\ \mathfrak{q}_1 \subseteq \mathfrak{q}_2 \subseteq \ . \ . \ . \ \subseteq \mathfrak{q}_{k-1} \subseteq \mathfrak{q}_k. \end{array}$$

Luego la cadena inferior se ha extendido al mismo número de eslabones que la cadena superior.■

Proposición 2.3.18: (Teorema de incomparabilidad). Sea $\mathbf{A} \subseteq \mathbf{B}$ una extensión entera y $\mathfrak{p}$ un ideal primo en $\mathbf{A}$. Si $\mathfrak{q}_1$ y $\mathfrak{q}_2$ son ideales primos en $\mathbf{B}$ tal que $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$ y ambos están sobre $\mathfrak{p}$, entonces $\mathfrak{q}_1 = \mathfrak{q}_2$.

Demostración:

Si $\mathfrak{q}_1$ y $\mathfrak{q}_2$ están sobre $\mathfrak{p}$, entonces por la definición 2.3.8, $\mathfrak{p} = \mathfrak{q}_1 \cap \mathbf{A} = \mathfrak{q}_2 \cap \mathbf{A}$. Supóngase $\mathfrak{q}_1 \subsetneq \mathfrak{q}_2$ y sea $u \in \mathfrak{q}_2 - \mathfrak{q}_1$. Como $\mathbf{A} \subseteq \mathbf{B}$ es una extensión entera, entonces u es entero sobre $\mathbf{A}$.

Luego existen $a_0, a_1\ ,\ .\ .\ .\ .\ ,\ a_{n-1}$ en $\mathbf{A}$ tal que,

$$u^n + a_{n-1}u^{n-1} + \ \cdot\ \cdot\ \cdot\ + a_1u + a_0 = 0.$$

Dado que $\mathfrak{q}_1$ y $\mathfrak{q}_2$ son ideales en $\mathbf{A}$,

$$u^n + a_{n-1}u^{n-1} + \ \cdot\ \cdot\ \cdot\ + a_1u + a_0 \equiv 0 \quad (\mathrm{mod}\ \mathfrak{q}_1 \quad \text{y} \quad \mathrm{mod}\ \mathfrak{q}_2). \qquad (1)$$

Tomando n como el menor de los posibles enteros verificando lo anterior. Por la elección de u se tiene $u \in \mathfrak{q}_2$, de donde,

$$a_0 \equiv 0(\mathrm{mod}\ \mathfrak{q}_2).$$

Entonces $a_0 \in \mathfrak{q}_2$ y $a_0 \in \mathbf{A}$, por tanto $a_0 \in \mathfrak{q}_2 \cap \mathbf{A} = \mathfrak{q}_1 \cap \mathbf{A} \subseteq \mathfrak{q}_1$. Luego,

$$a_0 \equiv 0(\mathrm{mod}\ \mathfrak{q}_1).$$

La expresión en (1) se reduce a;

$$u^n + a_{n-1}u^{n-1} + \ \cdot\ \cdot\ \cdot\ + a_1u \equiv 0(\mathrm{mod}\ \mathfrak{q}_1). \qquad (2)$$

Sacando como factor común, u en (2) se obtiene, un polinomio unitario con término independiente no nulo; es decir;

$$u\left\{u^{n-1} + a_{n-1}u^{n-2} + \ \cdot\ \cdot\ \cdot\ + a_1\right\} \equiv 0(\mathrm{mod}\ \mathfrak{q}_1).$$

Como $\mathfrak{q}_1$, es un ideal primo en $\mathbf{B}$,

$$u \equiv 0(\text{mod } \mathfrak{q}_1) \qquad \text{ó} \qquad u^{n-1} + a_{n-1}u^{n-2} + \cdot \cdot \cdot \cdot + a_1 \equiv 0(\text{mod } \mathfrak{q}_1).$$

Por la minimalidad del n y por la elección de u,

$$u \notin \mathfrak{q}_1 \quad \text{y} \quad u^{n-1} + a_{n-1}u^{n-2} + \cdot \cdot \cdot + a_1 \notin \mathfrak{q}_1.$$

Pero esto es una contradicción dado que $\mathfrak{q}_1$ es un ideal primo en $\mathbf{B}$. Por tanto lo supuesto es falso. De ahí $\mathfrak{q}_2 = \mathfrak{q}_1$. ■

Proposición 2.3.19: Sea $\mathbf{A} \subseteq \mathbf{B}$ una extensión entera de anillos; $\mathfrak{q}$ un ideal primo en $\mathbf{B}$ y $\mathfrak{p} = \mathfrak{q} \cap \mathbf{A}$. Son equivalentes los enunciados siguientes:

(i) $\mathfrak{q}$ es maximal en $\mathbf{B}$.

(ii) $\mathfrak{p}$ es maximal en $\mathbf{A}$.

Demostración:

$(\text{i}) \Rightarrow (\text{ii})$.

Supóngase $\mathfrak{q}$ es maximal en $\mathbf{B}$. Se demuestra que $\mathfrak{p}$ es maximal.

$(\mathfrak{q}$ es primo en $\mathbf{B}) \Rightarrow (\mathfrak{p} = \mathfrak{q} \cap \mathbf{A}$ es primo en $\mathbf{A})$, (Proposición 2.3.7)

$\Rightarrow \ (\mathfrak{p} \neq \mathbf{A})$

$\Rightarrow \ (\exists$ un ideal maximal $\mathfrak{m} \subsetneq \mathbf{A}$ tal que $\mathfrak{m} \supseteq \mathfrak{p})$, (Proposición 1.2.6)

$\Rightarrow \ (\exists$ un ideal primo $\mathfrak{m} \subsetneq \mathbf{A}$ tal que $\mathfrak{m} \supseteq \mathfrak{p}$ y $\mathfrak{q} \cap \mathbf{A} = \mathfrak{p})$, (Prop. 1.2.4)

$\Rightarrow \ (\exists$ un primo $\mathfrak{q}' \subsetneq \mathbf{B}$ tal que $\mathfrak{q}' \supseteq \mathfrak{q}$ y $\mathfrak{q}' \cap \mathbf{A} = \mathfrak{m})$, (Prop 2.3.17)

$\Rightarrow \ (\mathfrak{q}' = \mathfrak{q})$, ($\mathfrak{q}$ es maximal en $\mathbf{B}$)

$\Rightarrow \ (\mathfrak{p} = \mathfrak{q} \cap \mathbf{A} = \mathfrak{q}' \cap \mathbf{A} = \mathfrak{m})$

$\Rightarrow$ ($\mathfrak{p}$ es maximal en $\mathbf{A}$).

$\therefore$ $\mathfrak{p}$ es maximal en $\mathbf{A}$.

$(\text{ii}) \Rightarrow (\text{i})$.

Supóngase $\mathfrak{p}$ es maximal en $\mathbf{A}$. Se demuestra que $\mathfrak{q}$ es maximal $\mathbf{B}$.

($\mathfrak{q}$ es primo en $\mathbf{B}$) $\Rightarrow \ (\mathfrak{q} \neq \mathbf{B})$

$\Rightarrow \ (\exists$ un ideal maximal $\mathfrak{n} \subsetneq \mathbf{B}$ tal que $\mathfrak{n} \supseteq \mathfrak{q}$), (Proposición 1.2.6)

$\Rightarrow \ (\exists$ un ideal primo $\mathfrak{n} \subsetneq \mathbf{B}$ tal que $\mathfrak{n} \supseteq \mathfrak{q})$, (Proposición 1.2.4)

$$\Rightarrow \quad (1_{\mathbf{A}} = 1_{\mathbf{B}} \notin \mathfrak{n}), \quad (\mathbf{B} \text{ es anillo de extensión de } \mathbf{A})$$

$$\Rightarrow \quad (\mathfrak{p} = \mathfrak{q} \cap \mathbf{A} \subseteq \mathfrak{n} \cap \mathbf{A} \subsetneq \mathbf{A})$$

$$\Rightarrow \quad (\mathfrak{p} \subseteq \mathfrak{n} \cap \mathbf{A} \subsetneq \mathbf{A})$$

$$\Rightarrow \quad (\mathfrak{p} = \mathfrak{n} \cap \mathbf{A}), \quad (\mathfrak{p} \text{ es maximal en } \mathbf{A})$$

$$\Rightarrow \quad (\mathfrak{p} = \mathfrak{n} \cap \mathbf{A} \ \text{ y } \ \mathfrak{p} = \mathfrak{q} \cap \mathbf{A})$$

$$\Rightarrow \quad (\mathfrak{q} = \mathfrak{n}), \quad (\text{Proposición 2.3.18}, (\textbf{Teorema de incomparabilidad}))$$

$$\Rightarrow \quad (\mathfrak{q} \text{ es maximal en } \mathbf{B}).$$

$$\therefore \ \mathfrak{q} \text{ es maximal en } \mathbf{B}.$$

Luego se concluye que $\mathfrak{q}$ es maximal en $\mathbf{B}$ sí y sólo si $\mathfrak{p}$ es maximal en $\mathbf{A}$. ■

Proposición 2.3.20: Sea $\mathbf{A} \subseteq \mathbf{B}$ una extensión de dominios de integridad, siendo $\mathbf{B}$ entero sobre $\mathbf{A}$. Son equivalentes los siguientes enunciados:

(i) $\mathbf{B}$ es un cuerpo.

(ii) $\mathbf{A}$ es un cuerpo.

Demostración:

$(i) \Rightarrow (ii)$.

Supóngase que $\mathbf{B}$ es un cuerpo. Se demuestra que todo elemento no nulo en $\mathbf{A}$ es una unidad.

Sea $\alpha \in \mathbf{A}$ t. q. $\alpha \neq 0$.

$$\alpha \in \mathbf{A} \quad \Rightarrow \quad \alpha \in \mathbf{B} \quad (\mathbf{A} \subseteq \mathbf{B})$$

$$\Rightarrow \quad \exists \ \alpha^{-1} \in \mathbf{B} \quad \text{t. q.} \quad \alpha \cdot \alpha^{-1} = 1.$$

Luego existe α^{-1} que está contenido $\mathbf{B}$. Se demuestra que $\alpha^{-1} \in \mathbf{A}$.

Como $\alpha^{-1} \in \mathbf{B}$ es entero sobre $\mathbf{A}$, entonces existen $a_0,\ a_1,\ . \ . \ . \ , a_{n-1}$ en $\mathbf{A}$ tal que;

$$\left(\alpha^{-1}\right)^n + a_{n-1}\left(\alpha^{-1}\right)^{n-1} + \ \cdot \ \cdot \ \cdot + a_1\left(\alpha^{-1}\right) + a_0 = 0.$$

Reescribiendo exponentes en esta ecuación se obtiene,

$$\alpha^{-n} + a_{n-1}\alpha^{-n+1} + \ \cdot \ \cdot \ \cdot \ + a_1\alpha^{-1} + a_0 = 0.$$

Multiplicado por $\alpha^{n-1} \in \mathbf{A}$, pues $n \geq 1$,

$$\alpha^{-1} + a_{n-1}\alpha^0 + \ \cdot \ \cdot \ \cdot + a_1\alpha^{n-2} + a_0\alpha^{n-1} = 0.$$

Despejando α^{-1},

$$\alpha^{-1} = -\left(a_{n-1}\alpha^{0} + \cdot \cdot \cdot + a_1\alpha^{n-2} + a_0\alpha^{n-1}\right).$$

La parte de la derecha está en $\mathbf{A}$, pues es un subanillo de $\mathbf{B}$, entonces $\alpha^{-1} \in \mathbf{A}$. Luego todo elemento no nulo de $\mathbf{A}$ es una unidad.

$\therefore$ $\mathbf{A}$ es un cuerpo.

$(ii) \Rightarrow (i)$. Suponiendo que $\mathbf{A}$ es un cuerpo. Se demuestra que $\mathbf{B}$, es un cuerpo.

Sea $b \in \mathbf{B}$ t. q. $b \neq 0$.

Si $b \in \mathbf{B}$ y es entero sobre $\mathbf{A}$, entonces existe $a_0, a_1, \ . \ . \ . \ , a_{n-1}$ en $\mathbf{A}$ tal que

$$b^n + a_{n-1}b^{n-1} + \cdot \cdot \cdot + a_1 b + a_0 = 0. \qquad (1)$$

Se supone que n es el menor de los enteros posibles verificando lo anterior; $a_0 \neq 0$. Pues si $a_0 = 0$ se tiene:

$$b^n + a_{n-1}b^{n-1} + \cdot \cdot \cdot + a_1 b = 0.$$

Sacando como factor común, a *b*, se obtiene un polinomio unitario con término independiente no nulo; es decir:

$$b\left(b^{n-1} + a_{n-1}b^{n-2} + \cdot \cdot \cdot + a_1\right) = 0.$$

Como $\mathbf{B}$, es un dominio,

$$b = 0 \qquad \text{ó} \qquad b^{n-1} + a_{n-1}b^{n-2} + \cdot \cdot \cdot + a_1 = 0.$$

La minimalidad de $n,$ implica que $b = 0,$ $(\rightarrow\leftarrow).$ Así $a_0 \neq 0.$ Ahora en (1) el término independiente $a_0 \neq 0.$

Despejando:

$$b^n + a_{n-1}b^{n-1} + \cdot \cdot \cdot + a_1 b = -a_0.$$

Sacando factor común $b,$

$$b\left(b^{n-1} + a_{n-1}b^{n-2} + \cdot \cdot \cdot + a_1\right) = -a_0. \qquad (2)$$

Como $-a_0 \in \mathbf{A},$ entonces existe $-a_0^{-1} \in \mathbf{A},$ tal que $\left(-a_0^{-1}\right)\left(-a_0\right) = 1.$ ($\mathbf{A}$ es un cuerpo)

Multiplicando por $-a_0^{-1}$ en (2):

$$b\left(b^{n-1} + a_{n-1}b^{n-2} + \cdot \cdot \cdot + a_1\right)\left(-a_0^{-1}\right) = \left(-a_0\right)\left(-a_0^{-1}\right) = 1.$$

Entonces b es una unidad en $\mathbf{B}$. Luego todo elemento no nulo en $\mathbf{B}$ es unidad, lo que demuestra que $\mathbf{B}$ es un cuerpo. ■

2.4: Extensiones enteras en anillos de fracciones.

Esta sección se dedica a investigar el comportamiento de las extensiones enteras bajo las operaciones de localización. Se definen dominios normales y se demuestra el teorema del **descenso**, pero antes se introducen algunos elementos sobre extensiones de cuerpos que serán de mucha utilidad.

Definición 2.4.1: Sea $\mathbf{k}$ un cuerpo y $\mathbf{F} \subseteq \mathbf{k}$. Se dice que $\mathbf{F}$ es un **subcuerpo** de $\mathbf{k}$ si $\mathbf{F}$ es un cuerpo respecto a las operaciones $(+)$ y $(\cdot)$ de $\mathbf{k}$.

Definición 2.4.2: Sea $\mathbf{k}$ un cuerpo y $\mathbf{F}$ un subcuerpo de $\mathbf{k}$. Entonces se dice que $\mathbf{k}$ es una **extensión** (o **cuerpo de extensión**) de $\mathbf{F}$.

Definición 2.4.3: Sea $\mathbf{K}$ un cuerpo. Un elemento $x \in \mathbf{K}$, se dice que es **algebraico sobre** un subcuerpo $\mathbf{F}$, si existen elementos $\alpha_0, \alpha_1, \ldots, \alpha_n$ en $\mathbf{F}$ no todos cero, tal que

$$\alpha_n x^n + \alpha_{n-1} x^{n-1} + \cdot \cdot \cdot + \alpha_1 x + \alpha_0 = 0.$$

Definición 2.4.4: Un dominio $\mathbf{A}$ se llama **normal** ó **íntegramente cerrado,** si es íntegramente cerrado en su cuerpo de fracciones.

Definición 2.4.5: Sea $\mathbf{F} \subseteq \mathbf{k}$ una extensión de cuerpos. Si $\beta \in \mathbf{k}$ es algebraico sobre $\mathbf{F}$, entonces existe un polinomio mónico, irreducible $f(x) \in \mathbf{F}[x]$ tal que $f(\beta) = 0$ y cualquier otro polinomio que tenga a β como raíz será divisible por $f(x)$. Este polinomio se llama **polinomio minimal** de β sobre $\mathbf{F}$.

Definición 2.4.6: Dos números algebraicos α y β se dicen **conjugados,** si tienen el mismo polinomio minimal.

Proposición 2.4.7 (Regla de Ruffini): Un elemento $\alpha \in \mathbf{A}$ es un cero de un polinomio en $\mathbf{A}[x]$ si y sólo si $x-\alpha$ divide a ese polinomio.

Si se supone que un polinomio mónico $f(x)$ tiene n raíces, entonces por la Regla de Ruffini se descompone en factores lineales:

$$f(x) = x^n + \alpha_{n-1}x^{n-1} + \cdot\ \cdot\ \cdot + \alpha_1 x + \alpha_0 = (x-v_1)(x-v_2)\cdot\ \cdot\ \cdot\ (x-v_n).$$

Operando en el segundo miembro e igualando, se deduce que los coeficientes se pueden expresar en términos de las raíces con la fórmula:

$$\alpha_{n-k} = (-1)^k\, \delta_k\,(v_1,\, v_2,\, .\,.\,.\,, v_n),$$

donde δ_k es un polinomio en $v_1,\, v_2,\, .\,.\,.\,, v_n$. Por ejemplo.

$$\delta_1 = v_1 + v_2 + \cdot\cdot\cdot + v_n, \quad \delta_2 = v_1v_2 + v_1v_3 + \cdot\cdot\cdot + v_{n-1}v_n \ ,\ .\,.\,.\,,\ \delta_n = v_1v_2 \cdots v_n$$

Suponga que $n=2,$ entonces el polinomio se reduce a $f(x) = x^2 + \alpha_1 x^1 + \alpha_0.$

Descomponiendo en factores lineales,

$$x^2+\alpha_1 x^1+\alpha_0=(x-\nu_1)(x-\nu_2).$$

Operando en la derecha,

$$x^2+\alpha_1 x^1+\alpha_0=(x-\nu_1)(x-\nu_2)=x^2+(-\nu_2-\nu_1)x+\nu_1\nu_2.$$

Igualando coeficientes resulta,

$$\alpha_1=-\nu_2-\nu_1 \quad \text{y} \quad \alpha_0=\nu_1\nu_2.$$

Proposición 2.4.8: Sea $\mathbf{A}\subseteq\mathbf{B}$ una extensión de dominios, con $\mathbf{A}$ normal. Si $x\in\mathbf{B}$ es entero sobre un ideal $\mathfrak{a}\subseteq\mathbf{A}$. Entonces x es algebraico sobre el cuerpo de fracciones $\mathbf{k_A}$ y su polinomio minimal sobre $\mathbf{k_A}$ es,

$$t^n+a_{n-1}t^{n-1}+\cdot\cdot\cdot+a_1t+a_0, \qquad \text{con} \quad a_i\in r(\mathfrak{a}).$$

Demostración:

Por hipótesis x es entero sobre $\mathfrak{a}$.

Si $x\in\mathbf{B}$ es entero sobre $\mathfrak{a}$, entonces existe $g(t)$ en $\mathbf{A}[x]$ tal que:

$$g(x)=x^k+a'_{k-1}x^{k-1}+\cdot\cdot\cdot+a'_1x+a'_0=0, \text{ donde } a'_0,\ a'_1,\ .\ .\ .\ ,a'_{n-1}\in\mathfrak{a}. \qquad (1)$$

Como $\mathfrak{a} \subseteq \mathbf{A} \subseteq \mathbf{k}_{\mathbf{A}}$, de la definición 2.4.3, x es algebraico sobre el cuerpo de fracciones $\mathbf{k}_{\mathbf{A}}$.

Denote por $\mathbf{C}$ a la clausura entera de $\mathbf{A}$ en $\mathbf{k}_{\mathbf{A}}$. En consecuencia de 2.3.14, la clausura entera de $\mathfrak{a}$ en $\mathbf{k}_{\mathbf{A}}$ es $r(\mathfrak{a}\mathbf{C})$. Por hipótesis $\mathbf{A}$ es normal, de donde $\mathbf{C} = \mathbf{A}$. Por tanto $r(\mathfrak{a}\mathbf{C}) = r(\mathfrak{a}\mathbf{A}) \subseteq r(\mathfrak{a})$.

De acuerdo con la definición 2.4.5, si x es algebraico sobre $\mathbf{k}_{\mathbf{A}}$, entonces existe un polinomio $f(t) = t^n + b_{n-1}t^{n-1} + \cdot \cdot \cdot + b_1 t + b_0$ mínimo de x sobre $\mathbf{k}_{\mathbf{A}}$, tal que $f(x) = 0$. Se demuestra que los coeficientes de $f(t)$ están contenidos en $r(\mathfrak{a})$.

Sea $\mathbf{L}$ un cuerpo de extensión de $\mathbf{k}_{\mathbf{A}}$, que contenga todos los conjugados $x_1, . . . , x_n$ de x. En consecuencia de la definición 2.4.6, cada x_i con $i = 1, . . . , n$ satisface el mismo polinomio minimal de x sobre $\mathbf{k}_{\mathbf{A}}$, es decir $f(x_i) = 0$ para todo $i = 1, . . . , n$.

Por la **Regla de Ruffini**,

$$b_{n-k} = (-1)^k \delta_k (x_1, x_2, . . . , x_n).$$

Donde δ_k es un polinomio en $x_1, x_2, . . . , x_n$. De (1), x es raíz de $g(t)$, por la minimalidad de $f(t)$ existe $h(t)$ tal que $g(t) = f(t)h(t)$, donde $h(t) \in \mathbf{k}_{\mathbf{A}}[x]$.

Evaluando $g(t)$, en los $x_i, i=1,\ldots,n$:

$$g(x_1)=\cancel{f(x_1)}h(x_1)=0.$$

$$g(x_2)=\cancel{f(x_2)}h(x_2)=0.$$

$$\vdots \qquad\qquad \vdots$$

$$g(x_n)=\cancel{f(x_n)}h(x_n)=0.$$

De lo anterior cada x_i verifica la misma ecuación de dependencia entera que x por tanto x_i es entera sobre $\mathfrak{a}$ para todo $i=1,\ldots,n$. De donde $x_i \in r(\mathfrak{a}\mathbf{C}) \subseteq r(\mathfrak{a})$ y como los b_j, $j=1,\ldots,n-1$, son polinomios en x_i, se deduce que $b_j \in r(\mathfrak{a})$. ■

Definición 2.4.9: Sea $\mathbf{A}$ un anillo y $\{\mathfrak{a}_0, \mathfrak{a}_1, \ldots, \mathfrak{a}_n, \ldots\}$ un conjunto de ideales en $\mathbf{A}$. Una **cadena descendente** de ideales es una expresión de la forma

$$\mathfrak{a}_0 \supseteq \mathfrak{a}_1 \supseteq \cdots \supseteq \mathfrak{a}_n \supseteq \cdots .$$

Proposición 2.4.10: (Teorema del descenso). Sea $\mathbf{A} \subseteq \mathbf{B}$ una extensión entera de dominios con $\mathbf{A}$ normal. Sean $\mathfrak{p}_1 \supseteq \cdots \supseteq \mathfrak{p}_n$ una cadena finita descendente de ideales primos de $\mathbf{A}$ y $\mathfrak{q}_1 \supseteq \cdots \supseteq \mathfrak{q}_m$ una cadena de ideales primos en $\mathbf{B}$ verificando $\mathfrak{q}_i \cap \mathbf{A} = \mathfrak{p}_i$ para $1 \le i \le m < n$.

$$\mathfrak{p}_1 \supseteq \mathfrak{p}_2 \supseteq \ \ldots \ \supseteq \mathfrak{p}_m \supseteq \ \ldots \ \supseteq \mathfrak{p}_n;$$
$$\mathfrak{q}_1 \supseteq \mathfrak{q}_2 \supseteq \ \ldots \ \supseteq \mathfrak{q}_m.$$

Entonces la cadena $\mathfrak{q}_1 \supseteq \mathfrak{q}_2 \supseteq \ldots \supseteq \mathfrak{q}_m$ se puede extender a una cadena $\mathfrak{q}_1 \supseteq \mathfrak{q}_2 \supseteq \ \ldots \ \supseteq \mathfrak{q}_n$ verificando $\mathfrak{q}_i \cap \mathbf{A} = \mathfrak{p}_i,\ 1 \le i \le n.$

Demostración:

Por inducción se reduce al caso $m = 1,\ n = 2.$ Dado que la generalización se obtiene de manera análoga como en el t**eorema del ascenso** aplicando reiteradamente este caso.

Cuando $m = 1,\ n = 2.$ El enunciado del teorema es el siguiente:

**Si $\mathfrak{p}_1,\ \mathfrak{p}_2$ son ideales primos en $\mathbf{A}$ tal que $\mathfrak{p}_1 \supseteq \mathfrak{p}_2,\ \mathfrak{q}_1$ un ideal primo en $\mathbf{B}$ verificando $\mathfrak{q}_1 \cap \mathbf{A} = \mathfrak{p}_1,$ entonces existe un ideal primo $\mathfrak{q}_2$ en $\mathbf{B}$ tal que $\mathfrak{q}_1 \supseteq \mathfrak{q}_2$ y $\mathfrak{q}_2 \cap \mathbf{A} = \mathfrak{p}_2.$ **

Defínanse los conjuntos $\mathbf{S}_1 = \mathbf{A} - \mathfrak{p}_2$ y $\mathbf{S}_2 = \mathbf{B} - \mathfrak{q}_1.$ De la proposición 1.6.1, $\mathbf{S}_1$ y $\mathbf{S}_2$ son sistemas multiplicativos en $\mathbf{A}$ y $\mathbf{B}$, respectivamente.

Considere:

$$\mathbf{S} = \mathbf{S}_1\mathbf{S}_2 = \{ab \in \mathbf{B} \ \mid \ a \in \mathbf{S}_1 \ \text{ y } \ b \in \mathbf{S}_2 \ \}.$$

Se demuestra que $\mathbf{S}$ es un sistema multiplicativo en $\mathbf{B}$.

Para ello se verifica lo siguiente:

(1) $1 \in \mathbf{S}$.

(2) Si $x, y \in \mathbf{S}$, entonces $xy \in \mathbf{S}$.

Demostración (1):

$\mathbf{S}_1$ y $\mathbf{S}_2$ son sitemas multiplicativos $\Rightarrow$ $1_{\mathbf{A}} \in \mathbf{S}_1$ y $1_{\mathbf{B}} \in \mathbf{S}_2$

$\Rightarrow 1_{\mathbf{B}} \in \mathbf{S}$, $\left(\mathbf{B}\right.$ es un anillo de extensión de $\left.\mathbf{A}\right)$.

$\therefore\ 1 \in \mathbf{S}$.

Demostración (2):

Sean $x, y \in \mathbf{S}$.

$x, y \in \mathbf{S} \Rightarrow \exists\ a_1, b_1 \in \mathbf{S}_1$ y $a_2, b_2 \in \mathbf{S}_2$ t. q. $x = a_1 b_1$ y $y = a_2 b_2$

$\Rightarrow xy = (a_1 b_1)(a_2 b_2) = (a_1 a_2)(b_1 b_2)$, donde $a_1 a_1 \in \mathbf{S}_1$ y $b_2 b_2 \in \mathbf{S}_2$

$\Rightarrow xy \in \mathbf{S}$.

$\therefore$ Si $x, y \in \mathbf{S}$, entonces $xy \in \mathbf{S}$.

Luego $\mathbf{S}$ es un sistema multiplicativo en $\mathbf{B}$, que verifica $\mathbf{S}_1 \cup \mathbf{S}_2 \subseteq \mathbf{S}$. Se demuestra que el ideal generado por $\mathfrak{p}_2$ en $\mathbf{B}$ no corta a $\mathbf{S}$. Es decir, $\mathfrak{p}_2 \mathbf{B} \cap \mathbf{S} = \varnothing$.

Supóngase $\mathfrak{p}_2\mathbf{B}\cap \mathrm{S}\neq\varnothing$.

$$\mathfrak{p}_2\mathbf{B}\cap\mathbf{S}\neq\varnothing \quad\Rightarrow\quad \exists \quad x\in\mathfrak{p}_2\mathbf{B}\cap\mathbf{S}$$

$$\Rightarrow \quad x\in\mathfrak{p}_2\mathbf{B} \quad \text{y} \quad x\in\mathbf{S}$$

$$\Rightarrow \quad x\in r\left(\mathfrak{p}_2\mathbf{B}\right) \quad \text{y} \quad x\in\mathbf{S}, \quad \left(\text{Proposición 1.3.3 (i)}\right).$$

Se tiene que $\mathfrak{p}_2$ es un ideal en $\mathbf{A}$, entonces por el lema 2.3.14, la clausura entera de $\mathfrak{p}_2$ en $\mathbf{B}$ es $r\left(\mathfrak{p}_2\mathbf{B}\right)$. Como $x\in r\left(\mathfrak{p}_2\mathbf{B}\right)$, entonces x es entero sobre $\mathfrak{p}_2$. Luego por la proposición 2.4.8, x es algebraico sobre el cuerpo de fracciones $\mathbf{k}_{\mathbf{A}}$ y su polinomio minimal sobre $\mathbf{k}_{\mathbf{A}}$ es;

$$t^r+a_{n-1}t^{r-1}+\cdot\cdot\cdot\cdot+a_1t+a_0;$$

con $a_j\in r\left(\mathfrak{p}_2\right)=\mathfrak{p}_2$ para todo $j=0,\ldots,n-1$. Evaluando el polinomio anterior en x y por ser entero sobre $\mathfrak{p}_2$,

$$x^r+a_{r-1}x^{r-1}+\cdot\cdot\cdot\cdot+a_1x+a_0=0. \qquad (1)$$

Se tiene que $x\in\mathbf{S}$.

$$x\in\mathbf{S} \quad\Rightarrow\quad \exists \quad s_1\in\mathbf{S}_1 \quad \text{y} \quad s_2\in\mathbf{S}_2 \quad \text{t. q.} \quad x=s_1s_2$$

$$\Rightarrow \quad s_1 \in \mathbf{k_A}, \qquad \left(\mathbf{S}_1 \subseteq \mathbf{A} \subseteq \mathbf{k_A}\right)$$

$$\Rightarrow \quad \exists \quad s_1^{-1} \in \mathbf{k_A} \quad \text{t. q. } s_1^{-1} s_1 = 1$$

$$\Rightarrow \quad s_2 = \frac{x}{s_1} \in \mathbf{k_A}.$$

El polinomio minimal para s_2 sobre $\mathbf{k_A}$, se obtiene dividiendo (1) por s_1^r,

$$\frac{x^r}{s_1^r} + \frac{a_{r-1}x^{r-1}}{s_1^r} + \cdot \cdot \cdot \cdot + \frac{a_1 x}{s_1^r} + \frac{a_0}{s_1^r} = 0.$$

Reescribiendo exponente;

$$\left(\frac{x}{s_1}\right)^r + \left(\frac{a_{r-1}}{s_1}\right)\left(\frac{x}{s_1}\right)^{r-1} + \cdot \cdot \cdot \cdot + \left(\frac{a_1}{s_1^{r-1}}\right)\left(\frac{x}{s_1}\right) + \left(\frac{a_0}{s_1^r}\right) = 0.$$

Sustituyendo $s_2 = \dfrac{x}{s_1}$, en la expresión anterior,

$$s_2{}^r + \left(\frac{a_{r-1}}{s_1}\right) s_2{}^{r-1} + \cdot \cdot \cdot \cdot + \left(\frac{a_1}{s_1^{r-1}}\right) s_2 + \left(\frac{a_0}{s_1^r}\right) = 0.$$

Haciendo $v_i = \dfrac{a_i}{s_1^{r-i}}$ con $i = r-1, \ldots, 0$. Resulta:

$$s_2^r + v_{r-1} s_2^{r-1} + \cdot \cdot \cdot \cdot + v_1 s_2 + v_0 = 0. \qquad (2)$$

Para todo $i = r-1, \ldots, 0$ se tiene que $v_i = \dfrac{a_i}{s_1^{r-i}}$. Despejando se deduce:

$$v_i s_1^{r-i} = a_i \in \mathfrak{p}_2, \qquad (0 \leq i \leq r-1). \qquad\qquad (3)$$

$$v_i s_1^{r-i} \in \mathfrak{p}_2 \quad \Rightarrow \quad v_i \in \mathfrak{p}_2 \quad \text{ó} \quad s_1^{r-i} \in \mathfrak{p}_2 \quad \text{para todo} \quad 0 \leq i \leq r-1, \ \left(\mathfrak{p}_2 \text{ es primo en } \mathbf{A}\right)$$

$$\Rightarrow \quad v_i \in \mathfrak{p}_2 \subseteq \mathfrak{p}_1 \quad \text{para todo} \quad 0 \leq i \leq r-1, \qquad \left(s_1 \notin \mathfrak{p}_2\right)$$

$$\Rightarrow \quad s_2^r = -v_{r-1}s_2^{r-1} - \cdot\ \cdot\ \cdot - v_1 s_2 - v_0, \qquad \left(\text{ Despejando en } (2)\right)$$

$$\Rightarrow \quad s_2^r = \sum_{i=1}^{r} -v_{i-1}s_2^{i-1}$$

$$\Rightarrow \quad s_2^r \in \mathbf{B}\,\mathfrak{p}_1 = \mathbf{B}\left(\mathfrak{q}_1 \cap \mathbf{A}\right) \subseteq \mathfrak{q}_1, \quad \left(\text{Proposición 1.3.3 (iv)}\right)$$

$$\Rightarrow \quad s_2 \in \mathfrak{q}_1, \quad (\rightarrow\leftarrow).$$

Luego $\mathfrak{p}_2\,\mathbf{B} \cap \mathbf{S} = \varnothing$.

De la proposición 2.3.10, si $\mathfrak{p}_2\,\mathbf{B} \cap \mathbf{S} = \varnothing$, entonces existe un ideal primo $\mathfrak{q}_2$ en $\mathbf{B}$ tal que $\mathfrak{q}_2 \cap \mathbf{S} = \varnothing$ y $\mathfrak{p}_2\,\mathbf{B} \subseteq \mathfrak{q}_2$. Por la elección de $\mathbf{S}$, $\mathfrak{q}_2 \cap \mathbf{S}_1 = \varnothing$ y $\mathfrak{q}_2 \cap \mathbf{S}_2 = \varnothing$.

Si $\mathfrak{q}_2 \cap \mathbf{S}_2 = \varnothing$, y por la definición de $\mathbf{S}_2$, $\mathfrak{q}_2 \subseteq \mathfrak{q}_1$. De manera análoga si $\mathfrak{q}_2 \cap \mathbf{S}_1 = \varnothing$, entonces $\mathfrak{q}_2 \subseteq \mathfrak{p}_2$. Interceptando $\mathbf{A}$, resulta:

$$\mathfrak{q}_2 \cap \mathbf{A} \subseteq \mathfrak{p}_2 \cap \mathbf{A} \subseteq \mathfrak{p}_2.$$

De nuevo interceptando $\mathbf{A}$, en $\mathfrak{p}_2 \mathbf{B} \subseteq \mathfrak{q}_2$.

$$\mathfrak{p}_2 \mathbf{B} \cap \mathbf{A} \subseteq \mathfrak{q}_2 \cap \mathbf{A}.$$

De la proposición 1.3.3, inciso (iii):

$$\mathfrak{p}_2 \subseteq \mathfrak{p}_2 \mathbf{B} \cap \mathbf{A}.$$

De lo anterior,

$$\mathfrak{p}_2 \subseteq \mathfrak{p}_2 \mathbf{B} \cap \mathbf{A} \subseteq \mathfrak{q}_2 \cap \mathbf{A} \subseteq \mathfrak{p}_2.$$

Por transitividad,

$$\mathfrak{p}_2 \subseteq \mathfrak{q}_2 \cap \mathbf{A} \subseteq \mathfrak{p}_2.$$

Por tanto, $\mathfrak{p}_2 = \mathfrak{q}_2 \cap \mathbf{A}$. Lo que demuestra el teorema. ■

Las proposiciones de las **paginas 185-192,** muestran el comportamiento de las extensiones enteras bajo las operaciones de localización.

Proposición 2.4.11: Sea $\mathbf{A} \subseteq \mathbf{B}$ una extensión entera de anillos y $\mathbf{S}$ un sistema multiplicativo en $\mathbf{A}$, entonces $\mathbf{S}^{-1}\mathbf{A} \subseteq \mathbf{S}^{-1}\mathbf{B}$ es una extensión entera.

Demostración:

Se demuestra lo siguiente:

(1) $\mathbf{S}^{-1}\mathbf{A} \subseteq \mathbf{S}^{-1}\mathbf{B}$ es una extensión de anillos.

(2) $\mathbf{S}^{-1}\mathbf{B}$ es entero sobre $\mathbf{S}^{-1}\mathbf{A}$.

Demostración (1):

Se inyecta $\mathbf{S}^{-1}\mathbf{A}$ en $\mathbf{S}^{-1}\mathbf{B}$ haciendo corresponder al elemento $\frac{a}{s}$ de $\mathbf{S}^{-1}\mathbf{A}$ en el mismo elemento de $\mathbf{S}^{-1}\mathbf{B}$, es decir:

$$\begin{aligned} \iota :\ & \mathbf{S}^{-1}\mathbf{A} \longrightarrow \mathbf{S}^{-1}\mathbf{B} \\ & \frac{a}{s} \longrightarrow \iota\left(\frac{a}{s}\right) = \frac{a}{s}. \end{aligned}$$

La aplicación ι es inyectiva y se considera $\mathbf{S}^{-1}\mathbf{A}$ incluido en $\mathbf{S}^{-1}\mathbf{B}$ vía esta aplicación.

$$\therefore\ \mathbf{S}^{-1}\mathbf{A} \subseteq \mathbf{S}^{-1}\mathbf{B} \text{ es una extensión de anillos.}$$

Demostración (2):

Sea $\dfrac{b}{s} \in \mathbf{S}^{-1}\mathbf{B}$ $\left(b \in \mathbf{B},\ s \in \mathbf{S}\right)$ $\left(b \in \mathbf{B}\ \Rightarrow\ b \text{ es un elemento entero sobre } \mathbf{A}\right)$.

Si $b \in \mathbf{B}$ es entero sobre $\mathbf{A}$, entonces existen $a_0,\ a_1,\ .\ .\ .\ .\ , a_{n-1}$ en $\mathbf{A}$ tal que:

$$b^n + a_{n-1}b^{n-1} + \cdot\ \cdot\ \cdot + a_1 b + a_0 = 0.$$

Si $\mathbf{B}$ un anillo y $\mathbf{S}$ un sistema multiplicativo de $\mathbf{A}$, entonces $0 \in \mathbf{B}$ y $s^n \in \mathbf{S}$. Asi en $\mathbf{S}^{-1}\mathbf{B}$:

$$\frac{b^n + a_{n-1}b^{n-1} + \cdot\ \cdot\ \cdot + a_1 b + a_0}{s^n} = \frac{0}{1}.$$

Sacando factor común $\dfrac{1}{s^n}$ en la expresión anterior, se obtiene:

$$\left(\frac{1}{s^n}\right)\left(\frac{b^n + a_{n-1}b^{n-1} + \cdot\ \cdot\ \cdot + a_1 b + a_0}{1}\right) = \frac{0}{1}.$$

Por definición de suma en anillos de fracciones,

$$\left(\frac{1}{s^n}\right)\left(\frac{b^n}{1} + \frac{a_{n-1}b^{n-1}}{1} + \cdot\ \cdot\ \cdot + \frac{a_1 b}{1} + \frac{a_0}{1}\right) = \frac{0}{1}.$$

Distribuyendo $\dfrac{1}{s^n}$ y asociando,

$$\left(\frac{b}{s}\right)^n + \left(\frac{a_{n-1}}{s}\right)\left(\frac{b}{s}\right)^{n-1} + \cdot\ \cdot\ \cdot + \left(\frac{a_1}{s^{n-1}}\right)\left(\frac{b}{s}\right) + \left(\frac{a_0}{s^n}\right) = \frac{0}{1}.$$

Todo elemento de $\mathbf{S}^{-1}\,\mathbf{B}$ es una solución de una ecuación polinomial unitaria con coeficientes en $\mathbf{S}^{-1}\,\mathbf{A}$, entonces $\mathbf{S}^{-1}\,\mathbf{B}$ es entero sobre $\mathbf{S}^{-1}\,\mathbf{A}$.

$$\therefore\ \mathbf{S}^{-1}\,\mathbf{A} \subseteq \mathbf{S}^{-1}\,\mathbf{B} \text{ es una extensión entera.}\blacksquare$$

Proposición 2.4.12: Cada anillo de fracciones de un dominio normal es un dominio normal.

Demostración: Sea $\mathbf{A}$ un dominio normal y $\mathbf{S}$ un sistema multiplicativo en $\mathbf{A}$. Se demuestra que $\mathbf{S}^{-1}\,\mathbf{A}$ es un dominio.

Sea $\frac{a}{s},\ \frac{b}{t} \in \mathbf{S}^{-1}\,\mathbf{A}$ t. q. $\frac{a}{s}\frac{b}{t} = \frac{0}{1}$.

$$\frac{a}{s}\frac{b}{t} = \frac{0}{1} \quad \Rightarrow \quad (ab, st) \equiv (0, 1)$$

$$\Rightarrow \quad \exists\ h \in \mathbf{S} \quad \text{t. q.} \quad h\big((ab)\cdot 1 - 0\cdot(st)\big) = 0$$

$$\Rightarrow \quad h(ab) = 0$$

$$\Rightarrow \quad h = 0 \quad \text{ó} \quad a = 0 \quad \text{ó} \quad b = 0$$

$$\Rightarrow \quad \frac{a}{s} = \frac{0}{1} \quad \text{ó} \quad \frac{b}{t} = \frac{0}{1}. \qquad\qquad \therefore\ \mathbf{S}^{-1}\,\mathbf{A} \text{ es un dominio.}$$

Se denota por $\mathbf{k}_{\mathbf{A}}$ y $\mathbf{k}_{\mathbf{S}^{-1}\mathbf{A}}$ al cuerpo de fracciones de $\mathbf{A}$ y $\mathbf{S}^{-1}\mathbf{A}$ respectivamente. Sea $\mathbf{C}$ la clausura entera de $\mathbf{A}$ en $\mathbf{k}_{\mathbf{A}}$ y $\mathbf{C}'$ la clausura entera de $\mathbf{S}^{-1}\mathbf{A}$ en $\mathbf{k}_{\mathbf{S}^{-1}\mathbf{A}}$.

Por hipótesis $\mathbf{A}$ es un dominio normal, entonces $\mathbf{C}=\mathbf{A}$ en $\mathbf{k}_{\mathbf{A}}$. Se prueba que $\mathbf{S}^{-1}\mathbf{A}$ es dominio normal; es decir que $\mathbf{C}'=\mathbf{S}^{-1}\mathbf{A}$.

Se verifican los siguientes contenidos:

(1) $\mathbf{C}'\subseteq\mathbf{S}^{-1}\mathbf{A}$.

(2) $\mathbf{C}'\supseteq\mathbf{S}^{-1}\mathbf{A}$.

Demostración (1):

Sea $x\in\mathbf{C}'$, ($x\in\mathbf{C}'$ $\Rightarrow$ es un elemento entero sobre $\mathbf{S}^{-1}\mathbf{A}$.)

Si x es entero sobre $\mathbf{S}^{-1}\mathbf{A}$, entonces existen $\frac{a_0}{t_0}, \frac{a_1}{t_1}, \ldots, \frac{a_{n-1}}{t_{n-1}}$ en $\mathbf{S}^{-1}\mathbf{A}$ tal que

$$x^n+\left(\frac{a_{n-1}}{t_{n-1}}\right)x^{n-1}+\cdots+\left(\frac{a_1}{t_1}\right)x+\left(\frac{a_0}{t_0}\right)=0.$$

Haciendo $t=t_0t_1\cdots t_{n-1}$. Multiplicando por t para quitar denominadores,

$$tx^n+\left(t_0t_1\cdots t_{n-2}a_{n-1}\right)x^{n-1}+\cdots+\left(t_0t_2\cdots t_{n-1}a_1\right)x+\left(t_1t_2\cdots t_{n-1}a_0\right)=0.$$

Multiplicando por t^{n-1},

$$t^{n-1}\left(tx^n\right)+t^{n-1}\left(t_0t_1\cdot\ \cdot\ \cdot t_{n-2}a_{n-1}\right)x^{n-1}+\cdots+t^{n-1}\left(t_0t_2\cdot\ \cdot\ \cdot t_{n-1}a_1\right)x+t^{n-1}\left(t_1t_2\cdot\ \cdot\ \cdot t_{n-1}a_0\right)=0.$$

Asociando:

$$\left(tx\right)^n+\left(t_0t_1\cdot\ \cdot\ \cdot t_{n-2}a_{n-1}\right)\left(tx\right)^{n-1}+\cdots+\left(t^{n-2}t_0t_2\cdot\ \cdot\ \cdot t_{n-1}a_1\right)\left(tx\right)+\left(t_1t_2\cdot\ \cdot\ \cdot t_{n-1}a_0t^{n-1}\right)=0.$$

Luego xt es entero sobre $\mathbf{A}$ es decir $xt\in\mathbf{C}=\mathbf{A}$, entonces:

$$x=\left(\frac{t}{t}\right)\left(\frac{x}{1}\right)=\left(\frac{tx}{t}\right)\in\mathbf{S}^{-1}\,\mathbf{A}.$$

$$\therefore\ \mathbf{C}'\subseteq\mathbf{S}^{-1}\,\mathbf{A}.$$

Demostración (2):

Se tiene que $\mathbf{S}^{-1}\,\mathbf{A}$ es entero sobre sí mismo. De donde por la definición 2.3.4, observación (1), $\mathbf{S}^{-1}\,\mathbf{A}\subseteq\mathbf{C}'$, entonces $\mathbf{S}^{-1}\,\mathbf{A}=\mathbf{C}'$.

$\therefore$ $\mathbf{S}^{-1}\,\mathbf{A}$ en un dominio normal. ■

La siguiente proposición trata la clausura entera en anillos de fracciones.

Proposición 2.4.13: Sea $\mathbf{A} \subseteq \mathbf{B}$ una extensión de anillos, $\mathbf{C}$ la clausura entera de $\mathbf{A}$ en $\mathbf{B}$. Sea $\mathbf{S}$ un sistema multiplicativo de $\mathbf{A}$, entonces $\mathbf{S}^{-1}\mathbf{C}$ es la clausura entera de $\mathbf{S}^{-1}\mathbf{A}$ en $\mathbf{S}^{-1}\mathbf{B}$.

Demostración:

Denote por $\mathbf{C}'$ a la clausura entera de $\mathbf{S}^{-1}\mathbf{A}$ en $\mathbf{S}^{-1}\mathbf{B}$. Se demuestra que $\mathbf{S}^{-1}\mathbf{C} = \mathbf{C}'$.

Verifique lo siguiente:

(1) $\mathbf{C}' \subseteq \mathbf{S}^{-1}\mathbf{C}$.

(2) $\mathbf{C}' \supseteq \mathbf{S}^{-1}\mathbf{C}$.

Demostración (1):

Sea $\frac{b}{s} \in \mathbf{C}'$, ($\frac{b}{s} \in \mathbf{C}' \Rightarrow \frac{b}{s}$ es un elemento entero sobre $\mathbf{S}^{-1}\mathbf{A}$).

Si $\frac{b}{s}$ es entero sobre $\mathbf{S}^{-1}\mathbf{A}$, entonces existen a_i en $\mathbf{A}$ y t_i en $\mathbf{S}$ para todo $i = 1, \dots, n-1$ tal que

$$\left(\frac{b}{s}\right)^n + \left(\frac{a_{n-1}}{t_{n-1}}\right)\left(\frac{b}{s}\right)^{n-1} + \cdot \cdot \cdot + \left(\frac{a_1}{t_1}\right)\left(\frac{b}{s}\right) + \left(\frac{a_0}{t_0}\right) = 0.$$

Sea $t = t_0 t_1 \cdot \cdot \cdot t_{n-1}$. Multiplicando por $(st)^n$ la ecuación anterior se obtiene:

$$(st)^n\left(\frac{b}{s}\right)^n+(st)^n\left(\frac{a_{n-1}}{t_{n-1}}\right)\left(\frac{b}{s}\right)^{n-1}+\cdot\cdot\cdot+(st)^n\left(\frac{a_1}{t_1}\right)\left(\frac{b}{s}\right)+(st)^n\left(\frac{a_0}{t_0}\right)=0.$$

Asociando tb,

$$(bt)^n+(st)\left(\frac{a_{n-1}}{t_{n-1}}\right)(bt)^{n-1}+\cdot\cdot\cdot+(st)^{n-1}\left(\frac{a_1}{t_1}\right)(bt)+(st)^n\left(\frac{a_0}{t_0}\right)=0.$$

Eliminando denominadores,

$$(bt)^n+(st_0\cdots t_{n-2}a_{n-1})(bt)^{n-1}+\cdot\cdot\cdot+(st_0t_1\cdots t_{n-1})^{n-2}(st_0\cdots t_{n-1}a_1)(bt)$$

$$+(st_0t_1\cdots t_{n-1})^{n-1}(st_1\cdots t_{n-1}a_0)=0.$$

Luego tb, es solución de una ecuación polinomial unitaria con coeficientes en $\mathbf{A}$. Así tb es entero sobre $\mathbf{A}$.

$(tb$ es entero sobre $\mathbf{A}) \Rightarrow (tb\in\mathbf{C})$

$$\Rightarrow\left(\frac{b}{s}=\left(\frac{t}{t}\right)\left(\frac{b}{s}\right)=\left(\frac{tb}{ts}\right)\in\mathbf{S}^{-1}\,\mathbf{C}\right)$$

$$\Rightarrow\left(\frac{b}{s}\in\mathbf{S}^{-1}\,\mathbf{C}\right).$$

$$\therefore\ \mathbf{C}'\subseteq\mathbf{S}^{-1}\,\mathbf{C}.$$

Demostración (2):

Se consideran las cadenas de extensiones de anillos:

$$\mathbf{A} \subseteq \mathbf{C} \subseteq \mathbf{B} \qquad \text{y} \qquad \mathbf{S}^{-1}\mathbf{A} \subseteq \mathbf{S}^{-1}\mathbf{C} \subseteq \mathbf{S}^{-1}\mathbf{B}.$$

Como $\mathbf{A} \subseteq \mathbf{C}$ es una extensión entera y por la proposición 2.4.11, $\mathbf{S}^{-1}\mathbf{A} \subseteq \mathbf{S}^{-1}\mathbf{C}$ es una extensión entera, esto demuestra que $\mathbf{S}^{-1}\mathbf{C} \subseteq \mathbf{C}'$.

$$\therefore\ \mathbf{S}^{-1}\mathbf{C} \subseteq \mathbf{C}'.$$

Se ha demostrado que cada conjunto es subconjunto del otro, entonces $\mathbf{C}' = \mathbf{S}^{-1}\mathbf{C}$. ■

CAPITULO III: ANILLOS DE CADENAS.

Este capítulo tiene como propósitos principales el estudio de anillos que satisfacen la condición de cadena ascendente (**Noetherianos)** y descendente (**Artinianos**) en ideales.

3.1: Anillos Noetherianos: Primeras propiedades de finitud.

Se inicia introduciendo el concepto de dimensión de Krull de un anillo, estando especialmente interesados en aquellos anillos que tienen una dimensión de Krull igual a cero. Luego se define la estructura de los anillos noetherianos y algunas de sus propiedades.

Definición 3.1.1: Sea $\mathbf{A} \neq \mathbf{0}$ un anillo. Dada una cadena finita de ideales primos:

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n, \qquad \left(\text{inclusiones en sentido estricto}\right).$$

La **longitud** de la cadena es n (el número de eslabones). Se define la **dimensión** de $\mathbf{A}$ como el supremo de las longitudes de todas las cadenas de ideales primos de $\mathbf{A}$. Se denota por $\dim(\mathbf{A})$.

Definición 3.1.2: Si $\mathfrak{p}$ es un ideal primo de $\mathbf{A}$, se define la **altura** de $\mathfrak{p}$ como el supremo de las longitudes de las cadenas de ideales primos del siguiente tipo:

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n = \mathfrak{p}.$$

La altura del ideal $\mathfrak{p}$ se representa por $\mathrm{ht}(\mathfrak{p})$.

Como consecuencia,

$$\dim(\mathbf{A}) = \operatorname{Sup}\{\operatorname{ht}(\mathfrak{p}) \ : \ \mathfrak{p} \text{ es un ideal primo en } \mathbf{A}\}.$$

Observación:

1. Sea $\mathbf{A}$ un anillo. Si $\dim(\mathbf{A}) = 0,$ entonces los ideales primos son maximales.
2. Si $\mathbf{A}$ es un dominio con $\dim(\mathbf{A}) = 0,$ resulta que $\mathbf{0}$ es un ideal maximal, luego los dominios de dimensión 0 son los cuerpos.

Proposición 3.1.3: Para cada anillo $\mathbf{A}$, se verifica:

(i) $\operatorname{ht}(\mathfrak{p}) = \dim(\mathbf{A}_{\mathfrak{p}})$ donde $\mathfrak{p}$ es un ideal primo de $\mathbf{A}$.

(ii) $\dim(\mathbf{A}) = \sup\{\dim(\mathbf{A}_{\mathfrak{p}}) \mid \mathfrak{p} \text{ es un ideal primo de } \mathbf{A}\}.$

Demostración (i):

Dado $\mathfrak{p}$ un ideal primo de $\mathbf{A}$. Se supone que $\operatorname{ht}(\mathfrak{p}) = k$ con $k \in \mathbb{N}.$

Si $\operatorname{ht}(\mathfrak{p}) = k,$ entonces existen $\{\mathfrak{p}_0, \mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$ ideales primos en $\mathbf{A}$ tal que:

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_{k-1} \subsetneq \mathfrak{p}_k = \mathfrak{p}.$$

En consecuencia del corolario 1.7.5,

$$\mathbf{S}^{-1}\,\mathfrak{p}_0 \subsetneq \mathbf{S}^{-1}\,\mathfrak{p}_1 \subsetneq \;\cdot\;\cdot\;\cdot\; \subsetneq \mathbf{S}^{-1}\,\mathfrak{p}_{k-1} \subsetneq \mathbf{S}^{-1}\,\mathfrak{p}_k = \mathbf{S}^{-1}\,\mathfrak{p},$$

es una cadena estricta de ideales primos en $\mathbf{A}_{\mathfrak{p}}$. Se demuestra que $\operatorname{ht}\left(\mathbf{S}^{-1}\,\mathfrak{p}\right) = k.$ Supóngase que existe una cadena de ideales primos en $\mathbf{A}_{\mathfrak{p}}$, con más ideales que la cadena anterior. Por la proposición 1.7.1,

$$\mathbf{S}^{-1}\,\mathfrak{p}'_0 \subsetneq \mathbf{S}^{-1}\,\mathfrak{p}'_1 \subsetneq \;\cdot\;\cdot\;\cdot\; \subsetneq \mathbf{S}^{-1}\,\mathfrak{p}'_{h-1} \subsetneq \mathbf{S}^{-1}\,\mathfrak{p}'_h = \mathbf{S}^{-1}\,\mathfrak{p},$$

con $\mathfrak{p}'_j$ ideales en $\mathbf{A}$, para todo $j = 1, \ldots, h$ y $h \geq k$. De acuerdo con el corolario 1.7.5:

$$\mathfrak{p}'_0 \subsetneq \mathfrak{p}'_1 \subsetneq \;\cdot\;\cdot\;\cdot\; \subsetneq \mathfrak{p}'_{h-1} \subsetneq \mathfrak{p}'_h = \mathfrak{p}, \quad \text{donde } h \geq k.$$

Es una cadena estricta de ideales primos en $\mathbf{A}$. Lo que contradice que la $\operatorname{ht}(\mathfrak{p}) = k.$ De donde $\operatorname{ht}\left(\mathbf{S}^{-1}\,\mathfrak{p}\right) = k.$

Por la definición 3.1.2, $\dim\left(\mathbf{A}_{\mathfrak{p}}\right) = k.$

$$\therefore\;\; \operatorname{ht}(\mathfrak{p}) = \dim\left(\mathbf{A}_{\mathfrak{p}}\right).$$

Demostración (ii):

Sea $\mathfrak{p}$ un ideal primo en $\mathbf{A}$.

Del inciso (i),

$$\operatorname{ht}(\mathfrak{p}) = \dim(\mathbf{A}_{\mathfrak{p}}).$$

En consecuencia de la definición, 3.1.2:

$$\dim(\mathbf{A}) = \operatorname{Sup}\left\{\operatorname{ht}(\mathfrak{p}) \ : \ \mathfrak{p} \text{ es un ideal primo en } \mathbf{A}\right\}.$$

Sustituyendo lo anterior,

$$\dim(\mathbf{A}) = \operatorname{Sup}\left\{\dim(\mathbf{A}_{\mathfrak{p}}) \ : \ \mathfrak{p} \text{ es un ideal primo en } \mathbf{A}\right\}. \ \blacksquare$$

Definición 3.1.4: Un anillo $\mathbf{A}$ verifica la condición **maximal**, si toda familia no vacía de ideales, ordenadas por la inclusión, tiene elemento maximal.

Definición 3.1.5: Un anillo $\mathbf{A}$, se dice que es **noetheriano** si verifica la **condición de cadena ascendente** en ideales. Más explícitamente: Para toda cadena ascendente de ideales en $\mathbf{A}$,

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots \subseteq \mathfrak{a}_m \subseteq \mathfrak{a}_{m+1} \subseteq \cdots .$$

Existe $m \in \mathbb{N}$ tal que $\mathfrak{a}_m = \mathfrak{a}_{m+1} = \mathfrak{a}_{m+2} = \cdots$.

El siguiente resultado muestra la equivalencia de las definiciones 3.1.4 y 3.1.5.

Teorema 3.1.6: Sea $\mathbf{A}$ un anillo. Los siguientes enunciados son equivalentes:

(i) $\mathbf{A}$ es noetheriano.

(ii) Todo familia no vacía de ideales en $\mathbf{A}$ tiene un elemento maximal.

(iii) Todo ideal de $\mathbf{A}$ es finitamente generado.

Demostración:

$(i) \Rightarrow (ii)$.

Se demuestra que si $\mathbf{A}$ es noetheriano, entonces toda familia no vacía de ideales en $\mathbf{A}$ tiene elemento maximal.

Dada Γ una familia de ideales en $\mathbf{A}$ tal que $\Gamma \neq \varnothing$. Sé supone que Γ no tiene elemento maximal.

Sea $\mathfrak{a}_1 \in \Gamma$.

Γ no tiene elemento maximal, entonces existe un ideal $\mathfrak{a}_2 \in \Gamma$ tal que,

$$\mathfrak{a}_1 \subsetneq \mathfrak{a}_2.$$

Puesto que $\mathfrak{a}_2$ no es maximal, existe un ideal $\mathfrak{a}_3 \in \Gamma$ tal que,

$$\mathfrak{a}_1 \subsetneq \mathfrak{a}_2 \subsetneq \mathfrak{a}_3.$$

Sucesivamente para cada índice j se tiene que $\mathfrak{a}_j$ no es maximal, entonces existe $\mathfrak{a}_{j+1} \in \Gamma$ tal que:

$$\mathfrak{a}_1 \subsetneq \mathfrak{a}_2 \subsetneq \mathfrak{a}_3 \cdot \cdot \cdot \subsetneq \mathfrak{a}_j \subsetneq \mathfrak{a}_{j+1} \subsetneq \cdot \cdot \cdot .$$

Luego se ha construido una cadena ascendente de ideales en $\mathbf{A}$, que no es estacionaria, lo que contradice la hipótesis.

$$\therefore \ \Gamma \text{ tiene elemento maximal.}$$

$(ii) \Rightarrow (iii)$.

(Toda familia no vacía de ideales en $\mathbf{A}$ tiene un elemento maximal) $\Rightarrow$ (Todo ideal en $\mathbf{A}$ es finitamente generado).

Sea $\mathfrak{b}$ un ideal y se considera la familia de ideales en $\mathbf{A}$ definida como sigue:

$$\Gamma = \{ \mathfrak{a}' \subseteq \mathbf{A} \mid \ \mathfrak{a}' \text{ es un ideal finitamente generado, tal que } \mathfrak{a}' \subseteq \mathfrak{b} \}.$$

Como $0 \in \Gamma$ se tiene $\Gamma \neq \varnothing$, por hipótesis Γ tiene elemento maximal. Sea $\mathfrak{a}$ maximal. Se supone que $\mathfrak{a} \subsetneq \mathfrak{b}$ y sea $\{ x_1 , \ldots , x_n \}$ un conjunto de generadores de $\mathfrak{a}$. Entonces:

$$\mathfrak{a} = \langle x_1 , \ldots , x_n \rangle .$$

Si $\mathfrak{a} \subsetneq \mathfrak{b}$, entonces existe $x \in \mathbf{A}$, tal que $x \in \mathfrak{b} - \mathfrak{a}$.

Considere el ideal $\mathfrak{b}' = \langle x_1 \ , \ . \ . \ . \ , x_n \rangle + x\mathbf{A}$, el cual es un ideal finitamente generado que contiene a $\mathfrak{a}$ estrictamente, por tanto

$$\mathfrak{a} \subsetneq \mathfrak{b}' = \langle x_1 \ , \ . \ . \ . \ , \ x_n \rangle + x\mathbf{A} \subseteq \mathfrak{b}.$$

Lo cual contradice la maximalidad de $\mathfrak{a}$. Luego $\mathfrak{a} = \mathfrak{b}$ y es finitamente generado.

$\therefore$ Todo ideal en $\mathbf{A}$ es finitamente generado.

$(iii) \Rightarrow (i)$.

(Todo ideal en $\mathbf{A}$ es finitamente generado) $\Rightarrow$ ($\mathbf{A}$ es noetheriano).

Sea $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \ . \ . \ . \ \subseteq \mathfrak{a}_n \subseteq \ . \ . \ .$ una cadena ascendente de ideales en $\mathbf{A}$. Considere el conjunto,

$$\mathfrak{a} = \bigcup_{i=0}^{\infty} \mathfrak{a}_i.$$

De acuerdo con la proposición 2.3.9, $\mathfrak{a}$ es un ideal de $\mathbf{A}$; por tanto ha de ser de generación finita. Sea $\{x_1, \ . \ . \ . \ , x_s\}$ un conjunto de generadores de $\mathfrak{a}$, es decir;

$$\mathfrak{a} = \langle x_1, \ . \ . \ . \ , x_s \rangle.$$

Para cada x_k $1 \leq k \leq s$, existe $n_k \in \mathbb{N}$ tal que $x_k \in \mathfrak{a}_{n_k}$. Sea $n = \max\{n_1, n_2, \ . \ . \ . \ , n_s\}$; como los $\mathfrak{a}_i$ forman una cadena ascendente de ideales, entonces los $x_k \in \mathfrak{a}_n$ para todo

$1 \leq k \leq s.$ De donde:

$$\langle x_1 \ , \ . \ . \ . \ , x_s \rangle = \mathfrak{a} \subseteq \mathfrak{a}_n \subseteq \mathfrak{a}_{n+1} \subseteq \mathfrak{a}_{n+2} \subseteq \ . \ . \ . \ \subseteq \bigcup_{i=0}^{\infty} \mathfrak{a}_i = \mathfrak{a}.$$

Luego todas las inclusiones son iguales y la cadena ascendente se estaciona. Por tanto $\mathbf{A}$ es un anillo noetheriano. ■

Proposición 3.1.7: Sea $\mathbf{A}$ un anillo noetheriano, $\mathfrak{a}$ un ideal de $\mathbf{A}$. Entonces $\mathbf{A}/\mathfrak{a}$ es un anillo noetheriano.

Demostración:

Dada $\overline{\mathfrak{a}}_1 \subseteq \overline{\mathfrak{a}}_2 \subseteq \ . \ . \ . \ \subseteq \overline{\mathfrak{a}}_n \subseteq \overline{\mathfrak{a}}_{n+1} \subseteq \ . \ . \ .$ una cadena ascendente de ideales en $\mathbf{A}/\mathfrak{a}$. Considérese $\pi : \mathbf{A} \to \mathbf{A}/\mathfrak{a} \quad a \to \overline{a}$ el homomorfismo de paso al cociente y la correspondencia biunívoca dada en la proposición 1.1.14:

$$\left\{ \begin{array}{c} \text{Ideales de } \mathbf{A} \text{ que} \\ \text{contienen a } \mathfrak{a} \end{array} \right\} \leftrightarrow \left\{ \text{ Ideales de } \mathbf{A}/\mathfrak{a} \right\}.$$

Observe el diagrama siguiente:

$$\begin{array}{ccccccccccc} \overline{\mathfrak{a}}_1 & \subseteq & \overline{\mathfrak{a}}_2 & \subseteq & . \ . \ . & \subseteq & \overline{\mathfrak{a}}_n & \subseteq & \overline{\mathfrak{a}}_{n+1} & \subseteq & . \ . \ . \\ \updownarrow & & \updownarrow & & & & \updownarrow & & \updownarrow & & . \\ \mathfrak{a}_1 & \subseteq & \mathfrak{a}_2 & \subseteq & . \ . \ . & \subseteq & \mathfrak{a}_n & \subseteq & \mathfrak{a}_{n+1} & \subseteq & . \ . \ . \end{array}$$

La fila inferior es una cadena ascendente de ideales en $\mathbf{A}$ la cual se estaciona, entonces la cadena superior también se estaciona. Luego por la definición 3.1.5, $\mathbf{A}/\mathfrak{a}$ es un anillo noetheriano. ■

Corolario 3.1.8: Sea $\mathbf{A}$ un anillo noetheriano, $f:\mathbf{A}\to\mathbf{B}$ un homomorfismo sobreyectivo de anillos, entonces $\mathbf{B}$ es noetheriano.

Demostración:

De la proposición 1.1.13, existe un isomorfismo de anillos de $\mathbf{A}/\mathbf{ker}(f)$ en $\mathbf{Im}(f)$ es decir:

$$\mathbf{A}/\mathbf{ker}(f)\cong\mathbf{Im}(f)=\mathbf{B}.$$

En consecuencia de la proposición 3.1.7, $\mathbf{A}/\mathbf{ker}(f)$ es un anillo noetheriano, entonces $\mathbf{B}$ es un anillo de noetheriano.■

Proposición 3.1.9: Si $\mathbf{A}$ es un anillo noetheriano y $\mathbf{S}$ un sistema multiplicativo de $\mathbf{A}$, entonces $\mathbf{S}^{-1}\mathbf{A}$ es noetheriano.

Demostración:

Sea $\mathfrak{b}$ un ideal en $\mathbf{S}^{-1}\mathbf{A}$. Se demuestra que $\mathfrak{b}$ es finitamente generado.

De la proposición 1.7.1, si $\mathfrak{b}$ es un ideal en $\mathbf{S}^{-1}\mathbf{A}$, entonces existe un ideal $\mathfrak{a}$ en $\mathbf{A}$, tal que:

$$\mathbf{S}^{-1}\mathfrak{a} = \mathfrak{b}.$$

Todo ideal en $\mathbf{A}$ es finitamente generado. Sea $\{x_1, \ldots, x_n\}$ un conjunto finito de generadores de $\mathfrak{a}$. Por la proposición 1.6.7, $\left\{\frac{x_1}{1}, \ldots, \frac{x_n}{1}\right\}$ es un conjunto finito de generadores de $\mathbf{S}^{-1}\mathfrak{a}$. Así todo ideal en $\mathbf{S}^{-1}\mathbf{A}$ es finito generado, entonces $\mathbf{S}^{-1}\mathbf{A}$ es noetheriano de acuerdo con 3.1.6.■

Corolario 3.1.10: Si $\mathbf{A}$ es un anillo noetheriano y $\mathfrak{p}$ un ideal primo de $\mathbf{A}$, entonces $\mathbf{A}_{\mathfrak{p}}$ es noetheriano.

Demostración:

De la proposición 1.6.1, si $\mathfrak{p}$ es un ideal primo de $\mathbf{A}$, entonces $\mathbf{S} = \mathbf{A} - \mathfrak{p}$ es un sistema multiplicativo en $\mathbf{A}$. Luego por el teorema anterior $\mathbf{A}_{\mathfrak{p}}$ es noetheriano.■

El teorema de Hilbert que se estudiará a continuación es sin duda uno de los teoremas muy importantes del álgebra conmutativa. El **teorema de la base de Hilbert** se puede considerar como una forma de construir anillos noetherianos.

Proposición 3.1.11 (Teorema de la base de Hilbert): Si $\mathbf{A}$ es un anillo noetheriano, entonces el anillo de polinomios $\mathbf{A}[x]$ es un anillo noetheriano.

Demostración:

De acuerdo con la proposición 3.1.6, sólo es necesario mostrar que todo ideal $\mathbf{J}$ de $\mathbf{A}[x]$ es finitamente generado. La prueba se divide en dos pasos:

Paso 1:

Considere el conjunto:

$\mathbf{I}_n = \{a \in \mathbf{A} \mid a = 0 \;\; \text{ó} \;\; a$ es el coeficiente principal de un polinomio $f \in \mathbf{J}$ de grado $n\}$.

Se demuestra que $\mathbf{I}_n$ es un ideal en $\mathbf{A}$. Para ello se verifica lo siguiente:

(1) Si $a, b \in \mathbf{I}_n$, entonces $a + b \in \mathbf{I}_n$.

(2) Si $a \in \mathbf{I}_n$, entonces $ab \in \mathbf{I}_n$ para todo $b \in \mathbf{A}$.

Demostración (1):

Sean $a, b \in \mathbf{I}_n$. Se tienen los siguientes casos:

Caso 1: Si $a = 0$ ó $b = 0$.

$$a = 0 \;\text{ ó }\; b = 0 \;\Rightarrow\; a + b = 0 + b = b \in \mathbf{I}_n \quad \text{ó} \quad a + b = a + 0 = a \in \mathbf{I}_n.$$

Caso 2: Si $a \neq 0$ y $b \neq 0$.

Si $a \neq 0$ y $b \neq 0$, entonces a es el coeficiente principal de $f \in \mathbf{J}$ y b es el coeficiente principal de $g \in \mathbf{J}$, donde $\text{grd}(f) = \text{grd}(g) = n$. Como $\mathbf{J}$ es un ideal en $\mathbf{A}[x]$, entonces $f + g \in \mathbf{J}$ tal que $\text{grd}(f + g) \leq n$. Por tanto,

$$\text{grd}(f + g) = n \quad \Rightarrow \; a + b \neq 0$$

$$\Rightarrow \; a + b \text{ es el coeficiente principal de } f + g$$

$$\Rightarrow \; a + b \in \mathbf{I}_n.$$

$$\text{grd}(f + g) < n \quad \Rightarrow \; a + b = 0 \in \mathbf{I}_n.$$

En cualquiera de los casos se obtiene $a + b \in \mathbf{I}_n$.

$$\therefore \text{ Si } a, b \in \mathbf{I}_n, \text{ entonces } a + b \in \mathbf{I}_n.$$

Demostración (2):

Sea $a \in \mathbf{A}$ y $b \in \mathbf{I}_n$. De nuevo se tienen los casos siguientes:

Caso 1: $a = 0$ ó $b = 0$.

$$a = 0 \text{ ó } b = 0 \quad \Rightarrow \quad ab = 0 \in \mathbf{I}_n.$$

Caso 2: $a \neq 0$ y $b \neq 0$.

$b \neq 0 \;\; \Rightarrow \;\; b$ es el coeficiente principal de $f \in \mathbf{J}$ tal que $\operatorname{grd}(f) = n$

$\Rightarrow \;\; af \in \mathbf{J}$, donde $\operatorname{grd}(af) = n \qquad (a \neq 0)$

$\Rightarrow \;\; ab$ es el coeficiente principal de $af \in \mathbf{J}$

$\Rightarrow \;\; ab \in \mathbf{I}_n$.

Luego en cualquiera de los casos $ab \in \mathbf{I}_n$.

$$\therefore \; \mathbf{I}_n \text{ es un ideal en } \mathbf{A}.$$

Si a es un elemento no nulo de $\mathbf{I}_n$ y f es un polinomio en $\mathbf{A}[x]$ tal que $f \in \mathbf{J}$ de grado n con coeficiente principal a, entonces a es también coeficiente principal de xf que es un polinomio que pertenece a $\mathbf{J}$ de grado $n+1$. Se tiene una cadena ascendente de ideales en $\mathbf{A}$.

$$\mathbf{I}_0 \subseteq \mathbf{I}_1 \subseteq \;\cdot\;\cdot\;\cdot\; \subseteq \mathbf{I}_n \subseteq \mathbf{I}_{n+1} \subseteq \;\cdot\;\cdot\;\cdot\;\cdot\,.$$

Como $\mathbf{A}$ es un anillo noetheriano, existe $t \in \mathbb{N}$ tal que $\mathbf{I}_n = \mathbf{I}_t \;\; \forall\, n \geq t$; más aún por la proposición 3.1.6, cada $\mathbf{I}_n$ es finitamente generado. Sea $\left\{a_{n_1}, a_{n_2}, \ldots, a_{n_{i_n}}\right\}$ un conjunto finito de generadores de $\mathbf{I}_n$ es decir; $\mathbf{I}_n = \left\langle a_{n_1}, a_{n_2}, \ldots, a_{n_{i_n}} \right\rangle$.

De la definición de $\mathbf{I}_n$ para cada $a_{n_j} \in \mathbf{I}_n$, donde $0 \leq n \leq t,\ 1 \leq j \leq i_n$; existe un polinomio $f_{n_j} \in \mathbf{J}$ de grado n con coeficiente principal a_{n_j}.

Paso 2:

Se demuestra que el ideal $\mathbf{J}$ de $\mathbf{A}[x]$ está generado por el conjunto finito de polinomios:

$$\mathbf{X} = \left\{ f_{n_j} \in \mathbf{J} \mid 0 \leq n \leq t,\ 1 \leq j \leq i_n \right\}.$$

Sea $f \in (\mathbf{X})$.

$$\left(f \in (\mathbf{X})\right) \Rightarrow \left(f = \sum_{j=1}^{i_n} h_j f_{n_j},\ \text{ donde } 0 \leq n \leq t \quad \text{y} \quad h_j \in \mathbf{A}[x] \right).$$

$$\left(f_{n_j} \in \mathbf{J} \quad \text{y} \quad h_j \in \mathbf{A}[x]\right) \Rightarrow \left(h_j f_{n_j} \in \mathbf{J} \text{ para } 0 \leq n \leq t,\ 1 \leq j \leq i_n\right), \left(\mathbf{J} \text{ es ideal en } \mathbf{A}[x]\right)$$

$$\Rightarrow \left(f = \sum_{j=1}^{i_n} h_j f_{n_j} \in \mathbf{J} \right), \qquad \left(\mathbf{J} \text{ es ideal en } \mathbf{A}[x]\right)$$

$$\Rightarrow \left(f \in \mathbf{J}\right). \qquad\qquad \therefore\ (\mathbf{X}) \subseteq \mathbf{J}.$$

Para la otra inclusión se sigue por inducción sobre n.

- Suponga $n = 0$.

Si $n = 0$, se observa que $f_{0_j} = a_{0_j} \in \mathbf{I}_0 \subseteq \mathbf{A} \subseteq \mathbf{A}[x]$ para todo $0 \le j \le i_n$. Sea $g \in \mathbf{J}$ un polinomio de $\operatorname{grd}(g) = 0$. Si $\operatorname{grd}(g) = 0$, entonces $g = b_0 \in \mathbf{A}$. De donde $g \in \mathbf{I}_0$ y por tanto; g es una combinación lineal de los f_{0_j}. Luego los polinomios de grado cero en $\mathbf{J}$ están contenidos en $(\mathbf{X})$.

- (**Hipótesis inductiva**). Suponga que el resultado se verifica para $n-1$. Es decir, se asume $(\mathbf{X})$ contiene todos los polinomios de $\mathbf{J}$ de grado menor o igual que $n-1$.
- Se demuestra que $(\mathbf{X})$ contiene los polinomios de $\mathbf{J}$ con grado n.

Sea $g \in \mathbf{J}$ con $\operatorname{grd}(g) = n$ y coeficiente principal $r \ne 0 \in \mathbf{A}$. Se consideran los siguientes casos:

Caso I: Cuando $n \le t$.

Si $n \le t$, entonces $r \in \mathbf{I}_n$. Luego si $r \in \mathbf{I}_n$, existen $k_1, k_2, \ldots, k_{i_n}$ en $\mathbf{A}$ tal que

$$r = a_{n_1} k_1 + a_{n_2} k_2 + \cdots + a_{n_{i_n}} k_{i_n}.$$

Entonces el polinomio.

$$h = \sum_{j=1}^{i_n} k_j f_{n_j} = k_1 f_{n_1} + k_2 f_{n_2} + \cdots + k_{i_n} f_{n_{i_n}}$$

$$= k_1 \left(a_{n_1} x^n + \cdots \right) + k_2 \left(a_{n_2} x^n + \cdots \right) + \cdots + k_{i_n} \left(a_{n_{i_n}} x^n + \cdots \right)$$

$$=\left(k_1 a_{n_1}+a_{n_2}k_2+\ \cdot\ \cdot\ \cdot\ +a_{n_{i_n}}k_{i_n}\right)x^n+\ \cdot\ \cdot\ \cdot$$

$$=rx^n+\ \cdot\ \cdot\ \cdot\ .$$

Por definición de h se tiene que $h\in(\mathbf{X})$ con coeficiente principal r y $\operatorname{grd}(h)=n.$ En consecuencia:

$$g-h=g-\sum_{j=1}^{i_n}k_j f_{n_j}=\left(rx^n+d_{n-1}x^{n-1}+\ \cdot\ \cdot\ \cdot\right)-\left(rx^n+l_{n-1}x^{n-1}+\ \cdot\ \cdot\ \cdot\ \right)$$

$$=\left(d_{n-1}-l_{n-1}\right)x^{n-1}+\ \cdot\ \cdot\ \cdot\ .$$

Donde $\operatorname{grd}(g-h)\leq n-1.$ Por hipótesis inductiva $g-h\in(\mathbf{X}),$ pero $h\in(\mathbf{X})$ por tanto $g\in(\mathbf{X}).$

Caso II: Cuando $n\geq t.$

Si $n\geq t$ entonces $r\in\mathbf{I}_n=\mathbf{I}_t$. Luego existen $k_1,k_2\ ,\ \ldots,k_{i_t}$ en $\mathbf{A}$ tal que:

$$r=a_{t_1}k_1+a_{t_2}k_2+\ \cdot\ \cdot\ \cdot\ +a_{t_{i_t}}k_{i_t}$$

Considere el polinomio, construido de la marera siguiente,

$$h=\sum_{j=1}^{i_t}k_j x^{n-t}f_{t_j}=k_1x^{n-t}f_{t_1}+k_2x^{n-t}f_{t_2}+\ \cdot\ \cdot\ \cdot\ +k_{i_t}x^{n-t}f_{t_{i_t}}.$$

$$= k_1 x^{n-t}\left(a_{t_1} x^t + \cdots\right) + k_2 x^{n-t}\left(a_{t_2} x^t + \cdots\right) + \cdots + k_{i_t} x^{n-t}\left(a_{t_{i_t}} x^t + \cdots\right)$$

$$= \left(a_{t_1} k_1 x^n + \cdots\right) + \left(a_{t_2} k_2 x^n + \cdots\right) + \cdots + \left(a_{t_{i_t}} k_{i_t} x^n + \cdots\right)$$

$$= \left(k_1 a_{t_1} + k_2 a_{t_2} + \cdots + a_{t_{i_t}} k_{i_t}\right) x^n + \cdots$$

$$= r x^n + \cdots.$$

Luego $h \in \mathbf{(X)}$ con coeficiente principal r y $\operatorname{grd}(h) = n.$ En consecuencia:

$$g - h = g - \sum_{j=1}^{i_t} k_j x^{n-t} f_{t_j} = \left(r x^n + u x^{n-1} + \cdots\right) - \left(r x^n + v x^{n-1} + \cdots\right)$$

$$= (u - v) x^{n-1} + \cdots.$$

Donde $\operatorname{grd}(g-h) \leq n-1$. Por hipótesis inductiva, $g - h \in \mathbf{(X)}$, pero $h \in \mathbf{(X)}$, por tanto $g \in \mathbf{(X)}$. Luego la inducción está completa. Por tanto $\mathbf{J} \subseteq (\mathbf{X})$, así $\mathbf{J} = (\mathbf{X})$. ■

Observación:

El recíproco del teorema de la base de Hilbert es una consecuencia inmediata del corolario 3.1.8, considerando el homomorfismo sobreyectivo del anillo de polinomios $\mathbf{A}[x]$ hacia el anillo $\mathbf{A}$.

La siguiente propiedad es la generalización del teorema de la base de Hilbert a un anillo de polinomios $\mathbf{A}[x_1, \ldots, x_n]$ de varias indeterminadas.

Corolario 3.1.12: Si $\mathbf{A}$ es un anillo noetheriano, entonces el anillo de polinomios $\mathbf{A}[x_1, \ldots, x_n]$ es noetheriano.

Demostración:

Por inducción sobre *n*.

Si $n = 1$.

$$(\mathbf{A} \text{ es un anillo noetheriano}) \Rightarrow (\mathbf{A}[x_1] \text{ es un anillo noetheriano}), \ (\text{Propo. } 3.1.11).$$

Si $n > 1$. Sea $\mathbf{A}_{n-1} = \mathbf{A}[x_1, \ldots, x_{n-1}]$ y se supone que la condición se cumple, es decir, $\mathbf{A}$ es un anillo noetheriano, entonces $\mathbf{A}_{n-1}$ es un anillo noetheriano.

$$\begin{aligned}(\mathbf{A} \text{ es un anillo noetheriano}) &\Rightarrow (\mathbf{A}_{n-1} \text{ es un anillo noetheriano}) \\ &\Rightarrow (\mathbf{A}_{n-1}[x_n] \text{ es un anillo noetheriano}), \ (\text{Prop } 3.1.11) \\ &\Rightarrow (\mathbf{A}[x_1, \ldots, x_n] \text{ es un anillo noetheriano}).\end{aligned}$$

$\therefore$ Si $\mathbf{A}$ es noetheriano, entonces $\mathbf{A}[x_1, \ldots, x_n]$ es noetheriano.

Teorema 3.1.13: (Teorema de Cohen). Sea $\mathbf{A}$ un anillo, son equivalentes los siguientes enunciados:

(i) $\mathbf{A}$ es un anillo noetheriano.

(ii) Todos los ideales primos de $\mathbf{A}$ son finitamente generados.

Demostración:

$(i) \Rightarrow (ii)$.

De la proposición 3.1.6, si $\mathbf{A}$ es un anillo noetheriano, entonces todo ideal de $\mathbf{A}$ es finitamente generado; en particular los ideales primos.

$(ii) \Rightarrow (i)$.

Haciendo, $\Gamma = \{\mathfrak{a} \subseteq \mathbf{A} \mid \mathfrak{a} \text{ no es un ideal finitamente generado}\}$.

Suponga $\Gamma \neq \varnothing$, aplicando el **lema de Zorn** (Proposición 1.1.19), existen en Γ elementos maximales. Sea $\mathfrak{a} \in \Gamma$ un elemento maximal. Como $\mathfrak{a} \in \Gamma$, entonces $\mathfrak{a}$ no es primo, luego existen $a, b \in \mathbf{A}$ tal que $ab \in \mathfrak{a}$ y $a \notin \mathfrak{a}$, $b \notin \mathfrak{a}$.

Considere el ideal $\mathfrak{a} + a\mathbf{A}$, donde $\mathfrak{a} + a\mathbf{A} \supsetneq \mathfrak{a}$, pues en caso contrario si $\mathfrak{a} + a\mathbf{A} = \mathfrak{a}$, se tendría que $a \in \mathfrak{a}$ contradiciendo que $\mathfrak{a}$ no es primo. Luego $\mathfrak{a} + a\mathbf{A} \notin \Gamma$, por tanto es finitamente generado.

Si $\mathfrak{a}+a\,\mathbf{A}$ es finitamente generado, entonces existen $x_1, x_2, \ldots, x_t$ en $\mathfrak{a}+a\,\mathbf{A}$ tal que:

$$\mathfrak{a}+a\,\mathbf{A}=\sum_{i=1}^{t}\mathbf{A}\,x_i \quad .$$

Sea $k\in\mathfrak{a}+a\,\mathbf{A}$. Si $k\in\mathfrak{a}+a\,\mathbf{A}$, entonces existe $\alpha_i\in\mathbf{A}$ tal que;

$$k=x_1\alpha_1+x_2\alpha_2+\cdot\cdot\cdot+x_t\alpha_t$$

$$=(a_1+ah_1)\alpha_1+(a_2+ah_2)\alpha_2+\cdot\cdot\cdot+(a_t+ah_t)\alpha_t,\quad \text{con } a_j\in\mathfrak{a} \text{ y } h_j\in\mathbf{A}$$

$$=a_1\alpha_1+a(h_1\alpha_1)+a_2\alpha_2+a(h_2\alpha_2)+\cdot\cdot\cdot+a_t\alpha_t+a(h_t\alpha_t)$$

$$=a_1\alpha_1+a_2\alpha_2+\cdot\cdot\cdot+a_t\alpha_t+az,\qquad \text{con } z\in\mathbf{A}.$$

Luego $\{a_1, a_2, \ldots, a_t, a\}$ es un sistema finito de generadores de $\mathfrak{a}+a\,\mathbf{A}$. Se considera el ideal $(\mathfrak{a}:a)$. De acuerdo con la proposición 1.1.11 (i), $\mathfrak{a}\subseteq(\mathfrak{a}:a)$. Además:

$$ab\in\mathfrak{a} \text{ y } b\notin\mathfrak{a} \;\Rightarrow\; b\in(\mathfrak{a}:a) \text{ y } b\notin\mathfrak{a}$$

$$\Rightarrow\; \mathfrak{a}\subsetneq(\mathfrak{a}:a)$$

$$\Rightarrow\; (\mathfrak{a}:a)\notin\Gamma$$

$$\Rightarrow\; (\mathfrak{a}:a) \text{ es finitamente generado.}$$

Si $(\mathfrak{a} : a)$ es finitamente generado, entonces existen $b_1, b_2, \dots, b_m$ en $(\mathfrak{a} : a)$ tal que:

$$(\mathfrak{a} : a) = \sum_{i=1}^{m} \mathbf{A}\, b_i.$$

Dado $y \in \mathfrak{a}$. Si $y \in \mathfrak{a}$, entonces $y \in \mathfrak{a} + a\,\mathbf{A}$, luego existe una expresión de la forma:

$$y = a_1 r_1 + a_2 r_2 + \cdots + a_t r_t + ar, \quad \text{donde} \quad r_1, r_2, \dots, r_t, r \in \mathbf{A}.$$

Despejando ar se obtiene:

$$ar = y - a_1 r_1 - a_2 r_2 - \cdots - a_t r_t, \quad \text{donde} \quad r_1, r_2, \dots, r_t, r \in \mathbf{A}.$$

Todos los sumandos de la derecha están en $\mathfrak{a}$, así $ar \in \mathfrak{a}$, entonces $r \in (\mathfrak{a} : a)$ y por ser finitamente generado existen $s_1, s_2, \dots, s_m$ en $\mathbf{A}$ tal que:

$$r = b_1 s_1 + b_2 s_2 + \cdots + b_m s_m.$$

Uniendo todo resulta:

$$y = a_1 r_1 + a_2 r_2 + \cdots + a_t r_t + a\left(b_1 s_1 + b_2 s_2 + \cdots + b_m s_m\right).$$

Distribuyendo por ser elementos del anillo $\mathbf{A}$,

$$y = a_1 r_1 + a_2 r_2 + \cdots + a_t r_t + ab_1 s_1 + ab_2 s_2 + \cdots + ab_m s_m.$$

Por tanto $\{a_1 , a_2 , \ldots , a_t , ab_1, ab_2 , \ldots , ab_m\}$ es un sistema de generadores de $\mathfrak{a}$, lo que es una contradicción. Resulta entonces que $\Gamma = \varnothing$, luego todo ideal en $\mathbf{A}$ es finitamente generado, en consecuencia de la proposición 3.1.6, $\mathbf{A}$ es un anillo noetheriano.■

Nota: Si $\mathbf{A}$ es un anillo noetheriano, entonces $\mathbf{A}[\![x]\!]$ es noetheriano (Donde $\mathbf{A}[\![x]\!]$ es el anillo de las series formales de potencias $f = \sum_{i=0}^{\infty} a_i x^i$ con coeficientes en $\mathbf{A}$). La demostración se ve a continuación y es una consecuencia del teorema de **Cohen.**

Proposición 3.1.14: Sea $\mathbf{A}$ un anillo noetheriano, x una indeterminada, entonces el anillo de series formales de potencias de $\mathbf{A}[\![x]\!]$ es noetheriano.

Demostración: Sea $\mathfrak{p}[\![x]\!] \neq 0$ un ideal primo en $\mathbf{A}[\![x]\!]$. Se considera la aplicación definida por:

$$\delta : \mathbf{A}[\![x]\!] \longrightarrow \mathbf{A}$$
$$\sum_{j=0}^{\infty} s_j x^j \to \delta\left(\sum_{j=0}^{\infty} s_j x^j\right) = s_0.$$

Si $\mathfrak{p}[\![x]\!]$ es un ideal en $\mathbf{A}[\![x]\!]$, entonces por la proposición 1.3.6, $\delta\left(\mathfrak{p}[\![x]\!]\right)$ es un ideal de $\mathbf{A}$ y por tanto es finitamente generado. Luego existen $a_1, a_2 , \ldots , a_t$ en $\delta\left(\mathfrak{p}[\![x]\!]\right)$ tal que, $\delta\left(\mathfrak{p}[\![x]\!]\right) = \sum_{j=1}^{t} \mathbf{A}\, a_j$.

De forma más explícita, $\delta\left(\mathfrak{p}[\![x]\!]\right)$ es el conjunto de todos los elementos de $a \in \mathbf{A}$ tal que a es el termino independiente de alguna serie en $\mathfrak{p}[\![x]\!]$.

Suponga que $\delta\left(\mathfrak{p}[\![x]\!]\right) = \{0\}$. Sea $G \in \mathfrak{p}[\![x]\!]$.

Si $G \in \mathfrak{p}[\![x]\!]$, entonces existen $b_1', \ldots, b_k', b_{k+1}', \ldots$ en $\mathbf{A}$ tal que:

$$G = b_1'x^1 + b_2'x^2 + \cdots + b_k'x^k + b_{k+1}'x^{k+1} + \cdots .$$

En consecuencia,

$$G = \underbrace{\left(b_1' + b_2'x^1 \cdots + b_k'x^{k-1} + b_{k+1}'x^k + \cdots\right)}_{\in \mathbf{A}[\![x]\!]} x.$$

De donde $G \in (x)$. Luego $\mathfrak{p}[\![x]\!] \subseteq (x)$. Recíprocamente sea $0 \neq G'$ una serie no nula de $\mathfrak{p}[\![x]\!]$ y sea b_k'' el primer coeficiente no nulo de G'. Entonces:

$$G' = x^k\left(b_k'' + b_{k+1}''x^1 + \cdots\right) \in \mathfrak{p}[\![x]\!].$$

Como $\mathfrak{p}[\![x]\!]$ es un ideal primo en $\mathbf{A}[\![x]\!]$,

$$x^k \in \mathfrak{p}[\![x]\!] \qquad \text{ó} \qquad b_k'' + b_{k+1}''x + \cdots \in \mathfrak{p}[\![x]\!].$$

Supóngase que $b''_k + b''_{k+1}x^k + \cdot\cdot\cdot \in \mathfrak{p}[\![x]\!]$.

$$b''_k + b''_{k+1}x^k + \cdot\cdot\cdot \in \mathfrak{p}[\![x]\!] \;\Rightarrow\; \delta\left(b''_k + b''_{k+1}x^k + \cdot\cdot\cdot\right) \in \delta\left(\mathfrak{p}[\![x]\!]\right) = \{0\}$$

$$\Rightarrow\; b''_k \in \delta\left(\mathfrak{p}[\![x]\!]\right) = \{0\}$$

$$\Rightarrow\; b''_k = 0,\; (\rightarrow\leftarrow).$$

Por tanto, $x \in \mathfrak{p}[\![x]\!]$ y de esta forma $\mathfrak{p}[\![x]\!] = (x)$.

Suponga que $\delta\left(\mathfrak{p}[\![x]\!]\right) \neq \{0\}$.

Sean $h^{(1)}, h^{(2)}, \ldots, h^{(t)}$ en $\mathfrak{p}[\![x]\!]$ tal que cada $h^{(j)} = a_j + h_1^j x + h_2^j x^2 + \cdot\cdot\cdot$ y $\delta\left(h^j\right) = a_j$, para $j = 1, \ldots, t$. Se tienen los siguientes casos:

Caso I: Si $x \in \mathfrak{p}[\![x]\!]$. Se demuestra que $\mathfrak{p}[\![x]\!] = \langle a_1, a_2, \ldots, a_t, x\rangle$. Se considera la siguiente expresión contenida en $\mathfrak{p}[\![x]\!]$.

$$h^{(j)} - x\left(\sum_{i=1}^{\infty} h_i^j x^{i-1}\right) = \left(a_j + h_1^j x + h_2^j x^2 + \cdot\cdot\cdot\right) - x\left(h_1^j x^0 + h_2^j x^1 + h_3^j x^2 + \cdot\cdot\cdot\right)$$

$$= a_j + h_1^j x + h_2^j x^2 + \cdot\cdot\cdot - h_1^j x - h_2^j x^2 - h_3^j x^3 - \cdot\cdot\cdot$$

$$= a_j.$$

Entonces cada $a_j \in \mathfrak{p}[\![x]\!]$, para $j = 1, \ldots, t$. Sea G una serie en $\mathfrak{p}[\![x]\!]$.

Si $G \in \mathfrak{p}[\![x]\!]$, entonces existen $b_0, b_1, \ldots, b_k, b_{k+1}, \ldots$ en $\mathbf{A}$ tal que

$$G = b_0 + b_1 x^1 + \cdots + b_k x^k + b_{k+1} x^{k+1} + \cdots .$$

Puesto que b_0 es término independiente de la serie G, entonces $b_0 \in \delta\left(\mathfrak{p}[\![x]\!]\right)$; luego existen $\beta_1, \beta_2, \ldots, \beta_t$ en $\mathbf{A}$ tales que:

$$b_0 = \sum_{j=1}^{t} \beta_j a_j, \qquad \text{con} \quad a_1, a_2, \ldots, a_t \in \delta\left(\mathfrak{p}[\![x]\!]\right).$$

Uniendo todo lo anterior y factorizando x,

$$G = \sum_{j=1}^{t} \beta_j a_j + x\left(b_1 + b_2 x^1 + \cdots + b_k x^{k-1} + b_{k+1} x^k + \cdots\right).$$

Luego $\{a_1, a_2, \ldots, a_t, x\}$, es un sistema de generadores de $\mathfrak{p}[\![x]\!]$.

Caso II: Si $x \notin \mathfrak{p}[\![x]\!]$. Se demuestra que $\left\{h^{(1)}, h^{(2)}, \ldots, h^{(t)}\right\}$ es un sistema de generadores de $\mathfrak{p}[\![x]\!]$. Sea $s^{(0)} \in \mathfrak{p}[\![x]\!]$.

Si $s^{(0)} \in \mathfrak{p}[\![x]\!]$, entonces existe, $s_0^{(0)}, s_1^{(0)}, \ldots, s_k^{(0)}, s_{k+1}^{(0)}, \ldots$ en $\mathbf{A}$ tal que:

$$s^{(0)} = s_0^{(0)} + s_1^{(0)} x^1 + \cdots + s_k^{(0)} x^k + s_{k+1}^{(0)} x^{k+1} + \cdots .$$

Procedimiento (1):

Como $s_0^{(0)}$ es el término independiente en la serie, entonces $s_0^{(0)} \in \delta\left(\mathfrak{p}[\![x]\!]\right)$. De donde existen $c_{0_1}, c_{0_2}, \ldots, c_{0_t}$ en $\mathbf{A}$, tales que:

$$s_0^{(0)} = \sum_{j=1}^{t} c_{0_j} a_j.$$

Por tanto la serie contenida en $\mathfrak{p}[\![x]\!]$:

$$s^{(0)} - \sum_{j=1}^{t} c_{0_j} h^{(j)} = \left(s_0^{(0)} + s_1^{(0)} x^1 + \cdots + s_k^{(0)} x^k + \cdots\right) - \left(c_{0_1} h^{(1)} + c_{0_2} h^{(2)} + \cdots + c_{0_t} h^{(t)}\right)$$

$$= s_0^{(0)} + s_1^{(0)} x^1 + \cdot\cdot\cdot\cdot + s_k^{(0)} x^k + \cdot\cdot\cdot\cdot$$

$$\cdots - \left[c_{0_1}\left(a_1 + h_1^1 x + \cdots\right) + c_{0_2}\left(a_2 + h_1^2 x + \cdots\right) + \cdots + c_{0_t}\left(a_1 + h_1^t x + \cdots\right)\right]$$

$$= s_0^{(0)} + s_1^{(0)} x^1 + \cdot\cdot\cdot\cdot + s_k^{(0)} x^k + \cdot\cdot\cdot\cdot$$

$$\cdots - \left[\left(c_{0_1} a_1 + c_{0_1} h_1^1 x + \cdots\right) + \left(c_{0_2} a_2 + c_{0_2} h_1^2 x + \cdots\right) + \cdots + \left(c_{0_t} a_1 + c_{0_t} h_1^t x + \cdots\right)\right]$$

$$= s_0^{(0)} + s_1^{(0)} x^1 + \cdot\cdot\cdot\cdot + s_k^{(0)} x^k + \cdot\cdot\cdot$$

$$\cdots - \left[\sum_{j=1}^{t} c_{0_j} a_j + \left(c_{0_1} h_1^1 x + \cdots \right) + \left(c_{0_2} h_1^2 x + \cdots \right) + \cdots + \left(c_{0_t} h_1^t x + \cdots \right) \right]$$

$$= \left(s_1^{(0)} x^1 + \; s_2^{(0)} x^2 + \cdots \right) - \left(c_{0_1} h_1^1 x + \cdots \right) - \left(c_{0_2} h_1^2 x + \cdots \right) - \cdots - \left(c_{0_t} h_1^t x + \cdots \right)$$

$$= x \left[\underbrace{\left(s_1^{(0)} + s_2^{(0)} x^2 + \cdots \right) - \left(c_{0_2} h_1^1 + \cdots \right) - \left(c_{0_2} h_1^2 + \cdots \right) - \cdots - \left(c_{0_t} h_1^t + \cdots \right)}_{s^{(1)}} \right]$$

$$= x s^{(1)}.$$

Donde $s^{(1)} \in \mathbf{A}[\![x]\!]$. Como $\mathfrak{p}[\![x]\!]$ es primo y $x \notin \mathfrak{p}[\![x]\!]$, entonces $s^{(1)} \in \mathfrak{p}[\![x]\!]$.

Por lo tanto:

$$s^{(0)} = \sum_{j=1}^{t} c_{0_j} h^{(j)} + x s^{(1)}.$$

Fin del procedimiento (1). Sucesivamente se repite el procedimiento (1) para $s^{(r)}$ con $r \in \mathbb{N}$ obteniendo así:

$$s^{(r)} = \sum_{j=1}^{t} c_{r_j} h^{(j)} + x s^{(r+1)}.$$

Reemplazando se tiene:

$$s^{(0)} = \sum_{j=1}^{t} c_{0_j} h^{(j)} + xs^{(1)}$$

$$= \sum_{j=1}^{t} c_{0_j} h^{(j)} + x\left(\sum_{j=1}^{t} c_{1_j} h^{(j)} + xs^{(2)}\right)$$

$$= \sum_{j=1}^{t} c_{0_j} h^{(j)} + \sum_{j=1}^{t}\left(xc_{1_j}\right) h^{(j)} + x^2 s^{(2)}$$

$$= \sum_{j=1}^{t} c_{0_j} h^{(j)} + \sum_{j=1}^{t}\left(c_{1_j} x\right) h^{(j)} + x^2\left(\sum_{j=1}^{t} c_{2_j} h^{(j)} + xs^{(3)}\right)$$

$$= \sum_{j=1}^{t} c_{0_j} h^{(j)} + \sum_{j=1}^{t}\left(c_{1_j} x\right) h^{(j)} + \sum_{j=1}^{t}\left(c_{2_j} x^2\right) h^{(j)} + x^3 s^{(3)}$$

$$\vdots \qquad\qquad \vdots \qquad\qquad \vdots \qquad\qquad \vdots$$

$$= \sum_{j=1}^{t} c_{0_j} h^{(j)} + \sum_{j=1}^{t}\left(c_{1_j} x\right) h^{(j)} + \sum_{j=1}^{t}\left(c_{2_j} x^2\right) h^{(j)} + \cdots + x^{k-1}\left(\sum_{j=1}^{t} c_{k-1_j} h^{(j)} + xs^{(k)}\right) + \cdots$$

$$= \sum_{j=1}^{t} c_{0_j} h^{(j)} + \sum_{j=1}^{t}\left(c_{1_j} x\right) h^{(j)} + \sum_{j=1}^{t}\left(c_{2_j} x^2\right) h^{(j)} + \cdots + \sum_{j=1}^{t}\left(c_{k-1_j} x^{k-1}\right) h^{(j)} + \cdots$$

$$= \sum_{j=1}^{t}\left(c_{0_j} + c_{1_j} x + c_{2_j} x^2 + \cdots + c_{k-1_j} x^{k-1} + \cdots\right) h^{(j)}$$

$$= \sum_{j=1}^{t} \underbrace{\left(\sum_{i=0}^{\infty} c_{i_j} x^i\right)}_{\in \mathbf{A}[\![x]\!]} h^{(j)}.$$

Luego $\left\{h^{(1)}, h^{(2)}, \ldots, h^{(t)}\right\}$ es un sistema de generadores de $\mathfrak{p}[\![x]\!]$. Entonces cada ideal primo de $\mathbf{A}[\![x]\!]$ es finitamente generado. En virtud del teorema de **Cohen** $\mathbf{A}[\![x]\!]$ es un anillo noetheriano. ■

A continuación se demuestra la propiedad enunciada en la proposición 1.1.15 (**Cap. I**).

Proposición 1.1.15: Sea $\mathbf{A} = \prod_{i=1}^{n} \mathbf{A}_i$ un producto de anillos. Entonces cada ideal $\mathfrak{a}$ en $\mathbf{A}$ es de la forma $\mathfrak{a} = \prod_{i=1}^{n} \mathfrak{a}_i$, donde cada $\mathfrak{a}_i$ es ideal en $\mathbf{A}_i$.

Demostración:

Se demuestra que cada ideal $\mathbf{J}$ en el anillo $\mathbf{A} = \prod_{i=1}^{n} \mathbf{A}_i$ es de la forma $\mathbf{J} = \sum_{i=1}^{n} \oplus \mathbf{J}_i$, donde cada $\mathbf{J}_i$ es ideal en $\mathbf{A}_i$.

Considere el elemento en $\mathbf{A}$ definido como sigue:

$$e_i = \left\{\delta_{ij}\right\}_{j=1}^{n} \quad \text{donde} \quad \delta_{ij} = \begin{cases} 1_{\mathbf{A}_i} & \text{si } i = j \\ 0 & \text{si } i \neq j \end{cases},$$

para todo $i = 1, \ldots, n$. Para $\mathbf{A}$ se tiene la siguiente descomposición en suma de ideales:

$$\mathbf{A} = \sum_{i=1}^{n} \oplus \mathbf{I}_i.$$

Donde $\mathbf{I}_i = e_i\,\mathbf{A}$; pues cada $\mathbf{I}_i$ es isomorfo al anillo $\mathbf{A}_i$.

$$\mathbf{I}_i = e_i\,\mathbf{A} = 0\times\ \cdot\ \cdot\ \cdot\times\mathbf{A}_i\times\ \cdot\ \cdot\ \cdot\times 0 \cong \mathbf{A}_i\,.$$

Sea $\mathbf{J}$ un ideal en $\mathbf{A}$. Entonces $\mathbf{J}\,e_i = \mathbf{J}_i$ es un ideal en $\mathbf{A}$ contenido en $\mathbf{A}_i$;

$$\sum_{i=1}^{n}\oplus\,\mathbf{J}_i = \sum_{i=1}^{n}\oplus\,\mathbf{J}\,e_i = \mathbf{J}, \quad \text{con } \mathbf{J}_i \text{ ideal en } \mathbf{A}_i\,.$$

Proposición 3.1.15: Sean $\mathbf{A}_1,\ \mathbf{A}_2,\ldots,\ \mathbf{A}_n$ anillos noetherianos. Entonces el anillo producto $\mathbf{A} = \prod_{i=1}^{n}\mathbf{A}_i$ es noetheriano.

Demostración:

Sea $\mathbf{J}_1 \subseteq \mathbf{J}_2 \subseteq\ \cdot\ \cdot\ \cdot\ \subseteq \mathbf{J}_m \subseteq \mathbf{J}_{m+1} \subseteq\ \cdot\ \cdot\ \cdot$ una cadena ascendente de ideales en $\mathbf{A}$. De la proposición 1.1.15, para cada $\mathbf{J}_i$ existen $\mathbf{I}_1^i,\ \mathbf{I}_2^i\ ,\ldots,\ \mathbf{I}_n^i$ en $\mathbf{A}_1,\ \mathbf{A}_2\ ,\ldots,\ \mathbf{A}_n$ respectivamente, tal que $\mathbf{J}_i = \mathbf{I}_1^i\times\mathbf{I}_2^i\times\ \cdot\ \cdot\ \cdot\ \times\mathbf{I}_n^i$ para $1 \le i \le n$.

Luego:

$$\mathbf{I}_1^1\times\mathbf{I}_2^1\times\ \cdot\ \cdot\ \cdot\ \times\mathbf{I}_n^1 \subseteq \mathbf{I}_1^2\times\mathbf{I}_2^2\times\ \cdot\ \cdot\ \cdot\ \times\mathbf{I}_n^2 \subseteq\ \cdot\ \cdot\ \cdot\ \subseteq \mathbf{I}_1^m\times\mathbf{I}_2^m\times\ \cdot\ \cdot\ \cdot\ \times\mathbf{I}_n^m \subseteq\ \cdot\ \cdot\ \cdot\ .$$

Se obtienen, entonces las siguientes cadenas ascendentes de ideales en $\mathbf{A}_i$, con $i=1,\ldots,n.$

$$\begin{array}{l}
\mathcal{C}_1 : \mathbf{I}_1^1 \subseteq \mathbf{I}_1^2 \subseteq \cdots \subseteq \mathbf{I}_1^m \subseteq \mathbf{I}_1^{m+1} \subseteq \cdots . \\
\mathcal{C}_2 : \mathbf{I}_2^1 \subseteq \mathbf{I}_2^2 \subseteq \cdots \subseteq \mathbf{I}_2^m \subseteq \mathbf{I}_2^{m+1} \subseteq \cdots . \\
\quad \vdots \quad \vdots \qquad\qquad \vdots \quad \vdots \\
\mathcal{C}_n : \mathbf{I}_n^1 \subseteq \mathbf{I}_n^2 \subseteq \cdots \subseteq \mathbf{I}_n^m \subseteq \mathbf{I}_n^{m+1} \subseteq \cdots .
\end{array}$$

Para cada $1 \le j \le n$, $\mathbf{A}_j$ es noetheriano, entonces existe $m_j \in \mathbb{N}$ tal que $\mathbf{I}_j^{m_j} = \mathbf{I}_j^{m_j+1}$. Sea $p = \max\{m_j\}_{j=1}^{n}$. Se demuestra que $\mathbf{J}_p = \mathbf{J}_k$ para todo $k \ge p$. Se supone que $\mathbf{J}_p \subsetneq \mathbf{J}_k$.

Si $\mathbf{J}_p \subsetneq \mathbf{J}_k$, entonces

$$\mathbf{I}_1^p \times \mathbf{I}_2^p \times \cdots \times \mathbf{I}_n^p \subsetneq \mathbf{I}_1^k \times \mathbf{I}_2^k \times \cdots \times \mathbf{I}_n^k .$$

Por tanto existe $1 \le r \le n$, tal que:

$$\mathbf{I}_r^p \subsetneq \mathbf{I}_r^k \subsetneq \mathbf{I}_r^{k+1} \subsetneq \cdots .$$

Lo que es una contradicción pues por la definición de p, para todo $(1 \le j \le n \text{ y } k \ge p)$, se verifica que $\mathbf{I}_j^p = \mathbf{I}_j^k = \mathbf{I}_j^{k+1}$. Luego $\mathbf{J}_p = \mathbf{J}_k$ para todo $k \ge p$. Esto muestra que $\mathbf{A}$ es un anillo noetheriano.■

3.2: Ideales primos minimales en anillos noetherianos.

De acuerdo con la proposición 1.2.17, todo anillo $\mathbf{A}$ tiene ideales primos minimales, más aún, si $\mathbf{A}$ es un anillo noetheriano, cada ideal $\mathfrak{a}$ en $\mathbf{A}$ sólo tiene un número finito de ideales primos minimales sobre $\mathfrak{a}$, en particular, $\mathbf{A}$ tiene sólo un número finito de ideales primos minimales. Los primos minimales de un anillo están estrechamente relacionados con sus divisores de cero. Se dedica esta sección a estudiar con más detalle estas propiedades.

Proposición 3.2.1: Sea $\mathbf{A}$ un anillo noetheriano y $\mathfrak{a}$ un ideal propio de $\mathbf{A}$. Entonces existen ideales primos $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ tales que $\mathfrak{a} \subseteq \mathfrak{p}_i$ para cada $i = 1, \ldots, t$ y $\mathfrak{p}_1 \cdot \cdot \cdot \mathfrak{p}_t \subseteq \mathfrak{a}$.

Demostración:

Defina la familia:

$$\Gamma = \{\mathfrak{a} \subseteq \mathrm{A} : \mathfrak{a} \text{ no contiene un producto finito de ideales primos que contiene a } \mathfrak{a}\}.$$

Suponga que $\Gamma \neq \emptyset$. Como $\mathbf{A}$ es un anillo noetheriano, entonces Γ tiene elementos maximales. Sea $\mathfrak{q} \in \Gamma$ maximal. Se demuestra que $\mathfrak{q}$ es un ideal primo en $\mathbf{A}$. Supóngase que $\mathfrak{q}$ no es un ideal primo en $\mathbf{A}$.

Si $\mathfrak{q}$ no es un ideal primo en $\mathbf{A}$, entonces existen $a, b \in \mathbf{A}$ tal que $ab \in \mathfrak{q}$ y $a, b \notin \mathfrak{q}$.

Luego si $a \notin \mathfrak{q}$ y $b \notin \mathfrak{q}$, entonces $\mathfrak{q} \subsetneq (a)+\mathfrak{q}$ y $\mathfrak{q} \subsetneq (b)+\mathfrak{q}$, por la maximalidad de $\mathfrak{q}$:

$$(a)+\mathfrak{q} \notin \Gamma \quad \text{y} \quad (b)+\mathfrak{q} \notin \Gamma.$$

De donde, existen ideales primos $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_s, \mathfrak{p}_{s+1}, \mathfrak{p}_{s+2}, \ldots, \mathfrak{p}_r$ en $\mathbf{A}$ tal que:

$$\mathfrak{p}_1\mathfrak{p}_2 \cdot\cdot\cdot \mathfrak{p}_s \subseteq (a)+\mathfrak{q}, \quad \text{donde} \quad \mathfrak{q} \subsetneq (a)+\mathfrak{q} \subseteq \mathfrak{p}_i \quad \forall\, i=1,\ldots,s.$$

$$\mathfrak{p}_{s+1}\mathfrak{p}_{s+2} \cdot\cdot\cdot \mathfrak{p}_r \subseteq (b)+\mathfrak{q}, \quad \text{donde} \quad \mathfrak{q} \subsetneq (b)+\mathfrak{q} \subseteq \mathfrak{p}_j \quad \forall\, j=s+1,\ldots,r.$$

Multiplicando los productos anteriores,

$$\mathfrak{p}_1\mathfrak{p}_2 \cdot\cdot\cdot \mathfrak{p}_s\mathfrak{p}_{s+1}\mathfrak{p}_{s+2} \cdot\cdot\cdot \mathfrak{p}_r \subseteq \big((a)+\mathfrak{q}\big)\big((b)+\mathfrak{q}\big) \subseteq \mathfrak{q} \quad \text{y} \quad \mathfrak{q} \subsetneq \mathfrak{p}_i \quad \forall\, i=1,\ldots,r\,.$$

Lo que es una contradicción porque $\mathfrak{q} \in \Gamma$. Luego $a \in \mathfrak{q}$ ó $b \in \mathfrak{q}$, en consecuencia se tiene que $\mathfrak{q}$ es un ideal primo. Si $\mathfrak{q}$ es primo, entonces $\mathfrak{q} \notin \Gamma$. De donde el conjunto de maximales en Γ es vacío; lo que es una contradicción pues en un anillo noetheriano toda familia no vacía de ideales en $\mathbf{A}$ tiene elemento maximal.

Como consecuencia $\Gamma = \varnothing$. Por tanto cada ideal $\mathfrak{a}$ contiene un producto finito de ideales primos que contienen a $\mathfrak{a}$. ■

Corolario 3.2.2: Sea $\mathbf{A}$ un anillo noetheriano, entonces para cada ideal $\mathfrak{a} \neq (1)$ en $\mathbf{A}$ existe sólo un número finito de ideales primos minimales sobre $\mathfrak{a}$.

Demostración:

Sea $\mathfrak{a}$ un ideal propio en $\mathbf{A}$ y $\mathfrak{p}$ un ideal primo minimal sobre $\mathfrak{a}$. En virtud de la proposición 3.2.1, existe un número finito de ideales primos, $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ tal que $\mathfrak{a} \subseteq \mathfrak{p}_i$ para cada $i = 1, \ldots, t$ y $\mathfrak{p}_1 \cdot \cdot \cdot \mathfrak{p}_t \subseteq \mathfrak{a}$.

Si $\mathfrak{p}$ es un ideal primo minimal sobre $\mathfrak{a}$, entonces $\mathfrak{a} \subseteq \mathfrak{p}$, de lo anterior,

$$\mathfrak{p}_1 \cdot \cdot \cdot \mathfrak{p}_t \subseteq \mathfrak{a} \subseteq \mathfrak{p}.$$

Entonces de la proposición 1.2.19,

$$\mathfrak{a} \subseteq \mathfrak{p}_j \subseteq \mathfrak{p}, \quad \text{para algún} \qquad 1 \leq j \leq t.$$

Por la minimalidad de $\mathfrak{p}$,

$$\mathfrak{p}_j = \mathfrak{p}, \quad \text{para algún} \qquad 1 \leq j \leq t.$$

Luego en un anillo noetheriano, sólo existe un número finito de ideales primos minimales sobre $\mathfrak{a}$. ■

Observaciones 3.2.3:

1. En particular para el ideal $\mathbf{0}$ existen un número finito de ideales primos minimales. De la definición 1.2.16, los ideales primos minimales de $\mathbf{A}$ son los primos minimales del ideal cero. Luego en un anillo noetheriano sólo existe un número finito de ideales primos minimales.

2. De la proposición 1.2.17, se tiene que para cada ideal $\mathfrak{a}$ el radical de $\mathfrak{a}$ es:

$$r(\mathfrak{a}) = \bigcap \{\mathfrak{p} \mid \mathfrak{p} \text{ es un ideal primo minimal sobre } \mathfrak{a}\}.$$

Luego por el corolario 3.2.2 el radical de $\mathfrak{a}$ es la intersección finita de primos minimales sobre $\mathfrak{a}$.

3. Si $\mathbf{A}$ es un anillo noetheriano reducido, entonces:

$$\mathbf{0} = \mathfrak{p}_1 \cap \cdot \cdot \cdot \cap \mathfrak{p}_n.$$

Donde $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ son los ideales primos minimales de $\mathbf{A}$.

La relación fundamental entre los primos minimales de un anillo y sus divisores de cero viene dada por la siguiente proposición.

Proposición 3.2.4: Sea $\mathbf{A}$ un anillo noetheriano y $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ el conjunto de ideales primos minimales de $\mathbf{A}$. Se verifica lo siguiente:

(i) Los elementos no nulos de cada $\mathfrak{p}_i$ son divisores de cero.

(ii) Si $\mathbf{A}$ es reducido todo divisor de cero pertenece a algún $\mathfrak{p}_i$.

Demostración (i):

De la observación 3.2.3,

$$r(\mathbf{0})=\bigcap_{i=1}^{s}\mathfrak{p}_i.$$

Si $s=1$, entonces $\mathfrak{p}_1=r(\mathbf{0})=\mathfrak{R}_{\mathbf{A}}$. De donde $\mathfrak{p}_1$ está formado por los elementos nilpotentes de $\mathbf{A}$, luego en virtud de la definición 1.1.8 observación (1) todos sus elementos no nulos son divisores de ceros.

Suponga que $s>1$ y sea $p\in\mathfrak{p}_j$, tal que $p\neq 0$.

Se puede encontrar $q\in\bigcap_{i\neq j}\mathfrak{p}_i$ tal que $q\notin\mathfrak{p}_j$, pues en caso contrario se tendría que:

$$\bigcap_{i\neq j}\mathfrak{p}_i\subseteq\mathfrak{p}_j.$$

De acuerdo con la proposición 1.2.9 (ii),

$$\mathfrak{p}_i\subseteq\mathfrak{p}_j,\qquad \text{para algún } 1\leq i\neq j\leq s.$$

En contradicción con la minimalidad de $\mathfrak{p}_j$.

Ahora se tiene:

$$q\in\bigcap_{i\neq j}\mathfrak{p}_i \;\text{ y }\; q\notin\mathfrak{p}_j \;\Rightarrow\; pq\in\bigcap_{i\neq j}\mathfrak{p}_i \;\text{ y }\; pq\in\mathfrak{p}_j,\ \text{para algún } 1\leq j\leq s$$

$$\Rightarrow \quad pq \in \bigcap_{i=1}^{s} \mathfrak{p}_i = r(0) = \Re_{\mathbf{A}}$$

$$\Rightarrow \quad \exists \quad n \in \mathbb{N} \quad \text{t. q.} \quad (pq)^n = p^n q^n = 0.$$

Además:

$$q \notin \mathfrak{p}_j \text{ para algún } 1 \leq j \leq s \quad \Rightarrow \quad q \notin \bigcap_{i=1}^{s} \mathfrak{p}_i = r(0)$$

$$\Rightarrow \quad q \text{ no es nilpotente}$$

$$\Rightarrow \quad \text{para todo } n \in \mathbb{N} \quad q^m \neq 0.$$

Luego se puede considerar el mínimo $t \in \mathbb{N}$ tal que $p^t q^m \neq 0,$ entonces $p\left(p^t q^m\right) = p^{t+1} q^m = 0.$ Esto implica que p es un divisor de cero en $\mathbf{A}$.

$\therefore$ Los elementos no nulos de cada $\mathfrak{p}_i$ son divisores de cero.

Demostración (ii):

Suponga que $\mathbf{A}$ es reducido, en este caso se tiene:

$$\mathbf{0} = r(\mathbf{0}) = \bigcap_{i=1}^{s} \mathfrak{p}_i.$$

Sea $a \in \mathbf{A}$ un divisor de cero en $\mathbf{A}$.

a divide a cero $\Rightarrow\ \exists\quad a' \in \mathbf{A},\ a' \neq 0$ t. q. $a'a = 0$

$\Rightarrow\quad a' \notin \mathfrak{p}_j$ y $a'a \in \mathfrak{p}_j$ para algún $1 \leq j \leq$ s

$\Rightarrow\quad a \in \mathfrak{p}_j$ para algún $1 \leq j \leq$ s.

$\therefore$ Si $\mathbf{A}$ es reducido todo divisor de cero pertenece a algún $\mathfrak{p}_i$.

Observación: En consecuencia de la proposición anterior, el conjunto de divisores de cero de un anillo noetheriano $\mathbf{0} \neq \mathbf{A}$, con nilradical nulo coincide con la unión de sus ideales primos minimales.

Proposición 3.2.5: Sea $\mathbf{A} \subseteq \mathbf{B}$ una extensión entera de anillos y $\mathfrak{p}$ un ideal primo de $\mathbf{A}$. Demostrar que si $\mathbf{B}$ es noetheriano hay únicamente un número finito de ideales primos $\mathfrak{q}$ de $\mathbf{B}$ tales que $\mathfrak{q} \cap \mathbf{A} = \mathfrak{p}$.

Demostración:

Sea $\mathfrak{p}$ un ideal primo en $\mathbf{A}$. Considere los siguientes conjuntos en $\mathbf{B}$:

$$\mathfrak{F}_{\mathfrak{p}\mathbf{B}} = \{\mathfrak{q} \subseteq \mathbf{B} \mid \mathfrak{q} \text{ es un ideal primo minimal sobre } \mathfrak{p}\mathbf{B}\}.$$

$$\mathfrak{J} = \{\ \mathfrak{q} \subseteq \mathbf{B} \mid \mathfrak{q} \cap \mathbf{A} = \mathfrak{p}\ \}.$$

Se demuestra que $\mathfrak{F}_{\mathfrak{p}\mathbf{B}} = \mathfrak{J}$.

Sea $\mathfrak{q} \in \mathfrak{F}_{\mathfrak{p}\mathbf{B}}$ y suponga $\mathfrak{q} \notin \mathfrak{J}$.

$\mathfrak{q} \in \mathfrak{F}_{\mathfrak{p}\mathbf{B}} \quad \Rightarrow \quad \mathfrak{q}$ es un ideal primo minimal sobre $\mathfrak{p}\mathbf{B}$ y $\mathfrak{q} \supseteq \mathfrak{p}\mathbf{B}$

$\Rightarrow \quad \mathfrak{p}' = \mathfrak{q} \cap \mathbf{A} \supseteq \mathfrak{p}\mathbf{B} \cap \mathbf{A} \supseteq \mathfrak{p}$, $\big($Proposición 1.3.3 (iii)$\big)$

$\Rightarrow \quad \mathfrak{p}' \supsetneq \mathfrak{p}$ y $\mathfrak{p}' = \mathfrak{q} \cap \mathbf{A}$

$\Rightarrow \quad \exists \ \mathfrak{q}' \subsetneq \mathbf{B}$ tal que $\mathfrak{q}' \cap \mathbf{A} = \mathfrak{p}$ y $\mathfrak{q} \supsetneq \mathfrak{q}'$, $\big($Proposición 2.4.10$\big)$

$\Rightarrow \quad \mathfrak{q}' \supseteq \mathbf{B}(\mathfrak{q}' \cap \mathbf{A}) = \mathbf{B}\mathfrak{p}$, $\big($Proposición 1.3.3 (iv) $\big)$

$\Rightarrow \quad \mathbf{B}\mathfrak{p} \subseteq \mathfrak{q}' \subsetneq \mathfrak{q}$, $(\rightarrow\leftarrow)$ $\big($Minimalidad de $\mathfrak{q}\big)$.

$$\therefore \mathfrak{F}_{\mathfrak{p}\mathbf{B}} \subseteq \mathfrak{J}.$$

Sea $\mathfrak{q} \in \mathfrak{J}$ tal que $\mathfrak{q} \supseteq \mathfrak{p}\mathbf{B}$. Supóngase que $\mathfrak{q}$ no es un ideal primo minimal sobre $\mathfrak{p}\mathbf{B}$.

$\mathfrak{q}$ no es minimal sobre $\mathfrak{p}\mathbf{B} \quad \Rightarrow \quad \exists \ \mathfrak{q}' \subsetneq \mathbf{B}$ minimal sobre $\mathfrak{p}\mathbf{B}$ t. q. $\mathfrak{q}' \subseteq \mathfrak{q}$, $\big($Prop 1.2.17$\big)$

$\Rightarrow \quad \mathfrak{q}' \in \mathfrak{F}_{\mathfrak{p}\mathbf{B}} \subseteq \mathfrak{J}$

$\Rightarrow \quad \mathfrak{q}' \cap \mathbf{A} = \mathfrak{p}$ y $\mathfrak{q} \cap \mathbf{A} = \mathfrak{p}$

$\Rightarrow \quad \mathfrak{q}' = \mathfrak{q}$, $\big(\big($Prop. 2.3.18$\big)$ **Incomparabilidad**$\big)$

$$\Rightarrow \quad \mathfrak{q} \text{ es minimal sobre } \mathfrak{p}\mathbf{B}.$$

$$\therefore \mathfrak{J} \subseteq \mathfrak{F}_{\mathfrak{p}\mathbf{B}}.$$

Luego $\mathfrak{J} = \mathfrak{F}_{\mathfrak{p}\mathbf{B}}$. Como $\mathbf{B}$ es un anillo noetheriano, entonces por el corolario 3.2.2, existe un número finito de ideales primos minimales sobre $\mathfrak{p}\mathbf{B}$. Por tanto $\mathfrak{J}$ es un conjunto finito en $\mathbf{B}$. ■

3.3: Descomposición primaria en anillos noetherianos.

Esta sección tiene como objetivo principal demostrar que todo ideal propio en un anillo noetheriano puede descomponerse como intersección finita de ideales primarios; para ello se definen los ideales reducibles e irreducibles.

Definición 3.3.1: Un ideal $\mathfrak{a}$ en un anillo $\mathbf{A}$, se dice que es **reducible** si existen ideales $\mathfrak{b}, \mathfrak{c}$ en $\mathbf{A}$, tal que:

$$\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}, \quad \text{donde} \quad \mathfrak{a} \subsetneq \mathfrak{b} \quad \text{y} \quad \mathfrak{a} \subsetneq \mathfrak{c}.$$

Definición 3.3.2: Un ideal $\mathfrak{a}$ en un anillo $\mathbf{A}$, se dice que es **irreducible** si no existen ideales $\mathfrak{b}, \mathfrak{c}$ en $\mathbf{A}$, tal que:

$$\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}, \quad \text{donde} \quad \mathfrak{a} \subsetneq \mathfrak{b} \quad \text{y} \quad \mathfrak{a} \subsetneq \mathfrak{c}.$$

Lema 3.3.3: Sea $\mathbf{A}$ un anillo noetheriano. Todo ideal $\mathfrak{q} \neq (1)$ irreducible, es primario.

Demostración: Sea $\mathfrak{a}$ un ideal irreducible en $\mathbf{A}$.

Sean $a, b \in \mathbf{A}$ t. q. $ab \in \mathfrak{a}$, suponga que $a \notin \mathfrak{a}$. Se considera el ideal $\left(\mathfrak{a} : b^n\right)$ para $n \in \mathbb{N}$ y la cadena,

$$\mathfrak{a} \subseteq \left(\mathfrak{a} : b^1\right) \subseteq \left(\mathfrak{a} : b^2\right) \subseteq \left(\mathfrak{a} : b^3\right) \subseteq \ \cdot \ \cdot \ \cdot \ \subseteq \left(\mathfrak{a} : b^n\right) \subseteq \left(\mathfrak{a} : b^{n+1}\right) \subseteq \ \cdot \ \cdot \ \cdot \ .$$

Por ser $\mathbf{A}$ noetheriano, existe $n \in \mathbb{N}$ tal que $\left(\mathfrak{a} : b^n\right) = \left(\mathfrak{a} : b^{n+1}\right) = \left(\mathfrak{a} : b^{n+2}\right) = \cdots$.

Considere la intersección, $\left(\mathfrak{a} + (a)\right) \cap \left(\mathfrak{a} + (b^n)\right) = \mathfrak{c}$. Se demuestra que el ideal $\mathfrak{c}$ es igual a $\mathfrak{a}$.

Sea $x \in \mathfrak{c}$.

$$x \in \mathfrak{c} \ \Rightarrow \ x \in \mathfrak{a} + (a) \quad \text{y} \quad x \in \mathfrak{a} + (b^n)$$

$$\Rightarrow \ \exists \ c_1, c_2 \in \mathbf{A} \quad \text{y} \quad a_1, a_2 \in \mathfrak{a} \quad \text{t. q.} \quad x = a_1 + c_1 a = a_2 + c_2 b^n \quad .$$

Multiplicando por b lo anterior,

$$xb = a_1 b + c_1 ab = a_2 b + c_2 b^{n+1}.$$

Despejando $c_2 b^{n+1}$,

$$c_2 b^{n+1} = a_1 b + c_1 ab - a_2 b.$$

Donde todos los sumandos de la derecha están en $\mathfrak{a}$, por lo tanto $c_2 b^{n+1} \in \mathfrak{a}$. Luego $c_2 \in \left(\mathfrak{a} : b^{n+1}\right) = \left(\mathfrak{a} : b^n\right)$, de donde $c_2 b^n \in \mathfrak{a}$. Entonces $x = a_2 + c_2 b^n \in \mathfrak{a}$. Así,

$$\mathfrak{a} = \left(\mathfrak{a} + (a)\right) \cap \left(\mathfrak{a} + (b^n)\right).$$

Ahora como $\mathfrak{a}$ es irreducible, resulta $\mathfrak{a} = \mathfrak{a} + (a)$ ó $\mathfrak{a} = \mathfrak{a} + (b^n)$. Entonces:

$$\begin{aligned}
\mathfrak{a} = \mathfrak{a} + (a) \quad \text{ó} \quad \mathfrak{a} = \mathfrak{a} + (b^n) \; &\Rightarrow \; (a) \subseteq \mathfrak{a} \quad \text{ó} \quad (b^n) \subseteq \mathfrak{a} \\
&\Rightarrow \; a \in \mathfrak{a} \quad \text{ó} \quad b^n \in \mathfrak{a} \\
&\Rightarrow \; b^n \in \mathfrak{a}, \quad \left(a \notin \mathfrak{a}\right).
\end{aligned}$$

$\therefore$ $\mathfrak{a}$ es un ideal primario en $\mathbf{A}$.■

Teorema 3.3.4: Sea $\mathbf{A}$ un anillo noetheriano. Todo ideal $\mathfrak{q} \neq (1)$ es intersección finita de ideales primarios en $\mathbf{A}$.

Demostración:

De acuerdo con el lema 3.3.3, basta probar que todo ideal en $\mathbf{A}$ es una intersección finita de ideales irreducibles. Suponga lo contrario y considere la familia definida como sigue:

$$\Sigma = \left\{\mathfrak{q} \subsetneq \mathbf{A} \mid \mathfrak{q} \text{ no es intersección de un número finito de ideales irreducibles}\right\}.$$

Por lo supuesto $\Sigma \neq \emptyset$. Como $\mathbf{A}$ es un anillo noetheriano, existen elementos maximales en Σ. Sea $\mathfrak{a} \in \Sigma$ maximal.

Considere $\mathfrak{a} \in \Sigma$ irreducible. Si $\mathfrak{a}$ es irreducible y $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{a}$, entonces $\mathfrak{a} \notin \Sigma$, $(\rightarrow\leftarrow)$.

$$\therefore\ \mathfrak{a} \text{ es reducible.}$$

Si $\mathfrak{a}$ es reducible, existen ideales $\mathfrak{b}, \mathfrak{c}$ en $\mathbf{A}$, tal que:

$$\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}, \quad \text{donde} \quad \mathfrak{a} \subsetneq \mathfrak{b} \quad \text{y} \quad \mathfrak{a} \subsetneq \mathfrak{c}.$$

De lo anterior $\mathfrak{b}, \mathfrak{c} \notin \Sigma$, luego existen $\{\mathfrak{b}_1, \mathfrak{b}_2, \ldots, \mathfrak{b}_m\}$ y $\{\mathfrak{c}_1, \mathfrak{c}_2, \ldots, \mathfrak{c}_k\}$ conjuntos finitos de ideales irreducibles en $\mathbf{A}$ tal que:

$$\mathfrak{b} = \bigcap_{j=1}^{m} \mathfrak{b}_j \qquad \text{y} \qquad \mathfrak{c} = \bigcap_{j=1}^{k} \mathfrak{c}_j \ .$$

Sustituyendo $\mathfrak{b}$ y $\mathfrak{c}$ resulta que $\mathfrak{a}$ es intersección de un número finito de ideales irreducibles; lo es una contradicción. Por tanto $\Sigma = \emptyset$.

Así todo ideal en $\mathbf{A}$, es intersección de un número finito de ideales irreducibles, en consecuencia del lema 3.3.3, es intersección finita de ideales primarios.■

Observaciones:

(i) De acuerdo con el teorema 3.3.4, todo ideal $\mathfrak{q} \neq (1)$ en un anillo noetheriano $\mathbf{A}$, admite una descomposición primaria. De donde, todos los resultados de la sección 1 (**Capitulo 2**) son válidos para anillos noetherianos.

(ii) En consecuencia de la proposición 3.1.6, todo dominio de ideales principales $\mathbf{A}$, es noetheriano. Entonces todo ideal $\mathfrak{q} \neq (1)$ tiene una descomposición primaria.

Proposición 3.3.5: En un anillo $\mathbf{A}$ noetheriano cada ideal contiene una potencia de su radical.

Demostración:

Sea $\mathfrak{a}$ un ideal propio en $\mathbf{A}$. Se demuestra que existe $j \in \mathbb{N}$ tal que $\left(r(\mathfrak{a})\right)^j \subseteq \mathfrak{a}$.

Por hipótesis $\mathbf{A}$ es un anillo noetheriano, entonces $r(\mathfrak{a})$ es un ideal finitamente generado. Sea $\{x_1, \ldots, x_n\}$ un conjunto finito de generadores de $r(\mathfrak{a})$. Luego para cada $x_k \in r(\mathfrak{a})$, existe $n_k \in \mathbb{N}$ tal que $x_k^{n_k} \in \mathfrak{a} \quad \forall \quad k = 1, \ldots, n.$

Considere el elemento $m = \sum_{i=1}^{n} (n_i - 1) + 1.$

Observe un caso particular:

Se supone $r(\mathfrak{a}) = \mathbf{A}\,x_1 + \mathbf{A}\,x_2$ y $n_1 = 2$, $n_2 = 3$, entonces $x_1^{n_1}, x_2^{n_2} \in \mathfrak{a}$ y $m = 4$.

$$\left(r(\mathfrak{a})\right)^4 = \left(\mathbf{A}\,x_1 + \mathbf{A}\,x_2\right)^4 = \left(\mathbf{A}\,x_1 + \mathbf{A}\,x_2\right)^2 \left(\mathbf{A}\,x_1 + \mathbf{A}\,x_2\right)^2$$

$$\subseteq \left(\mathbf{A}\,x_1^2 + \mathbf{A}\,x_1x_2 + \mathbf{A}\,x_2^2\right)\left(\mathbf{A}\,x_1^2 + \mathbf{A}\,x_1x_2 + \mathbf{A}\,x_2^2\right)$$

$$\subseteq \mathbf{A}\,x_1^4 + \mathbf{A}\,x_1^3x_2 + \mathbf{A}\,x_1^2x_2^2 + \mathbf{A}\,x_1x_2^3 + \mathbf{A}\,x_2^4$$

$$\subseteq \left(\mathbf{A}\,x_1^2\right)x_1^2 + \left(\mathbf{A}\,x_1\,x_2\right)x_1^2 + \mathbf{A}\,x_1^2x_2^2 + \mathbf{A}\,x_1x_2^3 + \left(\mathbf{A}\,x_2\right)x_2^3 \subseteq \mathfrak{a}.$$

Luego $\left(r(\mathfrak{a})\right)^4$ es generado por el conjunto $\left\{x_1^4,\ x_1^3x_2,\ x_1^2x_2^2,\ x_1x_2^3,\ x_2^4\right\}$ con $\sum_{i=1}^{2} r_i = 4$ donde r_i son los exponentes de los x_k.

$$\therefore\ \left(r(\mathfrak{a})\right)^4 \subseteq \mathfrak{a}.$$

De forma general se tiene, $\left(r(\mathfrak{a})\right)^m$ es generado por los productos $x_1^{r_1}x_2^{r_2}\ \cdot\ \cdot\ \cdot\ x_j^{r_n}$ con $1 \le j \le n$ y $\sum_{i=1}^{n} r_i = m.$ Por la definición de m se tiene que $r_i \ge n_i$ para algún $1 \le i \le k,$ por tanto cada uno estos monomios está en $\mathfrak{a}.$ ■

Corolario 3.3.6: En un anillo $\mathbf{A}$ noetheriano el nilradical es nilpotente.

Demostración:

Se demuestra que existe $k \in \mathbb{N}$ tal que $\left(\mathfrak{R}_{\mathbf{A}}\right)^{k} = \mathbf{0}$. Tómese $\mathfrak{a} = \mathbf{0}$.

De la proposición anterior existe $k \in \mathbb{N}$ tal que $\left(r\left(\mathbf{0}\right)\right)^{k} \subseteq \mathbf{0}$. Por tanto $\left(r\left(\mathbf{0}\right)\right)^{k} = \mathbf{0}$, en consecuencia de la proposición 1.2.13 (1); $\mathfrak{R}_{\mathbf{A}} = r\left(\mathbf{0}\right)$. De donde $\left(\mathfrak{R}_{\mathbf{A}}\right)^{k} = \mathbf{0}$. ■

Corolario 3.3.7: Sea $\mathbf{A}$ un anillo noetheriano, $\mathfrak{m}$ un ideal maximal en $\mathbf{A}$, $\mathfrak{q}$ un ideal cualquiera en $\mathbf{A}$. Entonces las siguientes condiciones son equivalentes.

(i) $\mathfrak{q}$ es $\mathfrak{m}-$primario.

(ii) $r\left(\mathfrak{q}\right) = \mathfrak{m}$.

(iii) $\mathfrak{m}^{n} \subseteq \mathfrak{q} \subseteq \mathfrak{m}$ para algún $n \in \mathbb{N}$.

Demostración:

$\left(\mathrm{i}\right) \Rightarrow \left(\mathrm{ii}\right)$. $\left(\mathfrak{q} \text{ es } \mathfrak{m}-\text{primario}\right) \Rightarrow \left(r\left(\mathfrak{q}\right) = \mathfrak{m}\right)$, $\left(\text{Definición 2.1.5, } \left(\text{capitulo II}\right)\right)$.

$\left(\mathrm{ii}\right) \Rightarrow \left(\mathrm{iii}\right)$. De las proposiciones 3.3.5 y 1.2.15, inciso (i), se tiene

$$\left(r\left(\mathfrak{q}\right)\right)^{m} \subseteq \mathfrak{q} \quad \text{y} \quad \mathfrak{q} \subseteq r\left(\mathfrak{q}\right), \qquad \text{para algun } m \in \mathbb{N}.$$

Como $r(\mathfrak{q}) = \mathfrak{m}$, entonces

$$\mathfrak{m}^m \subseteq \mathfrak{q} \subseteq \mathfrak{m} \quad \text{para algun } m \in \mathbb{N}.$$

$(\text{iii}) \Rightarrow (\text{i})$. Si $\mathfrak{m}^n \subseteq \mathfrak{q} \subseteq \mathfrak{m}$ para algún $n \in \mathbb{N}$, entonces $\mathfrak{q}$ es $\mathfrak{m}-$primario, por el corolario 2.1.7, inciso (ii).■

Proposición 3.3.8: Sea $\mathfrak{a} \neq (1)$ un ideal en un anillo $\mathbf{A}$ noetheriano. Entonces los ideales primos asociados a $\mathfrak{a}$ son precisamente los ideales primos que aparecen en el conjunto de ideales $(\mathfrak{a} : x)$ para algún $x \in \mathbf{A}$.

Demostración:

Pasando al cociente $\mathbf{A}/\mathfrak{a}$ se supone que $\mathfrak{a} = 0$. Luego por el teorema 3.3.4 todo ideal en un anillo noetheriano es descomponible, más aun cada ideal tiene una descomposición primaria minimal.

Se demuestra que un ideal primo $\mathfrak{p}$ es un ideal primo asociado a un primario de la descomposición de $\mathfrak{a}$ si y sólo si existe $a \in \mathbf{A}$ tal que $\text{Ann}(a) = \mathfrak{p}$.

"$\Rightarrow$"

Sea $\mathbf{0}=\mathfrak{q}_1\cap\mathfrak{q}_2\cap...\cap\mathfrak{q}_n$ una descomposición primaria minimal del ideal cero y sea $\mathfrak{p}_i=r(\mathfrak{q}_i)$ $(1\le i\le n)$.

Sea $\mathfrak{a}_i=\bigcap\limits_{\substack{j=1\\ j\neq i}}^{n}\mathfrak{q}_j$. Como la descomposición primaria es minimal, entonces para algún

$$0\neq x\in\mathfrak{a}_i=\bigcap_{\substack{j=1\\ j\neq i}}^{n}\mathfrak{q}_j,\ \ x\notin\mathfrak{q}_i.$$

$$
\begin{aligned}
r(\operatorname{Ann}(x)) &= r(\mathbf{0}:x)\\
&= r\left(\bigcap_{i=1}^{n}\mathfrak{q}_i : x\right)\\
&= r\left(\left\{\bigcap_{\substack{j=1\\ j\neq i}}^{n}\mathfrak{q}_j\right\}\cap\mathfrak{q}_i : x\right)\\
&= r(\mathfrak{a}_i\cap\mathfrak{q}_i :\ x)\\
&= r((\mathfrak{a}_i : x)\cap(\mathfrak{q}_i : x))\\
&= r((1)\cap(\mathfrak{q}_i : x)), \qquad (\text{Lema } 2.1.9\ \ (\text{i}))
\end{aligned}
$$

$$= r\left(\left(\mathfrak{q}_i : x\right)\right)$$

$$= \mathfrak{p}_i, \qquad \left(\text{Lema 2.1.9 (ii)}\right).$$

Luego de la proposición 1.2.15, inciso (i) se tiene que $\operatorname{Ann}(x) \subseteq \mathfrak{p}_i$. Cada $\mathfrak{q}_i$ es $\mathfrak{p}_i$ – primario, en virtud de la proposición 3.3.5, existe $k \in \mathbb{N}$ tal que $\mathfrak{p}_i^k \subseteq \mathfrak{q}_i$, de donde,

$$\mathfrak{a}_i \mathfrak{p}_i^k \subseteq \mathfrak{a}_i \cap \mathfrak{p}_i^k \subseteq \mathfrak{a}_i \cap \mathfrak{q}_i = \bigcap_{\substack{j=1 \\ j \neq i}}^{n} \mathfrak{q}_j \cap \mathfrak{q}_i = \bigcap_{i=1}^{n} \mathfrak{q}_i = \mathbf{0}.$$

Sea $k \geq 1$ el menor entero tal que $\mathfrak{a}_i \mathfrak{p}_i^k = 0$, y sea x un elemento no nulo $\mathfrak{a}_i \mathfrak{p}_i^{k-1}$.

$$x \in \mathfrak{a}_i \mathfrak{p}_i^{k-1} \quad \Rightarrow \quad x = \sum_{j=1}^{s} a_j y_j, \quad \text{donde } a_j \in \mathfrak{a}_i \quad \text{y} \quad y_j \in \mathfrak{p}_i^{k-1}$$

$$\Rightarrow \quad xt = \sum_{j=1}^{s} a_j \left(y_j t\right) \quad \text{para todo } t \in \mathfrak{p}$$

$$\Rightarrow \quad t \in \mathfrak{p} \quad \text{y} \quad y_j \in \mathfrak{p}_i^{k-1} \quad \text{para todo } j = 1, \ldots, s$$

$$\Rightarrow \quad y_j t \in \mathfrak{p}_i^{k-1} \mathfrak{p} = \mathfrak{p}_i^k \quad \text{para todo } j = 1, \ldots, s$$

$$\Rightarrow \quad a_j y_j t \in \mathfrak{a}_i \mathfrak{p}_i^k = \mathbf{0} \quad \text{para todo } j = 1, \ldots, s$$

$$\Rightarrow \quad a_j y_j t = 0 \quad \text{para todo } j = 1, \ldots, s$$

$$\Rightarrow \quad xt = \sum_{j=1}^{s} a_j \left(y_j t \right) = 0 \quad \text{para todo } t \in \mathfrak{p}$$

$$\Rightarrow \quad x\mathfrak{p}_i = 0.$$

Sea $y \in \mathfrak{p}_i$. Si $y \in \mathfrak{p}_i$, entonces $xy = 0$ de donde $y \in \operatorname{Ann}(x)$. Luego $\mathfrak{p}_i \subseteq \operatorname{Ann}(x)$, por tanto $\mathfrak{p}_i = \operatorname{Ann}(x)$.

$"\Leftarrow"$

Recíprocamente sea $\mathfrak{p}$ un ideal primo en $\mathbf{A}$ tal que $\mathfrak{p} = \operatorname{Ann}(x)$ para algún $x \neq 0 \in \mathbf{A}/\mathfrak{a}$.

Si $\mathfrak{p} = \operatorname{Ann}(x)$, entonces $\mathfrak{p} = r(\operatorname{Ann}(x)) = r(\mathbf{0} : x)$, en consecuencia del **primer teorema de unicidad**, $\mathfrak{p}$ es un ideal primo asociado al ideal cero. ■

Proposición 3.3.9: Sea $\mathbf{A}$ un anillo noetheriano y $\mathfrak{a}$ un ideal en $\mathbf{A}$. Sea $\mathfrak{a} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n = \mathfrak{q}_1' \cap \ldots \cap \mathfrak{q}_n'$ dos descomposiciones primarias minimales de primos asociados $r(\mathfrak{q}_i') = r(\mathfrak{q}_i) = \mathfrak{p}_i$ $(1 \leq i \leq n)$. Se verifica:

$$\mathfrak{a} = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \ldots \cap \mathfrak{q}_{j-1} \cap \mathfrak{q}_j' \cap \mathfrak{q}_{j+1} \cap \ldots \cap \mathfrak{q}_n, \text{ para todo } 1 \leq j \leq n.$$

Demostración:

Reordenando los ideales con respecto a la inclusión se supone que, $\mathfrak{q}_i \subseteq \mathfrak{p}_k$ para todo $i \leq k$ donde $1 \leq k \leq n$. Tomando radicales:

$$\mathfrak{p}_i = r\left(\mathfrak{q}_i\right) \subseteq \mathfrak{p}_k \quad \text{con } i \leq k.$$

Se considera el sistema multiplicativo $\mathbf{S} = \mathbf{A} - \mathfrak{p}_k$, entonces $\mathfrak{p}_i \cap \mathbf{S} = \varnothing$ para todo $i \leq k$.

De donde por el **segundo teorema de unicidad**,

$$\mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_{k-1} = \mathfrak{q}_1' \cap \ldots \cap \mathfrak{q}_{k-1}', \quad \text{para todo } 1 \leq k \leq n.$$

Intersectando $\mathfrak{q}_k'$ en ambos lados:

$$\mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_{k-1} \cap \mathfrak{q}_k' = \mathfrak{q}_1' \cap \ldots \cap \mathfrak{q}_{k-1}' \cap \mathfrak{q}_k' = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_{k-1} \cap \mathfrak{q}_k.$$

Intersectando $\mathfrak{q}_{k+1} \cap \ldots \cap \mathfrak{q}_n$ en ambos lados de la igualdad anterior se obtiene:

$$\mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_{k-1} \cap \mathfrak{q}_k' \cap \mathfrak{q}_{k+1} \cap \ldots \cap \mathfrak{q}_n = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_{k-1} \cap \mathfrak{q}_k \cap \mathfrak{q}_{k+1} \cap \ldots \cap \mathfrak{q}_n = \mathfrak{a}.$$

De donde:

$$\therefore\ \mathfrak{a} = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \ldots \cap \mathfrak{q}_{j-1} \cap \mathfrak{q}_j' \cap \mathfrak{q}_{j+1} \cap \ldots \cap \mathfrak{q}_n. \blacksquare$$

3.4: Anillos de Artin.

En esta sección se define una clase muy particular de anillos, frente a la generalidad del concepto de anillos noetherianos, los anillos de Artin. Se demuestra la existencia de un número finito de ideales maximales en un anillo de Artin.

Definición 3.4.1: Un anillo $\mathbf{A}$ verifica la condición **minimal,** si toda familia no vacía de ideales, ordenadas por la inclusión, tiene elemento minimal.

Definición 3.4.2: Un anillo $\mathbf{A}$ verifica la **condición de cadena descendente,** si toda cadena descendente de ideales en $\mathbf{A}$ es **estacionaria**, esto es, si:

$$\mathfrak{a}_1 \supseteq \mathfrak{a}_2 \supseteq \cdots \supseteq \mathfrak{a}_m \supseteq \mathfrak{a}_{m+1} \supseteq \cdots.$$

Es una cadena descendente de ideales en $\mathbf{A}$, entonces existe $m \in \mathbb{N}$ tal que $\mathfrak{a}_m = \mathfrak{a}_{m+1} = \mathfrak{a}_{m+2} = \cdots$.

Proposición 3.4.3: Sea $\mathbf{A}$ un anillo. Son equivalentes los enunciados siguientes:

(i) $\mathbf{A}$ verifica la condición minimal.

(ii) $\mathbf{A}$ verifica la condición de cadena descendente.

Demostración:

$(i) \Rightarrow (ii)$.

Sea $\mathfrak{a}_1 \supseteq \mathfrak{a}_2 \supseteq \cdots \supseteq \mathfrak{a}_m \supseteq \mathfrak{a}_{m+1} \supseteq \cdots$ una cadena descendente de ideales en $\mathbf{A}$.

Entonces la familia:

$$\Gamma = \left\{ \mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_m, \mathfrak{a}_{m+1}, \ldots \right\},$$

tiene elemento minimal. Sea $\mathfrak{a}_j \in \Gamma$ minimal; por tanto para todo $h \in \mathbb{N}$ con $h \geq j$ se verifica que $\mathfrak{a}_h = \mathfrak{a}_j$, luego la cadena es estacionaria.

$\therefore$ $\mathbf{A}$ verifica la condición de cadena descendente.

$(ii) \Rightarrow (i)$.

Sea $\Gamma \neq \varnothing$ una familia de ideales en $\mathbf{A}$, ordenada por la inclusión. Suponga que Γ no tiene elemento minimal.

Sea $\mathfrak{b}_1 \in \Gamma$.

Como Γ no tiene elemento minimal, entonces existe un ideal $\mathfrak{b}_2 \in \Gamma$ tal que,

$$\mathfrak{b}_1 \supsetneqq \mathfrak{b}_2.$$

De nuevo $\mathfrak{b}_2$ no es minimal, entonces existe un ideal $\mathfrak{b}_3 \in \Gamma$ tal que

$$\mathfrak{b}_1 \supsetneqq \mathfrak{b}_2 \supsetneqq \mathfrak{b}_3.$$

Sucesivamente para cada índice j se tiene que $\mathfrak{a}_j$ no es minimal, entonces existe $\mathfrak{a}_{j+1} \in \Gamma$ tal que

$$\mathfrak{a}_1 \supsetneqq \mathfrak{a}_2 \supsetneqq \mathfrak{a}_3 \cdots \supsetneqq \mathfrak{a}_{j-1} \supsetneqq \mathfrak{a}_j \supsetneqq \mathfrak{a}_{j+1} \supsetneqq \cdots .$$

Luego se ha construido una cadena descendente de ideales en $\mathbf{A}$, que no es finalmente constante.

$\therefore$ $\mathbf{A}$ verifica la condición minimal.■

Definición 3.4.4: Un anillo que verifica las condiciones equivalentes de la proposición 3.4.3, se llama **artiniano**.

Proposición 3.4.5: Sea $\mathbf{A}$ un anillo artiniano, $\mathfrak{a}$ un ideal de $\mathbf{A}$. Entonces $\mathbf{A}/\mathfrak{a}$ es un anillo artiniano.

Demostración:

Sea $\mathfrak{F} = \{\mathfrak{b}_i \subseteq \mathbf{A}/\mathfrak{a} \mid i \in \mathbb{N}\}$ un conjunto no vacío de ideales en el anillo $\mathbf{A}/\mathfrak{a}$. En consecuencia de la proposición 1.1.14; $\mathfrak{J} = \{\pi^{-1}(\mathfrak{b}_i) \subseteq \mathbf{A} \mid i \in \mathbb{N}\}$ es una familia no vacía de ideales en $\mathbf{A}$, donde $\pi : \mathbf{A} \to \mathbf{A}/\mathfrak{a}, x \to x + \mathfrak{a}$ el epimorfismo canónico. Por ser $\mathbf{A}$ un anillo de Artin, $\mathfrak{J}$ tiene elemento minimal; sea $\pi^{-1}(\mathfrak{b}_{i_0})$ su elemento minimal.

Se demuestra que $\mathfrak{b}_{i_0}$ es minimal de $\mathfrak{F}$. Supóngase que existe $\mathfrak{b}_i \in \mathfrak{F}$ tal que $\mathfrak{b}_i \subseteq \mathfrak{b}_{i_0}$.

Tomando imagen inversa se tiene,

$$\pi^{-1}\left(\mathfrak{b}_i\right) \subseteq \pi^{-1}\left(\mathfrak{b}_{i_0}\right).$$

Por la minimalidad, de $\pi^{-1}\left(\mathfrak{b}_{i_0}\right)$,

$$\pi^{-1}\left(\mathfrak{b}_i\right) = \pi^{-1}\left(\mathfrak{b}_{i_0}\right).$$

Aplicando π a lo anterior:

$$\pi\left(\pi^{-1}\left(\mathfrak{b}_i\right)\right) = \pi\left(\pi^{-1}\left(\mathfrak{b}_{i_0}\right)\right).$$

Lo que equivale a

$$\mathfrak{b}_i = \mathfrak{b}_{i_0}.$$

Luego $\mathfrak{b}_{i_0}$ es el elemento minimal de $\mathfrak{F}$. De acuerdo con la proposición 3.4.4, $\mathbf{A}/\mathfrak{a}$ es un anillo de Artin.■

Proposición 3.4.6: Si $\mathbf{A}$ es un dominio artiniano, entonces $\mathbf{A}$ es un cuerpo.

Demostración:

Se demuestra que $\mathbf{A}$ es un cuerpo para ello se verifican las condiciones de la definición 1.1.7; es decir:

(1) $1 \neq 0,\ \left(1 \in \mathbf{A}\right).$

(2) Cada elemento no nulo en $\mathbf{A}$ es una unidad.

Demostración (1):

Suponga $1 = 0.$ Si $1 = 0,$ entonces $\mathbf{A} = \{0\}$ $\left(\rightarrow\leftarrow\right),$ $\left(\mathbf{A}\right.$ es un dominio integro$\left.\right).$

$$\therefore 1 \neq 0.$$

Demostración (2):

Sea $0 \neq x \in \mathbf{A}.$ Considere la cadena descendente de ideales en $\mathbf{A}$:

$$(x) \supseteq (x^2) \supseteq \cdot\ \cdot\ \cdot \supseteq (x^n) \supseteq (x^{n+1}) \supseteq \cdot\ \cdot\ \cdot\ \cdot\ .$$

Dado que $\mathbf{A}$ es artiniano, verifica la condición de cadena descendente, entonces existe $m \in \mathbb{N}$ tal que $(x^m) = (x^{m+1}).$

$$(x^m) = (x^{m+1}) \ \Rightarrow\ \exists\ \ y \in \mathbf{A}\quad \text{t. q.}\quad x^m = yx^{m+1}$$

$$\Rightarrow\ \exists\ \ y \in \mathbf{A}\quad \text{t. q.}\quad x^m\left(1 - yx\right) = 0$$

$$\Rightarrow\ x^m = 0\quad \text{ó}\quad 1 - yx = 0,\qquad \left(\mathbf{A}\ \text{es un dominio}\right)$$

$\Rightarrow \quad 1 - yx = 0$

$\Rightarrow \quad yx = 1$

$\Rightarrow \quad x$ es una unidad.

Luego todo elemento distinto de cero es una unidad en $\mathbf{A}$. Entonces en consecuencia de la proposición 1.1.7, $\mathbf{A}$ es un cuerpo.■

Corolario 3.4.7: En un anillo $\mathbf{A}$ de Artin cada ideal primo es maximal.

Demostración:

Sea $\mathfrak{p}$ un ideal primo en $\mathbf{A}$.

$$\begin{aligned}(\mathfrak{p} \text{ un ideal primo en } \mathbf{A}) \quad &\Rightarrow \quad (\mathbf{A}/\mathfrak{p} \text{ es un dominio de Artin}), \ (\text{Proposicion (1.2.3 (i), 3.4.5})\\ &\Rightarrow \quad (\mathbf{A}/\mathfrak{p} \text{ es un cuerpo}), \ (\text{Proposicion } 3.4.6)\\ &\Rightarrow \quad (\mathfrak{p} \text{ es un ideal maximal en } \mathbf{A}), \ (\text{Proposicion } 1.2.3 \text{ (ii)}).\end{aligned}$$

$\therefore$ Todo ideal primo en un anillo de Artin es maximal. ■

Corolario 3.4.8: Si $\mathbf{A}$ es un anillo artiniano, $\mathfrak{R}_{\mathbf{A}} = \mathfrak{I}_{\mathbf{A}}$.

Demostración:

$$\mathfrak{R}_{\mathbf{A}} = \bigcap \{\mathfrak{p}_k \mid \mathfrak{p}_k \text{ es un ideal primo de } \mathbf{A}\}$$

$$= \bigcap \{\mathfrak{m}_k \mid \mathfrak{m}_k \text{ es un ideal maximal de } \mathbf{A}\} \quad (\text{Corolario } 3.4.7)$$

$$= \mathfrak{I}_{\mathbf{A}}.$$

Se concluye que un anillo de artin el $\mathfrak{R}_{\mathbf{A}} = \mathfrak{I}_{\mathbf{A}}$. ■

Proposición 3.4.9: En un anillo artiniano $\mathbf{A}$, existe sólo un número finito de ideales maximales.

Demostración:

Sea $\mathbf{A} \neq 0$ un anillo de artin. De acuerdo con la proposición 1.2.5, existe al menos un ideal maximal de $\mathbf{A}$.

Supóngase que no existe un número finito de ideales maximales en $\mathbf{A}$. Si es así, entonces existe una sucesión $\{\mathfrak{m}_i\}_{i\in\mathbb{N}}$ de ideales maximales de $\mathbf{A}$ tal que $\mathfrak{m}_k \neq \mathfrak{m}_h$ para $h \neq k$.

Se construye el conjunto:

$$\Gamma = \left\{ \mathbf{I}_r \subseteq \mathbf{A} \;\middle|\; \mathbf{I}_r = \bigcap_{i=1}^{r} \mathfrak{m}_i, \;\; \text{donde } r \in \mathbb{N} \text{ y los } \mathfrak{m}_i \text{ son ideales maximales} \right\}.$$

Considere la cadena descendente de elementos de Γ.

$$\mathbf{I}_1 \supseteq \mathbf{I}_2 \supseteq \cdot\cdot\cdot \supseteq \mathbf{I}_m \supseteq \mathbf{I}_{m+1} \supseteq \cdot\cdot\cdot\cdot.$$

Como $\mathbf{A}$ es un anillo de artin, la cadena anterior es estacionaria y por tanto existe $n \in \mathbb{N}$ tal que $\mathbf{I}_n = \mathbf{I}_{n+1} = \cdot\cdot\cdot$. De donde:

$$\bigcap_{i=1}^{n} \mathfrak{m}_i = \bigcap_{i=1}^{n+1} \mathfrak{m}_i \subseteq \mathfrak{m}_{n+1}.$$

Del inciso (ii) de la proposición 1.2.9,

$$\mathfrak{m}_i \subseteq \mathfrak{m}_{n+1} \qquad \text{para algún } 1 \leq i \leq n.$$

Por la maximalidad de $\mathfrak{m}_i$,

$$\mathfrak{m}_i = \mathfrak{m}_{n+1} \qquad \text{para algún } 1 \leq i \leq n.$$

Lo cual contradice él supuesto. Luego en un anillo de artin, existe sólo un número finito de ideales maximales.■

Corolario 3.4.10: En un anillo $\mathbf{A}$ de Artin el nilradical es el producto de los ideales maximales.

Demostración:

De la proposición 3.4.9, los ideales maximales en un anillo de Artin son un número finito. Sea $\{\mathfrak{m}_1, \ldots, \mathfrak{m}_k\}$ el conjunto de ideales maximales distintos.

Se demuestra que para todo $1 \leq i, j \leq k$ con $i \neq j$, $\mathfrak{m}_j$, $\mathfrak{m}_i$ son comaximales. Supóngase que $\mathfrak{m}_j$, $\mathfrak{m}_i$ no son comaximales para algunos $i \neq j$; es decir, $\mathfrak{m}_j + \mathfrak{m}_i \neq (1)$.

$$\begin{aligned}
\mathfrak{m}_j \subseteq \mathfrak{m}_j + \mathfrak{m}_i \neq (1) \quad &\Rightarrow \quad \mathfrak{m}_j = \mathfrak{m}_j + \mathfrak{m}_i, \quad (\text{Maximalidad } \mathfrak{m}_j) \\
&\Rightarrow \quad \mathfrak{m}_i \subseteq \mathfrak{m}_j \neq (1) \\
&\Rightarrow \quad \mathfrak{m}_i = \mathfrak{m}_j, \quad (\rightarrow\leftarrow) \quad (\text{Maximalidad } \mathfrak{m}_i).
\end{aligned}$$

Se deduce que para todo $1 \leq i, j \leq k$ con $i \neq j$, $\mathfrak{m}_j$, $\mathfrak{m}_i$ son comaximales. Luego de la proposición 1.2.22, inciso (i):

$$\bigcap_{j=1}^{k} \{\mathfrak{m}_j \mid \mathfrak{m}_j \text{ es un ideal maximal de } \mathbf{A}\} = \prod_{j=1}^{k} \{\mathfrak{m}_j \mid \mathfrak{m}_j \text{ es un ideal maximal de } \mathbf{A}\}$$

De donde:

$$\mathfrak{R}_{\mathbf{A}} = \prod_{j=1}^{k} \{\mathfrak{m}_j \mid \mathfrak{m}_j \text{ es un ideal maximal de } \mathbf{A}\}.$$

Se concluye que en un anillo de Artin el nilradical es el producto de los ideales maximales.■

En consecuencia de las propiedades anteriores en un anillo $\mathbf{A}$ de Artin, se verifica lo siguiente:

1. $\dim(\mathbf{A}) = 0.$
2. Existe un número finito de ideales primos en $\mathbf{A}$.
3. Por la definición 1.2.20, los anillos de Artin son **semilocales.**

Corolario 3.4.11: Si $\mathbf{A}$ es un anillo de Artin, el cociente $\mathbf{A}/\mathfrak{I}_{\mathbf{A}}$ es isomorfo a un producto de cuerpos.

Demostración:

En un anillo de Artin existe un número finto de ideales maximales. Sea estos $\{\mathfrak{m}_1, \ldots, \mathfrak{m}_k\}$. Se tiene para todo $1 \le i, j \le k$ con $i \neq j$, $\mathfrak{m}_j$, $\mathfrak{m}_i$ son comaximales. Además $\mathfrak{I}_{\mathbf{A}} = \bigcap_{j=1}^{k} \mathfrak{m}_j$, luego por la proposición 1.2.22, inciso (ii) el homomorfismo φ:

$$\varphi : \mathbf{A} \to \prod_{i=1}^{n} (\mathbf{A}/\mathfrak{m}_i) .$$

Es sobreyectiva con núcleo $\mathfrak{I}_{\mathbf{A}} = \bigcap_{j=1}^{k} \mathfrak{m}_j$. De acuerdo con la proposición 1.1.13, existe un isomorfismo:

$$\mathbf{A}/\mathfrak{I}_{\mathbf{A}} \cong \mathbf{Im}(\varphi) = \prod_{j=1}^{k} (\mathbf{A}/\mathfrak{m}_j).$$

De donde en un anillo de Artin, el cociente $\mathbf{A}/\mathfrak{I}_{\mathbf{A}}$ es isomorfo a un producto de cuerpos.■

Proposición 3.4.12: En un anillo $\mathbf{A}$ de Artin el nilradical es nilpotente.

Demostración:

Sea $\mathbf{A}$ un anillo de artin y $\mathfrak{R}_{\mathbf{A}}$ el nilradical de $\mathbf{A}$. Se demuestra que existe $m \in \mathbb{N}$ tal que $(\mathfrak{R}_{\mathbf{A}})^m = \mathbf{0}$.

Considere la cadena:

$$\mathfrak{R}_{\mathbf{A}} \supseteq \mathfrak{R}_{\mathbf{A}}^2 \supseteq \cdot \cdot \cdot \supseteq \mathfrak{R}_{\mathbf{A}}^n \supseteq \mathfrak{R}_{\mathbf{A}}^{n+1} \supseteq \cdot \cdot \cdot \cdot .$$

Como $\mathbf{A}$ es artiniano existe $n \in \mathbb{N}$ tal que $\mathfrak{R}_{\mathbf{A}}^n = \mathfrak{R}_{\mathbf{A}}^{n+1} = \mathfrak{R}_{\mathbf{A}}^{n+2} \cdot \cdot \cdot \cdot$. Supóngase que $\mathfrak{R}_{\mathbf{A}}$ no es nilpotente; es decir $(\mathfrak{R}_{\mathbf{A}})^n \neq \mathbf{0}$ para todo $n \in \mathbb{N}$.

Se llama Γ al conjunto,

$$\Gamma = \left\{ \mathfrak{a} \subseteq \mathbf{A} \mid \mathfrak{a}\mathfrak{R}_{\mathbf{A}}^n \neq \mathbf{0} \right\}.$$

Como $\mathfrak{R}_{\mathbf{A}}$ no es nilpotente, se tiene que $\mathfrak{R}_{\mathbf{A}}\mathfrak{R}_{\mathbf{A}}^n = \mathfrak{R}_{\mathbf{A}}^{n+1} = \mathfrak{R}_{\mathbf{A}}^n \neq 0$, por tanto $\mathfrak{R}_{\mathbf{A}} \in \Gamma$, de donde $\Gamma \neq \varnothing$. De nuevo por ser $\mathbf{A}$ artiniano, existe $\mathfrak{c} \in \Gamma$ minimal.

$$\mathfrak{c} \in \Gamma \quad \Rightarrow \quad \mathfrak{c}\mathfrak{R}_{\mathbf{A}}^{n} \neq \mathbf{0}$$

$$\Rightarrow \quad \exists \quad 0 \neq x \in \mathfrak{c} \quad \text{t. q.} \quad x\mathfrak{R}_{\mathbf{A}}^{n} \neq \mathbf{0}$$

$$\Rightarrow \quad (x) \in \Gamma \quad \text{y} \quad (x) \subseteq \mathfrak{c}$$

$$\Rightarrow \quad (x) = \mathfrak{c}, \quad \left(\text{Minimalidad de } \mathfrak{c}\right).$$

También se verifica la relación:

$$\left(x\mathfrak{R}_{\mathbf{A}}\right)\mathfrak{R}_{\mathbf{A}}^{n} = x\mathfrak{R}_{\mathbf{A}}\mathfrak{R}_{\mathbf{A}}^{n} = x\mathfrak{R}_{\mathbf{A}}^{n+1} = x\mathfrak{R}_{\mathbf{A}}^{n} \neq 0.$$

De donde $x\mathfrak{R}_{\mathbf{A}} \in \Gamma$ y $x\mathfrak{R}_{\mathbf{A}} \subseteq (x) = \mathfrak{c}$ por la minimalidad de $\mathfrak{c}$ se tiene $x\mathfrak{R}_{\mathbf{A}} = \mathfrak{c} = (x)$. Entonces existe $y \in \mathfrak{R}_{\mathbf{A}}$, tal que $x = yx$. Multiplicando por y repetidas veces se obtiene, $x = xy = xy^2 = \cdot \cdot \cdot = xy^t = xy^{t+1} = xy^{t+2} = \cdot \cdot \cdot$.

Pero $y \in \mathfrak{R}_{\mathbf{A}}$, entonces existe $t \in \mathbb{N}$ tal que $y^t = 0$, por tanto $x = xy^t = 0$. Lo que contradice la elección del x. Luego $\mathfrak{R}_{\mathbf{A}}$ es nilpotente.■

3.5: Caracterización de los anillos de Artin.

El propósito de esta sección es demostrar el teorema de **caracterización** y **estructura de los anillos de Artin**, pero antes se dan algunas propiedades previas sobre módulos noetherianos y artinianos, que serán de mucha utilidad.

Los elementos relacionados con la teoría de módulos noetherianos y artinianos, que a continuación se enuncian no se demuestran; debido a que la teoría de módulos no está dentro de los objetivos de la investigación; no obstante para el lector interesado con estos resultados puede consultar **[1]** pag. 81-86 y **[4]** pag. 4 - 6.

Sea $\mathbf{A}$ un anillo local y $\mathfrak{m}$ su ideal maximal. Si $\mathbf{M}$ es un $\mathbf{A}-$ módulo de generación finita. $\mathbf{M}/\mathfrak{m}\mathbf{M}$ es anulado por $\mathfrak{m}$, luego $\mathbf{M}/\mathfrak{m}\mathbf{M}$ es un $\mathbf{A}/\mathfrak{m}-$módulo, es decir un $\mathbf{A}/\mathfrak{m}-$espacio vectorial.

Definición 3.5.1: Sea $\mathbf{A}$ un anillo y $\mathbf{M}$ un $\mathbf{A}-$ módulo, $\mathbf{M}$ es un $\mathbf{A}-$ módulo **noetheriano**, si toda cadena ascendente

$$\mathbf{N}_1 \subseteq \mathbf{N}_2 \subseteq \ \cdot\ \cdot\ \cdot\ \subseteq \mathbf{N}_m \subseteq \mathbf{N}_{m+1} \subseteq \ \cdot\ \cdot\ \cdot\ ,$$

de submódulos de $\mathbf{M}$, es estacionaria.

Definición 3.5.2: Sea $\mathbf{A}$ un anillo y $\mathbf{M}$ un $\mathbf{A}-$ módulo: $\mathbf{M}$ es un $\mathbf{A}-$ módulo **artiniano**, si toda cadena descendente,

$$\mathbf{N}_1 \supseteq \mathbf{N}_2 \supseteq \ \cdot\ \cdot\ \cdot\ \supseteq \mathbf{N}_m \supseteq \mathbf{N}_{m+1} \supseteq \ \cdot\ \cdot\ \cdot\ ,$$

de submódulos de $\mathbf{M}$, es estacionaria.

Considere un caso particular de módulos sobre un cuerpo $\mathbf{A}$; es decir un $\mathbf{k}-$ espacio vectorial.

Proposición 3.5.3: Sea $\mathbf{A}$ un cuerpo y $\mathbf{M}$ un $\mathbf{A}-$espacio vectorial, las siguientes propiedades son equivalentes:

(i) $\mathbf{M}$ es un $\mathbf{A}-$módulo noetheriano.

(ii) $\mathbf{M}$ es un $\mathbf{A}-$módulo artiniano.

Definición 3.5.4: Se dirá que una sucesión de homomorfismos de $\mathbf{A}-$módulos

$$\cdots \to \mathbf{M}_{n-1} \xrightarrow{f_n} \mathbf{M}_n \xrightarrow{f_{n+1}} \mathbf{M}_{n+1} \to \cdots,$$

es exacta cuando $\mathbf{Im}(f_n) = \mathbf{ker}(f_{n+1})$ para todo $n \in \mathbb{Z}$.

Casos concretos:

1. $\mathbf{0} \to \mathbf{N} \xrightarrow{i} \mathbf{M}$ es una sucesión exacta si y sólo si i es inyectiva.

2. $\mathbf{M} \xrightarrow{\pi} \mathbf{M}'' \to \mathbf{0}$ es una sucesión exacta si y sólo si π es epimorfismo.

3. $\mathbf{0} \to \mathbf{M}' \xrightarrow{i} \mathbf{M} \xrightarrow{\pi} \mathbf{M}'' \to \mathbf{0}$ es exacta si y sólo si i es inyectiva, π es sobreyectiva y $\mathbf{ker}(\pi) = \mathbf{Im}(i)$.

Proposición 3.5.5: Sea $\mathbf{A}$ un anillo y

$$\mathbf{0} \to \mathbf{M}' \xrightarrow{f} \mathbf{M} \xrightarrow{g} \mathbf{M}'' \to \mathbf{0},$$

una sucesión exacta corta de $\mathbf{A}-$ módulos. Las propiedades siguientes son equivalentes:

(i) $\mathbf{M}$ es un $\mathbf{A}-$ módulo (noetheriano ó artiniano).

(ii) $\mathbf{M}'$ y $\mathbf{M}''$ son $\mathbf{A}-$ módulos (noetherianos ó artinianos).

Corolario 3.5.6: Sea $\mathbf{A}$ un anillo y $\mathbf{M}$ un $\mathbf{A}-$ módulo. Se considera una cadena finita de submódulos en $\mathbf{M}$:

$$\{\mathbf{0}\} = \mathbf{M}_0 \subsetneq \mathbf{M}_1 \subsetneq \mathbf{M}_2 \subsetneq \ \cdot \ \cdot \ \cdot \ \subsetneq \mathbf{M}_{r-1} \subsetneq \mathbf{M}_r = \mathbf{M}.$$

Las propiedades siguientes son equivalentes:

(i) $\mathbf{M}$ es un $\mathbf{A}-$ módulo (noetheriano ó artiniano).

(ii) Cada cociente $\mathbf{M}_i / \mathbf{M}_{i-1}$, $i = 1, \ldots, r$, es un $\mathbf{A}-$ módulo (noetheriano ó artiniano).

Definición 3.5.7: Un anillo $\mathbf{A}$ es (**noetheriano** ó **artiniano**) si lo es como $\mathbf{A}-$ módulo.

Observación 3.5.8: Sea $\mathbf{A}$ un anillo, $\mathfrak{a} \subseteq \mathbf{A}$ un ideal y $\mathbf{M}$ un $\mathbf{A}-$ módulo tal que $\mathfrak{a}\mathbf{M} = 0$. $\mathbf{M}$ es un $\mathbf{A}/\mathfrak{a}-$ módulo, todos los submódulos $\mathbf{N}$ de $\mathbf{M}$ verifican $\mathfrak{a}\mathbf{N} = \mathbf{0}$. $\mathbf{M}$ es (noetheriano ó artiniano) como $\mathbf{A}-$ módulo si y sólo si $\mathbf{M}$ es (noetheriano ó artiniano) como $\mathbf{A}/\mathfrak{a}-$ módulo.

Dada una cadena ascendente de $\mathbf{A}-$submódulos de $\mathbf{M}$:

$$\mathbf{N}_1 \subseteq \mathbf{N}_2 \subseteq \cdot\cdot\cdot \subseteq \mathbf{N}_n \subseteq \mathbf{N}_{n+1} \subseteq \cdot\cdot\cdot\cdot \quad (1)$$

Si $\mathbf{M}$ es un $\mathbf{A}-$módulo noetheriano, entonces existe $n \in \mathbb{N}$ tal que $\mathbf{N}_n = \mathbf{N}_{n+1} = \cdot\cdot\cdot$. Los $\mathbf{N}_j$ tienen estructura de $\mathbf{A}/\mathfrak{a}-$submódulos; de donde la cadena en (1) se estaciona como $\mathbf{A}/\mathfrak{a}-$submódulos. Luego $\mathbf{M}$ es un $\mathbf{A}/\mathfrak{a}-$módulo noetheriano.

Lema 3.5.9: Sea $\mathbf{A}$ un anillo en el que existen ideales maximales $\mathfrak{m}_1, \ldots, \mathfrak{m}_s$, no necesariamente distintos, tal que $\mathbf{0} = \prod_{i=1}^{s} \mathfrak{m}_i$. Entonces las condiciones siguientes son equivalentes:

(i) $\mathbf{A}$ es un anillo noetheriano.

(ii) $\mathbf{A}$ es un anillo artiniano.

Demostración:

Considere la cadena ascendente de ideales de $\mathbf{A}$:

$$\{0\} = \mathfrak{m}_1 \cdot\cdot\cdot \mathfrak{m}_s \subseteq \mathfrak{m}_1 \cdot\cdot\cdot \mathfrak{m}_{s-1} \subseteq \cdot\cdot\cdot \subseteq \mathfrak{m}_1\mathfrak{m}_2 \subseteq \mathfrak{m}_1 \subsetneq \mathbf{A}.$$

Cada $\mathbf{Q}_i = \mathfrak{m}_1 \cdot\cdot\cdot \mathfrak{m}_{i-1} / \mathfrak{m}_1 \cdot\cdot\cdot \mathfrak{m}_i$, $i = 1, \ldots s$, es un $\mathbf{A}-$módulo anulado por $\mathfrak{m}_i$ y por tanto es un $\mathbf{A}/\mathfrak{m}_i-$espacio vectorial.

$(\mathbf{A} \text{ es un anillo de Noether}) \Leftrightarrow (\mathbf{A} \text{ es un } \mathbf{A}-\text{módulo noetheriano}), (\text{Def. } 3.5.7)$

$\Leftrightarrow (\mathbf{Q}_i \text{ es un } \mathbf{A}-\text{módulo noetheriano}), (\text{Coro. } 3.5.6)$

$\Leftrightarrow (\mathbf{Q}_i \text{ es un } \mathbf{A}/\mathfrak{m}_i-\text{módulo noetheriano}), (\text{Obs.}3.5.8)$

$\Leftrightarrow (\mathbf{Q}_i \text{ es un } \mathbf{A}/\mathfrak{m}_i-\text{módulo artiniano}), (\text{Prop. } 3.5.3)$

$\Leftrightarrow (\mathbf{Q}_i \text{ es un } \mathbf{A}-\text{módulo artiniano}), (\text{Obser.}3.5.8)$

$\Leftrightarrow (\mathbf{A} \text{ es un } \mathbf{A}-\text{módulo artiniano}), (\text{Coro. } 3.5.6)$

$\Leftrightarrow (\mathbf{A} \text{ es un anillo de Artin}), (\text{Definición } 3.5.7).$

Proposición 3.5.10: (Teorema de caracterización). Sea $\mathbf{A}$ un anillo. Las propiedades siguientes son equivalentes:

(i) $\mathbf{A}$ es un anillo artiniano.

(ii) $\mathbf{A}$ es un anillo noetheriano y $\dim(\mathbf{A}) = 0$.

Demostración:

$(\text{i}) \Rightarrow (\text{ii})$.

Por el corolario 3.4.7, cada ideal primo en un anillo artiniano $\mathbf{A}$, es maximal de donde la $\dim(\mathbf{A})=0$.

Sea $\mathfrak{m}_i$ $(1 \leq i \leq r)$ los distinto ideales maximales de $\mathbf{A}$. Por tanto en consecuencia del corolario 3.4.10, $\mathfrak{R}_{\mathbf{A}} = \prod_{i=1}^{r} \mathfrak{m}_i$. En virtud de la proposición 3.4.12, existe $k \in \mathbb{N}$ tal que $\mathfrak{R}_{\mathbf{A}}^k = 0$. Entonces:

$$\prod_{i=1}^{r} \mathfrak{m}_i^k = \mathfrak{m}_1^k \mathfrak{m}_2^k \cdot \cdot \cdot \mathfrak{m}_r^k = \left(\underbrace{\mathfrak{m}_1 \mathfrak{m}_1 \cdots \mathfrak{m}_1}_{k-\text{veces } \mathfrak{m}_1} \right) \left(\underbrace{\mathfrak{m}_2 \mathfrak{m}_2 \cdots \mathfrak{m}_2}_{k-\text{veces } \mathfrak{m}_2} \right) \cdot \cdot \cdot \left(\underbrace{\mathfrak{m}_r \mathfrak{m}_r \cdots \mathfrak{m}_r}_{k-\text{veces } \mathfrak{m}_r} \right)$$

$$= \left(\mathfrak{m}_1 \mathfrak{m}_2 \cdots \mathfrak{m}_r\right)\left(\mathfrak{m}_1 \mathfrak{m}_2 \cdots \mathfrak{m}_r\right) \cdot \cdot \cdot \left(\mathfrak{m}_1 \mathfrak{m}_2 \cdots \mathfrak{m}_r\right)$$

$$= \underbrace{\mathfrak{R}_{\mathbf{A}} \mathfrak{R}_{\mathbf{A}} \cdot \cdot \cdot \mathfrak{R}_{\mathbf{A}}}_{k-\text{veces } \mathfrak{R}_{\mathbf{A}}}$$

$$= \mathfrak{R}_{\mathbf{A}}^k = 0.$$

$$= 0.$$

Por tanto $\prod_{i=1}^{r} \mathfrak{m}_i^k = 0$. De donde por el lema 3.5.9, $\mathbf{A}$ es un anillo noetheriano.

$(\text{ii}) \Rightarrow (\text{i})$.

Supóngase que $\mathbf{A}$ es un anillo noetheriano. De acuerdo con la observación 3.2.3 (2), $\mathfrak{R}_{\mathbf{A}} = r(\mathbf{0})$ es la intersección de un número finito de ideales primos minimales $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$. Como la $\dim(\mathbf{A}) = 0$, los $\mathfrak{p}_j$ $(1 \leq j \leq r)$ han de ser maximales. Del corolario 3.3.6, $\mathfrak{R}_{\mathbf{A}}$ es nilpotente. Por ser $\mathfrak{R}_{\mathbf{A}}$ nilpotente existe $k \in \mathbb{N}$ tal que $\mathfrak{R}_{\mathbf{A}}^k = 0$. De $(\mathrm{i}) \Rightarrow (\mathrm{ii})$ $\prod_{j=1}^{r} \mathfrak{p}_j^k = 0$, aplicando el lema 3.5.9, $\mathbf{A}$ es un anillo artiniano.■

Proposición 3.5.11: (Teorema de estructura de anillos de Artin). Sea $\mathbf{A}$ un anillo artiniano con ideales maximales $\mathfrak{m}_1, \ldots, \mathfrak{m}_t$. Entonces $\mathbf{A}$ es isomorfo al anillo producto:

$$\mathbf{A}/\mathfrak{m}_1^n \times \mathbf{A}/\mathfrak{m}_2^n \times \cdots \times \mathbf{A}/\mathfrak{m}_t^n$$

Para algún $n \in \mathbb{N}$. Además, cada $\mathbf{A}/\mathfrak{m}_i^n$ para $i = 1, \ldots, n$ es un anillo local artiniano con ideal maximal $\mathfrak{m}_i / \mathfrak{m}_i^n$.

Demostración:

Por el corolario 3.4.10, $\mathfrak{R}_{\mathbf{A}} = \prod_{j=1}^{t} \left\{ \mathfrak{m}_j \mid \mathfrak{m}_j \text{ es un ideal maximal de } \mathbf{A} \right\}$.

En consecuencia del corolario 3.4.12, $\mathfrak{R}_{\mathbf{A}}$ es nilpotente. Luego existe $n \in \mathbb{N}$ tal que:

$$0 = \mathfrak{R}_{\mathbf{A}}^n = \left(\prod_{j=1}^{t} \mathfrak{m}_j \right)^n = \prod_{j=1}^{t} \mathfrak{m}_j^n.$$

Se demuestra que los ideales $\mathfrak{m}_j^n$ son comaximales dos a dos. Dado $\mathfrak{m}_h^n$ y $\mathfrak{m}_k^n$ con $k \neq h$ ideales en $\mathbf{A}$. Se verifica que $\mathfrak{m}_h^n + \mathfrak{m}_k^n = (1)$.

Aplicando radical a $\mathfrak{m}_h^n + \mathfrak{m}_k^n$ se obtiene:

$$
\begin{aligned}
r\left(\mathfrak{m}_h^n + \mathfrak{m}_k^n\right) &= r\left(r\left(\mathfrak{m}_h^n\right) + r\left(\mathfrak{m}_k^n\right)\right), \quad \left(\text{Proposición 1.2.15 (vi)}\right)\\
&= r\left(\mathfrak{m}_h + \mathfrak{m}_k\right), \quad \left(\text{Proposición 1.2.15 (v)}\right)\\
&= r\left((1)\right), \quad \left(\text{Para } k \neq h,\ \mathfrak{m}_h \text{ y } \mathfrak{m}_k \text{ son comaximales}\right)\\
&= (1), \quad \left(\text{Definición 1.2.13. observación } (1)\right).
\end{aligned}
$$

De donde por la proposición 1.2.15, inciso (iv), se deduce que, $\mathfrak{m}_h^n + \mathfrak{m}_k^n = (1)$. Se concluye que los ideales $\mathfrak{m}_j^n$ son comaximales dos a dos.

Por tanto:

$$\mathfrak{m}_1^n \mathfrak{m}_2^n \cdot \ \cdot \ \cdot \mathfrak{m}_t^n = \mathfrak{m}_1^n \cap \mathfrak{m}_2^n \cap \cdot \ \cdot \ \cdot \cap \mathfrak{m}_t^n.$$

Entonces de la proposición 1.2.22, existe un isomorfismo de anillos:

$$\mathbf{A} \cong \prod_{i=1}^{t} \left(\mathbf{A} / \mathfrak{m}_i^n\right).$$

Se demuestra que cada $\mathbf{A}/\mathfrak{m}_i^n$ es un anillo local artiniano para $i=1,\ldots,t$. De acuerdo con la proposición 3.4.5, los anillos $\mathbf{A}/\mathfrak{m}_i^n$ son artinianos. En la observación de la proposición 1.1.14, el ideal $\mathfrak{m}_i/\mathfrak{m}_i^n$ es maximal.

Se demuestra que $\mathfrak{m}_i/\mathfrak{m}_i^n=\mathfrak{J}_{\mathbf{A}/\mathfrak{m}_i^n}$. Por definición de $\mathfrak{J}_{\mathbf{A}/\mathfrak{m}_i^n}$ se tiene que $\mathfrak{J}_{\mathbf{A}/\mathfrak{m}_i^n}\subseteq\mathfrak{m}_i/\mathfrak{m}_i^n$. Para la otra inclusión, sea $\overline{x}\in\mathfrak{m}_i/\mathfrak{m}_i^n$.

$$
\begin{aligned}
\overline{x}\in\mathfrak{m}_i/\mathfrak{m}_i^n \quad &\Rightarrow \quad \exists \quad x'\in\mathfrak{m}_i \quad \text{t. q.} \quad \overline{x}=x'+\mathfrak{m}_i^n\\
&\Rightarrow \quad (\overline{x})^n=\left(x'+\mathfrak{m}_i^n\right)^n=(x')^n+\mathfrak{m}_i^n=\mathfrak{m}_i^n\\
&\Rightarrow \quad (\overline{x})^n=\mathfrak{m}_i^n\\
&\Rightarrow \quad \overline{x} \text{ es un elemento nilpotente.}
\end{aligned}
$$

En consecuencia del corolario 3.4.8, $\overline{x}\in\mathfrak{J}_{\mathbf{A}/\mathfrak{m}_i^n}$, por tanto $\mathfrak{m}_i/\mathfrak{m}_i^n\subseteq\mathfrak{J}_{\mathbf{A}/\mathfrak{m}_i^n}$. Así $\mathfrak{m}_i/\mathfrak{m}_i^n=\mathfrak{J}_{\mathbf{A}/\mathfrak{m}_i^n}$.

De nuevo por la definición de $\mathfrak{J}_{\mathbf{A}/\mathfrak{m}_i^n}$,

$$\mathfrak{m}_i/\mathfrak{m}_i^n=\mathfrak{J}_{\mathbf{A}/\mathfrak{m}_i^n}=\bigcap_{j=1}^{m}\mathfrak{g}_j,\quad \text{donde } \mathfrak{g}_j \text{ es maximal en } \mathbf{A}/\mathfrak{m}_i^n.$$

De lo anterior:

$$\mathfrak{m}_i / \mathfrak{m}_i^n \subseteq \mathfrak{g}_j \qquad \forall \quad j = 1, \ldots, m.$$

Por la maximalidad de $\mathfrak{m}_i / \mathfrak{m}_i^n$,

$$\mathfrak{m}_i / \mathfrak{m}_i^n = \mathfrak{g}_j \qquad \forall \quad j = 1, \ldots, m.$$

De donde $\mathfrak{m}_i / \mathfrak{m}_i^n$ es el único maximal en $\mathbf{A}/\mathfrak{m}_i^n$. Luego cada $\mathbf{A}/\mathfrak{m}_i^n$ es un anillo artiniano local. ■

Proposición 3.5.12: (Estructura de anillos locales artinianos). Sea $\mathbf{A}$ un anillo local noetheriano y $\mathfrak{m}$ su ideal maximal. Las propiedades siguientes son equivalentes:

(i) El ideal $\mathfrak{m}$ es nilpotente.

(ii) $\mathbf{A}$ es un anillo artiniano.

(iii) $\mathfrak{m}$ es el único ideal primo de $\mathbf{A}$. (Es decir, $\dim(\mathbf{A}) = \mathrm{ht}(\mathfrak{p}) = 0$.)

Demostración: $(\mathrm{i}) \Rightarrow (\mathrm{ii})$. $(\text{El ideal } \mathfrak{m} \text{ es nilpotente}) \Rightarrow (\mathbf{A} \text{ es un anillo artiniano})$.

Si $\mathfrak{m}$ es nilpotente, entonces existe $n \in \mathbb{N}$ tal que $\mathfrak{m}^n = 0$. Para cada ideal primo $\mathfrak{p}$ en $\mathbf{A}$, se tiene $\mathfrak{m}^n = 0 \subseteq \mathfrak{p}$. Del corolario 1.2.6,

$$\mathfrak{m}^n = 0 \subseteq \mathfrak{p} \subseteq \mathfrak{m}.$$

Tomando radicales y por el inciso (i) de la proposición 1.2.15,

$$r\left(\mathfrak{m}^n\right) \subseteq r(\mathfrak{p}) \subseteq r(\mathfrak{m}).$$

De nuevo por (v) de la proposición 1.2.15:

$$\mathfrak{m} \subseteq \mathfrak{p} \subseteq \mathfrak{m}.$$

De donde $\mathfrak{p} = \mathfrak{m}.$ Luego cada ideal primo de $\mathbf{A}$ es maximal, por tanto $\dim(\mathbf{A}) = 0,$ de acuerdo con la proposición 3.5.10, $\mathbf{A}$ es un anillo artiniano.

$(\text{ii}) \Rightarrow (\text{i}).$

$(\mathbf{A}$ es un anillo artiniano$) \Rightarrow ($El ideal $\mathfrak{m}$ es nilpotente$).$

Se considera la cadena descendente de ideales en $\mathbf{A}$.

$$\mathfrak{m}^1 \supseteq \mathfrak{m}^2 \supseteq \cdot \cdot \cdot \supseteq \mathfrak{m}^n \supseteq \mathfrak{m}^{n+1} \supseteq \cdot \cdot \cdot \cdot .$$

Como $\mathbf{A}$ es un anillo de Artin, existe $r \in \mathbb{N},$ tal que $\mathfrak{m}^r = \mathfrak{m}^{r+1} = \mathfrak{m}^r \cdot \mathfrak{m}.$ El lema de **Nakayama** proposición 1.4.4, nos dice que $\mathfrak{m}^r = 0.$

$(\text{i}) \Rightarrow (\text{iii}).$

(El ideal $\mathfrak{m}$ es nilpotente) $\Rightarrow$ ($\mathfrak{m}$ es el único ideal primo de $\mathbf{A}$).

(El ideal $\mathfrak{m}$ es nilpotente) $\Rightarrow$ ($\mathbf{A}$ es un anillo artiniano), $\left(\text{Por } (\mathrm{i}) \Rightarrow (\mathrm{ii})\right)$

$\Rightarrow$ (cada ideal primo primo $\mathfrak{p}$ en $\mathbf{A}$, es maximal)

$\Rightarrow$ $(\mathfrak{p} = \mathfrak{m})$, $\left(\mathfrak{m} \text{ es el único ideal maximal en } \mathbf{A}\right)$

$\Rightarrow$ ($\mathfrak{m}$ es el único ideal primo en $\mathbf{A}$)

$\Rightarrow$ $(\dim(\mathbf{A}) = \mathrm{ht}(\mathfrak{p}) = 0)$.

$(\mathrm{iii}) \Rightarrow (\mathrm{i})$. ($\mathfrak{m}$ es el único ideal primo de $\mathbf{A}$) $\Rightarrow$ (El ideal $\mathfrak{m}$ es nilpotente).

Si $\mathfrak{m}$ es el único ideal primo de $\mathbf{A}$, entonces $\mathfrak{R}_{\mathbf{A}} = \mathfrak{m}$. Como $\mathbf{A}$ es noetheriano y por el corolario 3.3.6, existe $n \in \mathbb{N}$, tal que $\mathfrak{R}_{\mathbf{A}}^n = \mathfrak{m}^n = 0$. ■

Proposición 3.5.13: Sea $\mathbf{A}$ un anillo local noetheriano con ideal maximal $\mathfrak{m}$, entonces se verifica una de las dos posibilidades siguientes:

(i) $\mathfrak{m}^n \neq \mathfrak{m}^{n+1}$ para cada $n \in \mathbb{N}$.

(ii) $\mathfrak{m}^n = 0$ para algún $n \in \mathbb{N}$ y en este caso $\mathbf{A}$ es artiniano.

Demostración: Supóngase (i) falso. Entonces existe $n \in \mathbb{N}$, tal que $\mathfrak{m}^n = \mathfrak{m}^{n+1}$,

$$\mathfrak{m}^n = \mathfrak{m} \cdot \mathfrak{m}^n = \mathfrak{m}^{n+1}.$$

Como consecuencia del lema de **Nakayama**:

$$\mathfrak{m}^n = 0.$$

En virtud del lema 3.5.9, **A** es artiniano.■

Existe mucha más teoría sobre anillos **noetherianos** y **artinianos**; además de la expuesta en este documento. Debido a eso se espera que esta investigación motive y dé utilidad al lector para seguir realizando estudios en anillos de cadenas. Entre otras cosas lo realizado en los capítulos I, II y III; puede trasladarse al contexto de módulos sobre un anillo (**Módulos de fracciones, descomposición de submódulos y módulos de cadenas**), temas que pueden ser útiles para nuevos trabajos de investigación en el área del álgebra conmutativa.

BIBLIOGRAFÍA

[1] Atiyah, M. F. y Macdonald, I. G., Introducción al álgebra Conmutativa, Ed. Reverté, Barcelona (1980).

[2] http://www.ugr.es/~pjara/Docen08/AC/textoSOL.pdf

[3] http://www.iam.conicet.gov.ar/cms/?q=es/system/files/u3/2006_-_Tartaglia_-_Descomposicion_Primaria.pdf.

[4] http://personal.us.es/arojas/files/notasAC.pdf

[5] http://www.rsme.es/gacetadigital/abrir.php?id=81