UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS NATURALES Y MATEMÁTICA

ESCUELA DE MATEMÁTICA

TRABAJO DE INVESTIGACIÓN TITULADO:

APLICACIÓN DE LOS ANILLOS NOETHERIANOS CONMUTATIVOS Y LAS VARIEDADES ALGEBRAICAS AFINES EN LA DEMOSTRACIÓN DEL TEOREMA DE LOS CEROS DE HILBERT .

PRESENTADO POR:

Br. ZENÓN PORTILLO RIVAS PR05054.

Br. ÁLVARO CAMPOS CHIQUILLO CC98162.

PARA OPTAR AL TITULO DE:

LICENCIADO EN MATEMÁTICA.

ASESORES DIRECTORES:

Licda. CLAUDIA PATRICIA CORCIO.

Licda. INGRID CAROLINA MARTÍNEZ BARAHONA.

CIUDAD UNIVERSITARIA, SAN SALVADOR, 26 DE AGOSTO DE 2011.

UNIVERSIDAD DE EL SALVADOR

MsC. RUFINO ANTONIO QUEZADA SANCHEZ.
RECTOR

Lic. DOUGLAS VLADIMIR ALFARO CHÁVEZ.
SECRETARIO GENERAL

FACULTAD DE CIENCIAS NATURALES Y MATEMÁTICA

Dr. RAFAEL ANTONIO GÓMEZ ESCOTO.
DECANO

MsC. MARIA TRINIDAD TRIGUERROS DE CASTRO
SECRETARIA

ESCUELA DE MATEMÁTICA

Ing. CARLOS MAURICIO CANJURA
DIRECTOR

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

TRABAJO DE INVESTIGACIÓN TITULADO:

APLICACIÓN DE LOS ANILLOS NOETHERIANOS CONMUTATIVOS Y LAS VARIEDADES ALGEBRAICAS AFINES EN LA DEMOSTRACIÓN DEL TEOREMA DE LOS CEROS DE HILBERT .

PRESENTADO POR:
Br. ZENÓN PORTILLO RIVAS PR05054.
Br. ÁLVARO CAMPOS CHIQUILLO CC98162.

PARA OPTAR AL TITULO DE:
LICENCIADO EN MATEMÁTICA.

Licda. CLAUDIA PATRICIA CORCIO.
ASESOR DIRECTOR

Licda. INGRID CAROLINA MARTÍNEZ BARAHONA.
ASESOR DIRECTOR

CIUDAD UNIVERSITARIA, SAN SALVADOR, 26 DE AGOSTO DE 2011.

Bien sé yo, oh Jehová, que al hombre terrestre no le pertenece su camino. No pertenece al hombre que está andando siquiera dirigir su paso

(Jeremias 10:23)

DEDICATORIA:

A JEHOVÁ

MIS PADRES, ESPOSA E HIJAS

Y

DEMAS FAMILIARES

Álvaro Campo Chiquillo

Si nos cuesta conocer las cosas terrestres, y descubrir lo que está al alcance de la mano, quiën podra comprender lo que está en los cielos. Quiën podrá conocer tus intenciones, si tu no los has dado primero la Sabiduría o no los has enviado de lo alto el Espiritu Santo

(Sagradas Escrituras, Sabiduria 8: 16-17)

DEDICADA A:

A MI DIOS JEHOVÁ, A JESUCRISTO

MIS PADRES, EN ESPECIAL A MI MAMÁ ROSITA

Y

DEMAS FAMILIARES Y AMIGOS

Zenón Portillo Rivas

AGRADECIMIENTOS

- Damos gracias en primer lugar a Dios Altísimo y a nuestro Señor Jesucristo por darnos la oportunidad de terminar nuestros estudios de una manera exitosa, y porque a lo largo de nuestra carrera nos ha dado la fortaleza y la perseverancia para alcanzar todas nuestras metas, y superar los obstáculos que se nos han presentado.

- De igual forma a nuestras familias, por el apoyo incondicional que nos han brindado día con día en nuestros estudios y en toda nuestra vida, ya que su apoyo y cariño ha sido una de las principales fortalezas que nos ha impulsado a poder cruzar esta etapa de nuestras vidas y poder culminar nuestra carrera.

- A nuestros asesores directores Licda. Claudia Patricia Corcio y Licda. Ingrid Carolina Martínez Barahona, ya que han sido las personas que nos brindaron sus conocimientos y fueron guiando durante todo el proceso de nuestro trabajo de Graduación.

- Agradecemos también a nuestros amigos que nos han apoyado tanto económicamente, como moral y espiritualmente, que además nos han motivado a seguir con nuestro sueño de ser licenciados en matemática para poder culminar nuestra meta.

- Del mismo modo agradecemos a las autoridades de la Universidad Nacional, por brindarnos la oportunidad de formarnos en esta institución de prestigio para convertirnos en verdaderos profesionales por medio de todos los conocimientos que hemos adquirido a lo largo de nuestra carrera.

Resumen

En este trabajo desarrollamos un estudio de todas las herramientas necesarias para llegar al teorema de los ceros de Hilbert el cual luego se demuestra en sus formas débil y fuerte.

En el **primer capítulo,** nos dedicamos a introducir los conceptos básicos relacionados con los anillos noetherianos y las variedades algebraicas afines que son fundamentales para el estudio del teorema de los ceros de Hilbert. Es por ello que estudiamos detenidamente el concepto de ideal primo e ideal primario, como también las distintas operaciones entre ideales, en particular la descomposición primaria de ideales.

En el **segundo capítulo,** se desarrollan las demostraciones de algunos de los teoremas importantes de los anillos noetherianos, haciendo uso de la descomposción primaria de un ideal y un resultado fundamental: el teorema de la base de Hilbert.

En el **tercer capítulo,** se desarrollan las definiciones, proposiciones, teoremas de una variedad algebraica afín y el ideal asociado a una variedad, asi como también el ideal de una variedad y lo más interesante es la descomposición de ideales en variedades algebraicas afines, como la condición de cadena descendente de variedades.

En el **cuarto capítulo,** se desarrolla la aplicación de los resultados obtenidos en los capítulos anteriores, para demostrar el teorema de los ceros de Hilbert en su forma dedíl así como en la forma fuerte.

Finalmente en el **quinto capítulo,** adoptamos una Topología que es muy débil pero sosprendentemente útil ocupando los resultados de los capítulos anteriores, probando propiedades que cumple esta topología como la cerradura topológica y compacidad.

Índice general

INTRODUCCIÓN

En la matemática actual el dominio del álgebra conmutativa es esencial en la comprensión de la teoría de las estructuras algebraicas, así como también de la geometría algebraica, las cuales contribuyeron al origen de esta rama de la matemática. De hecho esta tendencia fue desarrollada por célebres matemáticos como David Hilbert, Max Noether, Emanuel Lasker, Emmy Noether, Wolfgang Krull y otros. Antes de sus aportes no existían fundamentos estándares para la geometría algebraica.

Incluso podemos mencionar que en un intento por demostrar el último teorema de Fermat[1], Richard Dedekind (1831-1916), alumno de Carl Friederich Gauss, introdujo el concepto de *ideal* tal y como lo conocemos hoy en día. -Más adelante daremos a conocer dicho concepto, como los muchos otros a los cuales hacemos mención aquí-. Además generalizó la noción de un número primo a un *ideal primo*. Esto contribuyó como fundamento de la geometría algebraica y de la geometría analítica compleja.

Por otro lado en 1921 Emmy Neother descubre que la *descomposición primaria de ideales* es una consecuencia de *la condición de cadena ascendente*, y de una derivación extremadamente simple de los resultados anteriores de anillos conmutativos que satisfacen dicha condición y en 1927 caracteriza axiomáticamente los anillos de Dedekind. A Emmy Noether debemos la formulación general del *lema de normalización de Noether* en su honor, donde emana entre otras cosas el *teorema de los ceros de Hilbert*. Su trabajo proporciona una nueva dirección al álgebra y las consecuencias de este se convierten en uno de los más importantes del siglo XX.

En los años (1930-1931) Bartel Leendert van der Waerden publica su obra Algebre Moderne, siguiendo los lineamientos de la escuela axiomática alemana de Hilbert, y recogiendo los resultados de Noether y Artin entre otros. En esta obra exponen sistemáticamente la teoría de grupos, cuerpos, anillos, ideales, etc., es decir, la teoría de las estructuras algebraicas con lo que el álgebra se convierte, por su objetivo, en una nueva disciplina moderna.

[1]La ecuación $x^n + y^n = z^n$ no tiene solución entera no trivial(es decir, que x e y no son nulos) cuando $n \geq 3$.

En la actualidad el álgebra abstracta sigue siendo, una herramienta necesaria para el estudio del análisis ya que en ella se involucran diversidad de contenidos como los conjuntos, la estructura de grupo, las categorías, los anillos y módulos en donde estos se dividen en las importantes ramas de campos, teoría de Galois, álgebra lineal, anillos conmutativos y estructura de anillos entre otros. En este trabajo se pretende hacer un estudio de todas las herramientas necesarias para llegar al teorema de los ceros de Hilbert entre las cuales resalta el estudio de los *anillos noetherianos conmutativos* y las *variedades algebraicas afines* dentro lo cual se pretende tomar como base para la demostración de dicho teorema tanto en la forma débil y como la fuerte.

Capítulo 1

Descomposición Primaria en ideales

1.1. Ideales y Sus Operaciones

En este trabajo la palabra $anillo$ denotará a un anillo conmutativo con elemento identidad y las pequeñas letras alemanas $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$, etc, denotarán a los ideales y emplearemos pequeñas letras latinas y griegas para referirnos a los elementos.

Definición 1.1.1 *Sea R un anillo, y sea $\mathfrak{a}$ un subconjunto no vacío de R, entonces $\mathfrak{a}$ es llamado un $ideal$ de R cuando satisface las siguientes condiciones:*

- *Siempre que a_1 y a_2 tal que a_1,$a_2 \in \mathfrak{a}$, entonces $a_1 \pm a_2$ ambos pertenecen a $\mathfrak{a}$.*
- *Si $a \in \mathfrak{a}$, entonces $ra \in \mathfrak{a}$ para todo $r \in R$.*

Ejemplos:

- Para todo entero relativo k, $k\mathbb{Z}$ es un ideal de $\mathbb{Z}$.
- Si R es un anillo, 0 y R son ideales triviales de R. Estos dos ideales tienen un interés muy limitado. Por esta razón se llamará *ideal propio* a todo ideal no trivial.
- Si R es un anillo unitario y si $\mathfrak{a}$ es un ideal que contiene a 1 entonces $\mathfrak{a} = R$. De modo más general, si, $\mathfrak{a}$ contiene un elemento inversible, entonces $\mathfrak{a} = R$
- Los únicos ideales en un cuerpo k son los ideales triviales.

1.1.1. Suma de ideales

Definición 1.1.2 *Sean $\mathfrak{a}$ y $\mathfrak{b}$, dos ideales en R, definamos la suma de $\mathfrak{a}$ y $\mathfrak{b}$ como el conjunto*

$$\mathfrak{a}+\mathfrak{b}=\left\{a+b/a\in\mathfrak{a},\ b\in\mathfrak{b}\right\}$$

Este conjunto resulta ser un ideal.

Para probarlo supongamos que $x_1\in\mathfrak{a}+\mathfrak{b}$, que $x_2\in\mathfrak{a}+\mathfrak{b}$, entonces $x_1=a_1+b_1$, y $x_2=a_2+b_2$ donde $a_1,a_2\in\mathfrak{a}$ y $b_1,b_2\in\mathfrak{b}$, y tenemos:

$$\begin{aligned}x_1+x_2 &= (a_1+b_1)+(a_2+b_2)\\ &= \underbrace{(a_1+a_2)}_{\in\mathfrak{a}}+\underbrace{(b_1+b_2)}_{\in\mathfrak{b}}\end{aligned}$$

y para la resta tenemos:

$$\begin{aligned}x_1-x_2 &= (a_1+b_1)-(a_2+b_2)\\ &= \underbrace{(a_1-a_2)}_{\in\mathfrak{a}}+\underbrace{(b_1-b_2)}_{\in\mathfrak{b}}\end{aligned}$$

Sea $r\in R$, entonces

$$\begin{aligned}rx_1 &= r(a_1+b_1)\\ &= \underbrace{r(a_1)}_{\in\mathfrak{a}}+\underbrace{r(b_2)}_{\in\mathfrak{b}}\end{aligned}$$

Como $x_1+x_2,\ \ x_1-x_2\in\mathfrak{a}+\mathfrak{b}$ y $rx_1\in\mathfrak{a}$ por la definición $\mathfrak{a}+\mathfrak{b}$ es un ideal.

Por lo tanto $\mathfrak{a}+\mathfrak{b}$ es un ideal.

1.1.2. Producto de ideales

Definición 1.1.3 *Sean $\mathfrak{a}$ y $\mathfrak{b}$, dos ideales en R, definamos el producto de $\mathfrak{a}$ y $\mathfrak{b}$ como el conjunto*

$$\mathfrak{a}\mathfrak{b}=\left\{\sum_{i=1}^{n}a_ib_i/a_i\in\mathfrak{a},b_i\in\mathfrak{b}\right\}$$

Este conjunto es un ideal. Veamos su prueba:

Supongamos que $x_1,x_2\in\mathfrak{a}\mathfrak{b}$, entonces $x_1=\sum_{i=1}^{p}a_ib_i$, y $x_2=\sum_{j=1}^{q}a_j^{'}b_j^{'}$ donde a_i y $a_j^{'}$ están en $\mathfrak{a}$ y b_i y $b_j^{'}$ están en $\mathfrak{b}$, luego obtenemos:

$$\begin{aligned} x_1 + x_2 &= \sum_{i=1}^{p} a_i b_i + \sum_{j=1}^{q} a_j^{'} b_j^{'} \\ &= (a_1 b_1 + a_2 b_2 + ... + a_p b_p) + (a_1^{'} b_1^{'} + a_2^{'} b_2^{'} + ... + a_q^{'} b_q^{'}) \\ &= a_1 b_1 + ... + a_q^{'} b_q^{'} \in \mathfrak{ab} \end{aligned}$$

ya que por hipótesis tenemos que a_i y $a_j^{'}$ están en $\mathfrak{a}$ y b_i y $b_j^{'}$ están en $\mathfrak{b}$.

Para la resta de forma análoga:

$$\begin{aligned} x_1 - x_2 &= \sum_{i=1}^{p} a_i b_i - \sum_{j=1}^{q} a_j^{'} b_j^{'} \\ &= (a_1 b_1 + a_2 b_2 + ... + a_p b_p) - (a_1^{'} b_1^{'} + a_2^{'} b_2^{'} + ... + a_q^{'} b_q^{'}) \\ &= a_1 b_1 + ... + a_p b_p + (-a_1^{'}) b_1^{'} + (-a_2^{'}) b_2^{'} + ... + (-a_q^{'}) b_q^{'} \in \mathfrak{ab} \end{aligned}$$

Ahora, sea $r \in R$,

$$\begin{aligned} rx_1 &= r(\sum_{i=1}^{p} a_i b_i) \\ &= r(a_1 b_1 + a_2 b_2 + ... + a_p b_p) \\ &= ra_1 b_1 + ra_2 b_2 + ... + ra_p b_p \\ &= r(a_1) b_1 + r(a_2) b_2 + ... + r(a_p) b_p \in \mathfrak{ab} \end{aligned}$$

Ahora como $-a_j^{'} \in \mathfrak{a}$ y $ra_i \in \mathfrak{a}$, entonces concluimos que $x_1 + x_2, x_1 - x_2$ y rx_1 están en $\mathfrak{ab}$, es decir, que $\mathfrak{ab}$ es un ideal.

1.1.3. Intersección de ideales

Definición 1.1.4 *Sean $\mathfrak{a}$ y $\mathfrak{b}$, dos ideales en R, podemos tomar la intersección de $\mathfrak{a}$ y $\mathfrak{b}$ y definir el conjunto*

$$\mathfrak{a} \cap \mathfrak{b} = \Big\{ a \in R / a \in \mathfrak{a} \ y \ \ a \in \mathfrak{b} \Big\}$$

Y en forma general podemos escribir $\bigcap_{i \in I} \mathfrak{a}_i$ con I finito.

Este conjunto resulta ser un ideal, supongamos que $x_1, x_2 \in \bigcap_{i=1}^{n} \mathfrak{a}_i$ y que $r \in R$ entonces como x_1, x_2 pertenecen a la intersección de los $\mathfrak{a}_\mathfrak{i}$ entonces ambos están en cada $\mathfrak{a}_i$; es decir que que cumplen con

que $x_1 + x_2 \in \mathfrak{a}_i$ para todo i y $x_1 - x_2 \in \mathfrak{a}_i$ para todo i, entonces $x_1 + x_2 \in \cap_{i=1}^{n} \mathfrak{a}_i$ y $x_1 - x_2 \in \bigcap_{i=1}^{n} \mathfrak{a}_i$, luego probemos que $rx \in \bigcap_{i=1}^{n} \mathfrak{a}_i$ para esto tomemos a $x_1 \in \bigcap_{i=1}^{n} \mathfrak{a}_i$ y $r \in R$ y como $x_1 \in \bigcap_{i=1}^{n} \mathfrak{a}_i$ entonces tenemos $x_1 \in \mathfrak{a}_i$ para todo i y luego si lo multiplicamos por un elemento $r \in R$ tenemos $rx_1 \in \mathfrak{a}_i$ para todo i y como es para todo i entonces $rx_1 \in \bigcap_{i=1}^{n} \mathfrak{a}_i$.

Ahora como $x_1 + x_2, x_1 - x_2$ y rx_1 pertenecen a $\bigcap_{i=1}^{n} \mathfrak{a}_i$ entonces el conjunto $\bigcap_{i=1}^{n} \mathfrak{a}_i$ es un ideal.

En particular para dos ideales $\mathfrak{a}\ \ y\ \ \mathfrak{b}$ la intersección también es un ideal

Por lo tanto $\mathfrak{a} \cap \mathfrak{b}$ es un ideal.

1.1.4. Cociente de ideales

Definición 1.1.5 *Sean $\mathfrak{a}$ y $\mathfrak{b}$, dos ideales en R, y definamos el conjunto de todos los elementos x tal que $xb \in \mathfrak{a}$ para todo $b \in \mathfrak{b}$, es decir, el conjunto cociente de ideales lo podemos definir como:*

$$(\mathfrak{a} : \mathfrak{b}) = \Big\{ x \in R / xb \in \mathfrak{a},\ \ \forall b \in \mathfrak{b} \Big\}.$$

y que esta división residual es un ideal, supongamos que $x_1, x_2 \in (\mathfrak{a} : \mathfrak{b})$, entonces para cualquier $b \in \mathfrak{b}$ tenemos:

$$(x_1 + x_2)b = \underbrace{x_1 b}_{\in \mathfrak{a}} + \underbrace{x_2 b}_{\in \mathfrak{a}}$$

Para todo $b \in \mathfrak{b}$, por lo tanto

$$(x_1 + x_2)b \in \mathfrak{a}.$$

Entonces $x_1 + x_2 \in (\mathfrak{a} : \mathfrak{b})$

Ahora para cualquier $b \in \mathfrak{b}$ tenemos:

$$\begin{aligned} (x_1 - x_2)b &= x_1 b - x_2 b \\ &= \underbrace{x_1 b}_{\in \mathfrak{a}} + \underbrace{x_2(-b)}_{\in \mathfrak{a}} \end{aligned}$$

Como se cumple para todo $b \in \mathfrak{b}$, entonces por definición de división residual tenemos:

$$(x_1 - x_2)b \in \mathfrak{a}.$$

Entonces $x_1 - x_2 \in (\mathfrak{a} : \mathfrak{b})$.

Finalmente sea $r \in R$ entonces:

$$(rx_1)b = r \underbrace{(x_1 b)}_{\in \mathfrak{a}}$$

Entonces tenemos que $r(x_1 b) \in \mathfrak{a}$, entonces $rx_1 \in (\mathfrak{a} : \mathfrak{b})$.

Y por lo tanto $(\mathfrak{a} : \mathfrak{b})$ es un ideal.

Proposición 1.1.1 *Si* $\mathfrak{a}, \mathfrak{b}$ *y* $\mathfrak{c}$ *son ideales de un anillo* R *conmutativo entonces:*

1) $\mathfrak{a} + \mathfrak{b} = \mathfrak{b} + \mathfrak{a}$;

1.1) $\mathfrak{a} + (\mathfrak{b} + \mathfrak{c}) = (\mathfrak{a} + \mathfrak{b}) + \mathfrak{c}$.

2) $\mathfrak{a}\mathfrak{b} = \mathfrak{b}\mathfrak{a}$;

2.1) $\mathfrak{a}(\mathfrak{b}\mathfrak{c}) = (\mathfrak{a}\mathfrak{b})\mathfrak{c}$;

2.1) $\mathfrak{a}(\mathfrak{b} + \mathfrak{c}) = \mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{c}$.

3) $\mathfrak{a} \subseteq \mathfrak{a} + \mathfrak{b}$,

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

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

5) $(\cap \mathfrak{a}_i : \mathfrak{b}) = \cap(\mathfrak{a}_i : \mathfrak{b})$.

6) $((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}) = (\mathfrak{a} : (\mathfrak{b}\mathfrak{c}))$.

7) $(\mathfrak{a} : (\sum_{i=1}^{n} \mathfrak{b}_i)) = \cap_{i=1}^{n}(\mathfrak{a} : \mathfrak{b})$.

8) $(\mathfrak{a} : \mathfrak{b}) = (\mathfrak{a} : (\mathfrak{a} + \mathfrak{b}))$.

Demostración:

1) Esta prueba es inmediata de la definición de suma de ideales y la hacemos por doble inclusión.

Sea $x \in \mathfrak{a} + \mathfrak{b}$ y como la suma de dos ideales esta definida $\mathfrak{a} + \mathfrak{b} = \{a + b / a \in \mathfrak{a}, b \in \mathfrak{b}\}$, entonces $x = a + b$ donde $a \in \mathfrak{a}$ y $b \in \mathfrak{b}$ y luego como ya son elementos de ideales son conmutativos, es decir, $x = b + a$ por lo tanto $x \in \mathfrak{b} + \mathfrak{a}$, es decir, $\mathfrak{a} + \mathfrak{b} \subseteq \mathfrak{b} + \mathfrak{a}$.

Luego de forma parecida probamos que $\mathfrak{a} + \mathfrak{b} \supseteq \mathfrak{b} + \mathfrak{a}$. Sea $y \in \mathfrak{b} + \mathfrak{a}$ entonces $y = b + a$, donde $b \in \mathfrak{b}$ y $a \in \mathfrak{a}$, ahora por ser elementos de ideales los conmutamos, es decir, $y = a + b$ entonces por definición de suma de ideales tenemos $y \in \mathfrak{a} + \mathfrak{b}$ entones $\mathfrak{a} + \mathfrak{b} \supseteq \mathfrak{b} + \mathfrak{a}$.

Por lo tanto tenemos:

$$\mathfrak{a} + \mathfrak{b} = \mathfrak{b} + \mathfrak{a}.$$

1.1) Ahora demostremos que $\mathfrak{a}+(\mathfrak{b}+\mathfrak{c})=(\mathfrak{a}+\mathfrak{b})+\mathfrak{c}$. Partamos de la definición:

$$\begin{aligned}\mathfrak{a}+(\mathfrak{b}+\mathfrak{c}) &= \Big\{a+(b+c)/a\in\mathfrak{a},(b+c)\in\mathfrak{b}+\mathfrak{c}\Big\}\\ &= \Big\{a+b_1+c_1\,/\,a\in\mathfrak{a},\ b_1\in\mathfrak{b},\ c_1\in\mathfrak{c}\Big\}\\ &= \Big\{(a+b_1)+c_1\,/\,(a+b_1)\in\mathfrak{a}+\mathfrak{b},\ c_1\in\mathfrak{c}\Big\}\\ &= (\mathfrak{a}+\mathfrak{b})+\mathfrak{c}\end{aligned}$$

Por lo tanto tenemos:

$$(\mathfrak{a}+\mathfrak{b})+\mathfrak{c}=\mathfrak{a}+(\mathfrak{b}+\mathfrak{c})$$

2) Probemos que $\mathfrak{ab}=\mathfrak{ba}$.

Es inmediata de la definición del producto de ideales:

$$\begin{aligned}\mathfrak{ab} &= \Big\{\sum_{i=1}^{n}a_ib_i/a_i\in\mathfrak{a},b_i\in\mathfrak{b}\Big\}\\ &= \Big\{a_1b_1+a_2b_2+...+a_nb_n/a_i\in\mathfrak{a},b_i\in\mathfrak{b}\Big\}\\ &= \Big\{b_1a_1+b_2a_2+...+b_na_n/b_i\in\mathfrak{b},a_i\in\mathfrak{a}\Big\}\\ &= \mathfrak{ba}\end{aligned}$$

Entonces hemos demostrado que $\mathfrak{ab}=\mathfrak{ba}$.

2.1) Probemos $\mathfrak{a}(\mathfrak{bc})=(\mathfrak{ab})\mathfrak{c}$.

Sea $y\in\mathfrak{a}(\mathfrak{bc})$ entonces

$$y=\textstyle\sum_{i=1}^{p}a_iz_i\text{, con }a_i\in\mathfrak{a}\text{ y }z_i\in\mathfrak{bc}$$

ahora como $z_i\in\mathfrak{bc}$ tenemos que

$$z_i=\textstyle\sum_{j=1}^{k_{i(p)}}b_jc_j,$$

luego

$$y=\textstyle\sum_{i=1}^{p}a_i\Big[\sum_{j=1}^{k_i(p)}c_jb_j\Big]$$

claramente y es una suma de elementos de la forma

$y = a_i(b_i c_i)$, para toda $a_i \in \mathfrak{a}, b_i \in \mathfrak{b}$, y $c_i \in \mathfrak{c}$, donde $y \in (\mathfrak{ab})\mathfrak{c}$.

y por lo tanto

$$\mathfrak{a}(\mathfrak{bc}) \subseteq (\mathfrak{ab})\mathfrak{c}.$$

De manera similar se comprueba que

$$\mathfrak{a}(\mathfrak{bc}) \supseteq (\mathfrak{ab})\mathfrak{c}$$

Entonces tenemos $\mathfrak{a}(\mathfrak{bc}) = (\mathfrak{ab})\mathfrak{c}$.

2.2) Ahora probemos que $\mathfrak{a}(\mathfrak{b} + \mathfrak{c}) = \mathfrak{ab} + \mathfrak{ac}$.

$$\begin{aligned}
\mathfrak{ab} + \mathfrak{ac} &= \left\{\sum_{i=1}^{n} a_i b_i / a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\right\} + \left\{\sum_{i=1}^{n} a_j c_j / a_j \in \mathfrak{a}, c_j \in \mathfrak{c}\right\} \\
&= \left\{a_1 b_1 + ... + a_n b_n + a_1 c_1 + ... + a_n c_n \ / \ a_i \in \mathfrak{a}, b_i \in \mathfrak{b}, c_i \in \mathfrak{c}\right\} \\
&= \left\{a_1(b_1 + c_1) + a_2(b_2 + c_2) + ... + a_n(b_n + c_n) \ / \ a_i \in \mathfrak{a}, (b_i + c_i) \in \mathfrak{b} + \mathfrak{c}\right\} \\
&= \mathfrak{a}(\mathfrak{b} + \mathfrak{c})
\end{aligned}$$

Por lo tanto

$$\mathfrak{ab} + \mathfrak{ac} = \mathfrak{a}(\mathfrak{b} + \mathfrak{c}).$$

3) Probemos que $\mathfrak{a} \subseteq \mathfrak{a} + \mathfrak{b}$, tenemos por definición que $\mathfrak{a} + \mathfrak{b} = \{a + b / a \in \mathfrak{a},\ b \in \mathfrak{b}\}$.

Sea $x \in \mathfrak{a}$ y dado que $a \in \mathfrak{a}$ entonces $x = a + 0$, donde $0 \in \mathfrak{b}$, entonces $x \in \mathfrak{a} + \mathfrak{b}$.

Por lo tanto $\mathfrak{a} \subseteq \mathfrak{a} + \mathfrak{b}$.

3.1) Ahora probemos que $\mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b}$.

Sea $x \in \mathfrak{ab}$ entonces por la definición de producto de dos ideales tenemos que $x = \sum_i^n a_i b_i$ donde $a_i \in \mathfrak{a}$, y $b_i \in \mathfrak{b}$ para todo i finito, y como hay elementos $a_i \in \mathfrak{a}$ y $b_i \in \mathfrak{b}$ para todo i entonces $x \in \mathfrak{a}$ y $x \in \mathfrak{b}$.

Entonces tenemos que $x \in \mathfrak{a} \cap \mathfrak{b}$ y por lo tanto $\mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b}$.

4) Probemos que $(\mathfrak{a} : \mathfrak{b})\mathfrak{b} \subseteq \mathfrak{a}$

Sea $x \in (\mathfrak{a} : \mathfrak{b})\mathfrak{b}$ entonces $x = \sum_{i=1}^{n} y_i z_i$ por definición de producto de ideales, donde $y_i \in (\mathfrak{a} : \mathfrak{b})$ y $z_i \in \mathfrak{b}$ para todo $i = 1, 2, 3, ..., n$, como $y_i \in (\mathfrak{a} : \mathfrak{b})$, por definición de división residual ó cociente residual tenemos que $y_i\mathfrak{b} \subseteq \mathfrak{a}$, es decir, $y_i b \in \mathfrak{b}$ para todo $b \in \mathfrak{b}$ y para todo $i = 1, 2, 3, ..., n$, pero como $z_i \in \mathfrak{b}$ entonces $y_i z_i \in \mathfrak{a}$ para todo $i = 1, 2, 3, ..., n$ y entonces $x \in \mathfrak{a}$ ya que x es de la forma

$x = \sum_{i=1}^{n} y_i z_i$ y por lo tanto tenemos $(\mathfrak{a} : \mathfrak{b}) \subseteq \mathfrak{a}$.

4.1) Probemos que $\mathfrak{a} \subseteq (\mathfrak{a} : \mathfrak{b})$. Sea $x \in \mathfrak{a}$ y si logramos probar que $x\mathfrak{b} \subseteq \mathfrak{a}$ la prueba esta completa. Como sabemos que $x\mathfrak{b} = \{xb_i / b_i \in \mathfrak{b}\}$ y por ser $\mathfrak{a}$ un ideal tenemos que $xb_i \in \mathfrak{a}$ entonces $x\mathfrak{b} \subseteq \mathfrak{a}$, así por definición de cociente residual tenemos que $x \in (\mathfrak{a} : \mathfrak{b})$.

Por lo tanto $\mathfrak{a} \subseteq (\mathfrak{a} : \mathfrak{b})$.

5) Probemos que $(\cap \mathfrak{a}_i : \mathfrak{b}) = \cap(\mathfrak{a}_i : \mathfrak{b})$.

Probemos primero que $(\cap \mathfrak{a}_i : \mathfrak{b}) \subseteq \cap(\mathfrak{a}_i : \mathfrak{b})$.

Sea $x \in (\cap \mathfrak{a}_i : \mathfrak{b})$ entonces $xb \in \cap \mathfrak{a}_i$ para todo $b \in \mathfrak{b}$ por definición de cociente residual y como $xb \in \cap \mathfrak{a}_i$ entonces tenemos que $xb \in \mathfrak{a}_i$. Tomemos i fijo, entonces $xb \in \mathfrak{a}_i$ para todo $b \in \mathfrak{b}$, es decir, que $x \in (\mathfrak{a}_i : \mathfrak{b})$ para todo i, por lo tanto $x \in \cap(\mathfrak{a}_i : \mathfrak{b})$ pero como x es cualquier elemento de $(\cap \mathfrak{a}_i : \mathfrak{b})$, es decir, que:

$$(\cap \mathfrak{a}_i : \mathfrak{b}) \quad \subseteq \quad \cap(\mathfrak{a}_i : \mathfrak{b}) \tag{1.1}$$

Sea $y \in \cap(\mathfrak{a}_i : \mathfrak{b})$, para cada i tenemos que $y \in (\mathfrak{a}_i : \mathfrak{b})$, entonces $yb \in \mathfrak{a}_i$ para todo i, entonces tenemos que $yb \in \cap \mathfrak{a}_i$ para todo $b \in \mathfrak{b}$ y como $yb \in \cap \mathfrak{a}_i$ entonces $y \in (\cap \mathfrak{a}_i : \mathfrak{b})$, pero como y es un elemento arbitrario de $\cap(\mathfrak{a}_i : \mathfrak{b})$ entonces probamos que:

$$\cap\,(\mathfrak{a}_i : \mathfrak{b}) \quad \subseteq \quad (\cap \mathfrak{a}_i : \mathfrak{b}) \tag{1.2}$$

Por tanto por (1.1) y (1.2) tenemos que $(\cap \mathfrak{a}_i : \mathfrak{b}) = \cap(\mathfrak{a}_i : \mathfrak{b})$.

6) Probemos que $((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}) = (\mathfrak{a} : (\mathfrak{b}\mathfrak{c}))$.

Sea $x \in ((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c})$, entonces por la definición de cociente residual tenemos $xc \in (\mathfrak{a} : \mathfrak{b})$ para todo $c \in \mathfrak{c}$ y aplicando nuevamente la definición tenemos $(xc)b \in \mathfrak{a}$ para todo $b \in \mathfrak{b}$ y asociando los elementos de forma conveniente tenemos $x(cb) \in \mathfrak{b}$.

Ahora podemos conmutar los elementos b y c de manera conveniente $x(bc) \in \mathfrak{a}$ y aplicando de nuevo dicha definición tenemos $x \in (\mathfrak{a} : (\mathfrak{b}\mathfrak{c}))$ así tenemos:

$$((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}) \quad \subseteq \quad (\mathfrak{a} : (\mathfrak{b}\mathfrak{c})) \tag{1.3}$$

Ahora sea $x \in (\mathfrak{a} : (\mathfrak{b}\mathfrak{c}))$, por definición de cociente residual tenemos que $x(bc) \in \mathfrak{a}$ para todo $bc \in \mathfrak{b}\mathfrak{c}$, permutando los elementos y asociando de forma conveniente tenemos $x(cb) = (xc)b \in \mathfrak{a}$,

donde $b \in \mathfrak{b}$ y por definición sabemos que $(xc) \in (\mathfrak{a} : \mathfrak{b})$ para todo $c \in \mathfrak{c}$, aplicando de nuevo la definición tenemos $x \in ((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c})$ y por lo tanto:

$$(\mathfrak{a} : (\mathfrak{bc})) \quad \subseteq \quad ((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}) \tag{1.4}$$

Por lo tanto por la ecuación (1.3) y (1.4) tenemos que $(\mathfrak{a} : (\mathfrak{bc})) = ((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c})$.

7) Ahora probemos que $(\mathfrak{a} : (\sum_{i=1}^{n} \mathfrak{b}_i)) = \cap_{i=1}^{n} (\mathfrak{a} : \mathfrak{b})$.

Sea $x \in (\mathfrak{a} : (\sum_{i=1}^{n} \mathfrak{b}_i))$, por la definición de cociente residual tenemos $x \sum_{i=1}^{n} b_i \in \mathfrak{a}$ para todo $\sum_{i=1}^{n} b_i \in \sum_{i=1}^{n} \mathfrak{b}_i$, en particular podemos escribir $(n-1)$ ceros y entonces $xb_i \in \mathfrak{a}$ para todo i; aplicando la definición de cociente residual una ves más $x \in (\mathfrak{a} : \mathfrak{b}_i)$ para todo i, de esta forma $x \in \bigcap_{i=1}^{n} (\mathfrak{a} : \mathfrak{b}_i)$.

Por tanto tenemos:

$$(\mathfrak{a} : (\sum_{i=1}^{n} \mathfrak{b}_i)) \quad \subseteq \quad \bigcap_{i=1}^{n} (\mathfrak{a} : \mathfrak{b}_i) \tag{1.5}$$

Sea $x \in \cap_{i=i}^{n} (\mathfrak{a} : \mathfrak{b}_i)$, como x pertenece a la intersección, $x \in (\mathfrak{a} : \mathfrak{b}_i)$ para todo i y $b_i \in \mathfrak{b}_i$ y aplicando la definición de cociente residual tenemos $xb_i \in \mathfrak{a}$ para todo i y por ser para todo i tenemos $x \sum_{i=1}^{n} b_i \in \mathfrak{a}$, nuevamente por la definición residual, $x \in (\mathfrak{a} : \sum_{i=1}^{n} \mathfrak{b}_i)$. Por lo tanto :

$$\bigcap_{i=1}^{n} (\mathfrak{a} : \mathfrak{b}_i) \quad \subseteq \quad (\mathfrak{a} : \sum_{i=1}^{n} \mathfrak{b}_i) \tag{1.6}$$

Entonces por (1.5) y (1.6) tenemos que $(\mathfrak{a} : (\sum_{i=1}^{n} \mathfrak{b}_i)) = \cap_{i=1}^{n} (\mathfrak{a} : \mathfrak{b}_i)$.

8) Finalmente probemos $(\mathfrak{a} : \mathfrak{b}) = (\mathfrak{a} : (\mathfrak{a} + \mathfrak{b}))$.

Por 7) de la misma proposición sabemos que:

$$(\mathfrak{a} : (\mathfrak{a} + \mathfrak{b})) \quad = \quad (\mathfrak{a} : \mathfrak{a}) \cap (\mathfrak{a} : \mathfrak{b})$$

Como es evidente que $\mathfrak{a} \subseteq \mathfrak{a}$, entonces todos los elementos del anillo R están en $(\mathfrak{a} : \mathfrak{a})$, es decir que, $(\mathfrak{a} : \mathfrak{a})$ es todo el anillo R, por lo tanto:

$$\begin{aligned} (\mathfrak{a} : (\mathfrak{a} + \mathfrak{b})) &= (\mathfrak{a} : \mathfrak{a}) \cap (\mathfrak{a} : \mathfrak{b}) \\ &= R \cap (\mathfrak{a} : \mathfrak{b}) \\ &= (\mathfrak{a} : \mathfrak{b}) \end{aligned}$$

1.2. Ideales generados por un conjunto

Definición 1.2.1 *Sea A un conjunto de elementos arbitrarios no vacíos del anillo R. El conjunto de todos los elementos de la forma $\sum_{i=1}^{n} r_i a_i$ donde $r_i \in R$ y $a_i \in A$ siempre que sea una suma finita, es llamado el ideal generado por un conjunto.*

Veamos que es un ideal.

Supongamos que $x_1, x_2 \in \sum_{i=1}^{n} r_i a_i$ y $k \in R$ entonces $x_1 = \sum_{i=1}^{n} r_i a_i$ y $x_2 = \sum_{i=1}^{m} r_i^{'} a_i^{'}$, veamos que la suma de $x_1 + x_2$ esta en el conjunto:

$$\begin{aligned} x_1 + x_2 &= \sum_{i=1}^{n} r_i a_i + \sum_{i=1}^{m} r_i^{'} a_i^{'} \\ &= r_1 a_1 + r_2 a_2 + ... + r_n a_n + r_1^{'} a_1^{'} + r_2^{'} a_2^{'} + ... + r_m^{'} a_m^{'} \\ &= r_1 a_1 + ... + r_m^{'} a_m^{'}. \end{aligned}$$

Así $x_1 + x_2 \in \sum_{i=1}^{n} r_i a_i$.
Ahora vemos que $x_1 - x_2 \in \sum_{i=1}^{n} r_i a_i$.

$$\begin{aligned} x_1 - x_2 &= \sum_{i=1}^{n} r_i a_i - \sum_{i=1}^{m} r_i^{'} a_i^{'} \\ &= r_1 a_1 + r_2 a_2 + ... + r_n a_n - (r_1^{'} a_1^{'} + r_2^{'} a_2^{'} + ... + r_m^{'} a_m^{'}) \end{aligned}$$

$$\begin{aligned} &= r_1 a_1 + r_2 a_2 + ... + r_n a_n + r_1^{'}(-a_1^{'}) + r_2^{'}(-a_2^{'}) + ... + r_m^{'}(-a_m^{'}) \\ &= r_1 a_1 + ... + r_m^{'}(-a_m^{'}) \end{aligned}$$

Pero como $(-a_i^{'}) \in A$ con $1 \leq i \leq n$, $x_1 - x_2 \in \sum_{i=1}^{n} r_i a_i$
Ahora sea $k \in R$, entonces tenemos:

$$\begin{aligned} kx_1 &= k(r_1 a_1 + r_2 a_2 + ... + r_n a_n) \\ &= kr_1 a_1 + kr_2 a_2 + ... + kr_n a_n \\ &= (kr_1) a_1 + (kr_2) a_2 + ... + (kr_n) a_n. \end{aligned}$$

Dado que $a_i \in A$ y $kr_i \in R$ para todo $i = 1, 2, ..., n$ entonces $kx_1 \in \sum_{i=1}^{n} r_i a_i$
Por lo tanto el conjunto $\sum_{i=1}^{n} r_i a_i$ es un ideal y es llamado el ideal generado por A.

Definición 1.2.2 *Si A consta de un número finito de elementos $a_1, a_2, ..., a_n$, entonces el ideal generado por $a_1, a_2, ..., a_n$ es denotado por $(a_1, a_2, ..., a_n)$ y consiste en todos los elementos que se pueden escribir de la forma $r_1 a_1 + r_2 a_2 + ... + r_n a_n$, donde los r_i son cualquier elemento de R.*

Se dice que tal ideal es generado finitamente y los elementos a_i son llamados una Base ó Bases de un Ideal.
Además, el ideal generado por la suma y el producto se definen de la siguiente manera:

$$\begin{aligned} (a_1, a_2, ..., a_m) + (b_1, b_2, ..., b_n) &= (a_1, ..., a_m, b_1, ..., b_n) \\ (a_1, a_2, ..., a_m)(b_1, b_2, ..., b_n) &= (..., a_i b_j, ...) \end{aligned}$$

Cuando el ideal es generado por un solo elemento, es decir, por (a) es llamado el Ideal Principal.

1.3. Ideales Primos e Ideales Maximales

Definición 1.3.1 *Un ideal $\mathfrak{p}$ es llamado ideal primo siempre que $ab \in \mathfrak{p}$ al menos uno de ellos pertenece a $\mathfrak{p}$, es decir, a pertenece a $\mathfrak{p}$ ó b pertenece a $\mathfrak{p}$.*

Una definición equivalente es la siguiente:

Definición 1.3.2 *Diremos que $\mathfrak{p}$ es primo si y sólo si para todo $ab \in \mathfrak{p}$ y $a \notin \mathfrak{p}$ siempre cumple la condición que $b \in \mathfrak{p}$.*

Proposición 1.3.1 .
Sea $\mathfrak{p}$ un ideal primo, y supongamos que $a_1 a_2 ... a_n \in \mathfrak{p}$, entonces para al menos un valor de i tenemos que $a_i \in \mathfrak{p}$. Además, si $\mathfrak{a}_1 \mathfrak{a}_2 ... \mathfrak{a}_n$ son ideales y $\mathfrak{a}_1 \mathfrak{a}_2 ... \mathfrak{a}_n \subseteq \mathfrak{p}$, entonces $\mathfrak{a}_i \subseteq \mathfrak{p}$ para al menos un valor de i.

Demostración:

Supongamos que $a_1a_2...a_n \in \mathfrak{p}$ y que $a_i \notin \mathfrak{p}$.

Tenemos $a_1a_2...a_n = a_1(a_2...a_n) \in \mathfrak{p}$ y $a_1 \notin \mathfrak{p}$ por definición de un ideal primo sabemos que si $a_1(a_2...a_n) \in \mathfrak{p}$ y $a_1 \notin \mathfrak{p}$ entonces $a_2a_3...a_n \in \mathfrak{p}$. Ahora repetimos el argumento y para ello tenemos $a_2a_3...a_n = a_2(a_3...a_n) \in \mathfrak{p}$ y $a_2 \notin \mathfrak{p}$ entonces $a_3...a_n \in \mathfrak{p}$ y así sucesivamente obtenemos una sucesión $a_2a_3...a_n \in \mathfrak{p}, a_3a_4...a_n \in \mathfrak{p}, a_4a_5...a_n \in \mathfrak{p}$, y finalmente $a_n \in \mathfrak{p}$ pero esto es una contración ya que habíamos supuesto que $a_n \notin \mathfrak{p}$.

Luego por otra parte asumamos que $\mathfrak{a}_1\mathfrak{a}_2...\mathfrak{a}_n \subseteq \mathfrak{p}$, pero que $\mathfrak{a}_i \nsubseteq \mathfrak{p}$. Luego para cada i podemos elegir $a_i \in \mathfrak{a}_i$ de manera que $a_i \notin \mathfrak{p}$ entonces $a_1(a_2...a_n) \in \mathfrak{a}_1(\mathfrak{a}_2...\mathfrak{a}_n) \subseteq \mathfrak{p}$ y entonces tenemos que $a_1(a_2...a_n) \in \mathfrak{p}$ pero esto es una contradicción ya que en la contrucción de la sucesión tenemos que $a_1, (a_2, ..., a_n) \notin \mathfrak{p}$. Por la tanto $\mathfrak{a}_\mathfrak{i} \subseteq \mathfrak{p}$ para al menos un valor de i.

Definición 1.3.3 *Un ideal primo* $\mathfrak{p}$ *en el anillo* R *es llamado un ideal primo minimal de* $\mathfrak{a}$*, si está contenido en* $\mathfrak{a}$ *y si no existe un ideal primo contenido en* $\mathfrak{a}$*, que está estrictamente contenido en* $\mathfrak{p}$.

Definición 1.3.4 *Un ideal* $\mathfrak{m}$ *en* R *es maximal si* $\mathfrak{m} \neq R$ *y no existe ningún ideal* $\mathfrak{a}$ *tal que* $\mathfrak{m} \subset \mathfrak{a} \subset R$.

Definición 1.3.5 *Un ideal primo propio* $\mathfrak{p}$ *se dice que es un ideal maximal primario del anillo* R*, si no hay otro ideal primo propio contenido en* $\mathfrak{p}$.

1.4. El radical de un ideal

Definición 1.4.1 *Sea* $\mathfrak{a}$ *un ideal en un anillo* R*. El conjunto de todos los elementos* x*, tal que para algún exponente positivo de* x *está en* $\mathfrak{a}$*, es llamado el radical del ideal* $\mathfrak{a}$ *y lo podemos definir como:*

$$r(\mathfrak{a}) = \Big\{x \in R / x^n \in \mathfrak{a};\ \ \textit{para algún}\ n > 0\ \textit{con}\ n \in \mathbb{N}\Big\}.$$

Este conjunto es un ideal.

Sea $x \in r(\mathfrak{a})$, entonces existe $n > 0$ tal que $x^n \in \mathfrak{a}$, es claro que $rx \in r(\mathfrak{a})$ para todo $r \in R$, pues $(rx)^n = r^n x^n \in \mathfrak{a}$ por ser $\mathfrak{a}$ un ideal.

Sean $x,\ y \in r(\mathfrak{a})$, entonces existen m y n tales que $x^m \in \mathfrak{a},\ y^n \in \mathfrak{a}$. Aplicando el teorema del binomio, $(x+y)^{m+n-1}$ es una suma de enteros multiplicados por productos $x^r y^s$, donde $r + s = m + n - 1$; no podemos tener $r < m\ y\ que\ s < n$, entonces cada uno de estos productos está en $\mathfrak{a}$ y por consiguiente

$(x+y)^{m+n-1} \in \mathfrak{a}$. Por lo tanto $x+y \in r(\mathfrak{a})$, de forma análoga se prueba que $x-y \in r(\mathfrak{a})$.
Por tanto $r(\mathfrak{a})$ es un ideal.

Proposición 1.4.1 *Sean* $\mathfrak{a}$ *y* $\mathfrak{a}_1, \mathfrak{a}_2, ..., \mathfrak{a}_n$ *ideales en el anillo* R*, entonces*

1) $\mathfrak{a} \subseteq r(\mathfrak{a}) = r(r(\mathfrak{a}))$

2) $r(\mathfrak{a}_1\mathfrak{a}_2...\mathfrak{a}_n) = r(\bigcap_{j=1}^{n} \mathfrak{a}_j) = \bigcap_{j=1}^{n} r(\mathfrak{a}_j)$

3) $r(\mathfrak{a}) = R$ *si y sólo si* $\mathfrak{a} = R$.

4) $r(\mathfrak{a}_1 + \mathfrak{a}_2) = r(r(\mathfrak{a}_1) + r(\mathfrak{a}_2))$.

5) *Si* $\mathfrak{p}$ *es un ideal primo, entonces* $r(\mathfrak{p}^n) = \mathfrak{p}$ *para todo* $n > 0$.

Demostración:
1) Para toda $x \in \mathfrak{a}$, se tendrá que $x^1 \in \mathfrak{a}$; $1 \in \mathbb{N}$, entonces $x \in r(\mathfrak{a})$.
Por lo tanto $\mathfrak{a} \subseteq r(\mathfrak{a})$.
Luego sea $x \in r(\mathfrak{a})$, entonces existe un $n > 0 \in \mathbb{N}$ tal que $x^n \in \mathfrak{a}$, tomando algún $m > 0 \in \mathbb{N}$ entonces $(x^n)^m \in r(\mathfrak{a})$, es decir, $x \in r(\mathfrak{a})$.
Por lo tanto $r(\mathfrak{a}) \subseteq r(r(\mathfrak{a}))$.
Si $x \in r(r(\mathfrak{a}))$, existe un $n > 0$, tal que $x^n \in r(\mathfrak{a})$ y entonces $x^{nm} = (x^n)^m$ para cierto $m > 0 \in \mathbb{N}$, entonces $x \in \mathfrak{a}$ y por lo tanto $r(r(\mathfrak{a})) \subseteq r(\mathfrak{a})$.
2) Si $x \in \bigcap_{j=1}^{n} r(\mathfrak{a}_j)$, existen $m_1, m_2, ..., m_n > 0$ tal que $x^{m_j} \in \mathfrak{a}_j$ para cada $j = 1, 2, ..., n$; luego tomando $m = m_1 + m_2 + ... + m_n$ tenemos

$$\begin{aligned} x^m &= x^{m_1+m_2+...+m_n} \\ &= x^{m_1}x^{m_2}...x^{m_n} \in \mathfrak{a}_1\mathfrak{a}_2...\mathfrak{a}_n, \end{aligned}$$

así $\bigcap_{j=1}^{n} r(\mathfrak{a}_j) \subseteq r(\mathfrak{a}_1, \mathfrak{a}_2, ..., \mathfrak{a}_n)$. dado que $\mathfrak{a}_1\mathfrak{a}_2...\mathfrak{a}_n \subseteq \bigcap_{j=1}^{n} \mathfrak{a}_j$ por la proposición 1.1.1 literal 3.2 tenemos que $r(\mathfrak{a}_1\mathfrak{a}_2...\mathfrak{a}_n) \subseteq r(\bigcap_{j=1}^{n} \mathfrak{a}_j)$. Finalmente, si $x \in r(\bigcap_{j=1}^{n} \mathfrak{a}_j)$, existe un $n > 0$ tal que $x^n \in \bigcap_{j=1}^{n} \mathfrak{a}_j$, entonces para cada $j = 1, 2, ..., n$, $x^n \in \mathfrak{a}_j$, es decir, $x \in r(\mathfrak{a}_j)$, entonces $x \in \bigcap_{j=1}^{n} r(\mathfrak{a}_j)$ y $r(\bigcap_{j=1}^{n} \mathfrak{a}_j) = \bigcap_{j=1}^{n} r(\mathfrak{a}_j)$.
Así $r(\bigcap_{j=1}^{n} \mathfrak{a}_j) = \bigcap_{j=1}^{n} r(\mathfrak{a}_j) \subseteq r(\mathfrak{a}_1\mathfrak{a}_2...\mathfrak{a}_n) \subseteq r(\bigcap_{j=1}^{n} \mathfrak{a}_j)$, es lo que se quería probar.
3) Sea $r(\mathfrak{a}) = R$, para todo $r \in R$, existe un $n > 0$ tal que $r^n \in \mathfrak{a}$, en particular $1 = 1^n \in \mathfrak{a}$. Por lo

tanto $\mathfrak{a} = R$.

Recíprocamente por 1) sabemos que $\mathfrak{a} \subseteq r(\mathfrak{a})$ pero $\mathfrak{a} = R$ entonces $R \subseteq r(\mathfrak{a})$.

Sea $x \in r(\mathfrak{a})$, entonces existe un $n > 0$, tal que $x^n \in \mathfrak{a}$, en particular para un $n = 1$ tenemos que $x \in R$ por ser $\mathfrak{a} = R$ y por lo tanto $r(\mathfrak{a}) \subseteq R$.

4) Dado que $\mathfrak{a}_1 \subseteq r(\mathfrak{a}_1)$ y $\mathfrak{a}_2 \subseteq r(\mathfrak{a}_2)$ por 1) tenemos:

$$\begin{aligned} \mathfrak{a}_1 + \mathfrak{a}_2 &\subseteq r(\mathfrak{a}_1) + r(\mathfrak{a}_2) \\ r(\mathfrak{a}_1 + \mathfrak{a}_2) &\subseteq r(r(\mathfrak{a}_1) + r(\mathfrak{a}_2)). \end{aligned}$$

Para probar la otra inclusión, tomemos $x \in r(r(\mathfrak{a}_1) + r(\mathfrak{a}_2))$, entonces existe un $n > 0$ tal que $x_n \in r(\mathfrak{a}_1) + r(\mathfrak{a}_2)$, luego sea $x^n = x_1 + x_2$ donde $x_1 \in \mathfrak{a}_1$ y $x_2 \in \mathfrak{a}_2$, es decir, existen n_1 y n_2 tales que $x_1^{n_1} \in \mathfrak{a}_1$ y $x_2^{n_2} \in \mathfrak{a}_2$, luego $(x^n)^{n_1+n_2-1} = (x_1+x_2)^{n_1+n_2-1}$, por el binomio de Newton $(x_1+x_2)^{n_1+n_2-1}$ es una suma de enteros multiplicativos por productos $x_1^r x_2^s$ donde $r + s = n_1 + n_2 - 1$ y no podemos tener $r < n_1$ y $s < n_2$, entonces cada uno estos productos están en $\mathfrak{a}_1$ ó en $\mathfrak{a}_2$, por lo tanto $x^{n(n_1+n_2-1)} \in \mathfrak{a}_1 + \mathfrak{a}_2$ y $x \in r(\mathfrak{a}_1 + \mathfrak{a}_2)$.

Por lo tanto $r(r(\mathfrak{a}_1) + r(\mathfrak{a}_2)) \subseteq r(\mathfrak{a}_1 + \mathfrak{a}_2)$.

5) Sea $\mathfrak{p}$ un ideal primo, por 2) tenemos

$$\begin{aligned} r(\mathfrak{p}^n) &= r(\underbrace{\mathfrak{p}\mathfrak{p}...\mathfrak{p}}_{n \ veces}) \\ &= r(\mathfrak{p} \cap \mathfrak{p} \cap ... \cap \mathfrak{p}) \\ &= r(\mathfrak{p}). \end{aligned}$$

Pero por 1) sabemos que $r(\mathfrak{p}^n) = r(\mathfrak{p}) \supseteq \mathfrak{p}$.

Solo nos hace falta probar que $r(\mathfrak{p}) \subseteq \mathfrak{p}$, sea $x \in r(\mathfrak{p})$ y sea n el menor entero positivo tal que $x^n \in \mathfrak{p}$, luego como $\mathfrak{p}$ es primo entonces $x \in \mathfrak{p}$ ó $x^{n-1} \in \mathfrak{p}$, pero como n es el menor entero positivo entonces $n = 1$ y por lo tanto $x \in \mathfrak{p}$, entonces $r(\mathfrak{p}) \subseteq \mathfrak{p}$.

1.5. Ideales Primarios.

Definición 1.5.1 *Un ideal $\mathfrak{q} \neq R$ en un anillo R es llamado un ideal primario si para todo $a, b \in R$ tenemos que $ab \in \mathfrak{q}$ y $a \notin \mathfrak{q}$ entonces existe un exponente n positivo de b que pertenece a $\mathfrak{q}$.*

En otras palabras,$\mathfrak{q} \neq R$ es un ideal primario *si* $a, b \in R$ *tenemos que* $ab \in \mathfrak{q}$ *y* $a \notin \mathfrak{q}$*, entonces* $b^n \in \mathfrak{q}$ *para algún* $n > 0$.
Una definición equivalente es la siguiente.

Definición 1.5.2 *Un ideal* $\mathfrak{q}$ *en un anillo* R *es primario si* $\mathfrak{q} \neq R$ *y si* $ab \in \mathfrak{q}$ *entonces para cada* $a \in \mathfrak{q}$ *ó* $b^n \in \mathfrak{q}$ *para algún* $n > 0$.

Es claro que todo ideal primo es primario, pero no es cierto el recíproco. Veamos un ejemplo:

Ejemplo 1.5.1 * *Si* $\mathfrak{p}$*, es un número primo para todo entero positivo* $n \geqslant 2$*, se tiene que* $(\mathfrak{p}^n) = (\mathfrak{p})^n$*, es un ideal primario en* $\mathbb{Z}$ *pero no es primo en* $\mathbb{Z}$.

* Veamos primero que no es primo, pues $\mathfrak{p}\mathfrak{p}^{n-1} \in (\mathfrak{p}^n)$ pero $\mathfrak{p}$ y $\mathfrak{p}^{n-1}$ no están en $(\mathfrak{p}^n)$.
Por lo tanto $(\mathfrak{p})^n$ no es primo en $\mathbb{Z}$.
Para ver que es primario, sean $a, b \in \mathbb{Z}$ tales que $ab \in (\mathfrak{p}^n)$ y que $a \notin (\mathfrak{p}^n)$, luego $\mathfrak{p}^n$ divide a ab, pero no divide a a ya que $a \notin (\mathfrak{p}^n)$ entonces $\mathfrak{p}$ divide a b y en consecuencia $b^n \in (\mathfrak{p}^n)$.
Por lo tanto $(\mathfrak{p})^n$, es un ideal primario en $\mathbb{Z}$.

Proposición 1.5.1 *Sea* $\mathfrak{q}$ *un ideal primario y, sea* $\mathfrak{p}$ *el conjunto de todos los elementos* x *tal que* $x^n \in \mathfrak{q}$ *para al menos un valor entero positivo* n *entonces* $\mathfrak{p}$ *es un ideal primo conteniendo* $\mathfrak{q}$*, y para cualquier otro ideal primo* $\mathfrak{p}'$ *conteniendo* $\mathfrak{q}$*, se tiene que* $\mathfrak{p} \subseteq \mathfrak{p}'$*. Esto es* $\mathfrak{q} \subseteq \mathfrak{p} \subseteq \mathfrak{p}'$.

Demostración:
Demostremos que $\mathfrak{p}$ es un ideal.
Sean $x, y \in \mathfrak{p}$ y $r \in R$, entonces existen enteros m y n, tal que $x^m \in \mathfrak{q}$ y $y^n \in \mathfrak{q}$. Ahora tenemos:

$$\begin{aligned}(x+y)^{m+n} &= \sum_{k=0}^{m+n} \binom{m+n}{k} x^{(m+n)-k} y^k \\ &= x^{m+n} + ... + \binom{(m+n)-k}{k} x^{(m+n)-k} y^k + ... + y^{m+n} \\ &= x^m x^n + ... + \binom{(m+n)-k}{k} x^{(m+n)-k} y^k + ... + y^m y^n.\end{aligned}$$

Pero como en el primer caso $x^m \in \mathfrak{q}$ y en el segundo caso $y^n \in \mathfrak{q}$, de modo que en ambos casos $x^m y^n \in \mathfrak{q}$. Esto demuestra que $(x+y)^{m+n} \in \mathfrak{q}$, en consecuencia, por la definición del ideal $\mathfrak{p}$, $x+y \in \mathfrak{p}$.

Y haciendo un argumento parecido demostramos que $x - y \in \mathfrak{p}$.
Ahora, sea $x \in \mathfrak{p}$ entonces existe entero m tal que $x^m \in \mathfrak{q}$ y sea $r \in R$ entonces:

$$(rx)^m = r^m \underbrace{x^m}_{\in \mathfrak{q}}$$

Por lo tanto $r^m x^m \in \mathfrak{q}$ y entonces $rx \in \mathfrak{p}$ por hipótesis con respecto al ideal $\mathfrak{p}$.
Y como $x + y,\ x - y \in \mathfrak{p}$ y $rx \in \mathfrak{p}$, entonces $\mathfrak{p}$ es un ideal.

Ahora probemos que $\mathfrak{p}$ es primo. Asumamos que $ab \in \mathfrak{p}$ y que $a \notin \mathfrak{p}$ por definición de un ideal primo, basta probar que $b \in \mathfrak{p}$. Ya que $ab \in \mathfrak{p}$, por hipótesis existe un entero positivo s tal que $(ab)^s \in \mathfrak{q}$ pero como $(ab)^s = a^s b^s \in \mathfrak{q}$, pero $a^s \notin \mathfrak{q}$, por definición de un ideal primario, pues de lo contrario a pertenecería a $\mathfrak{p}$. Por lo tanto ya que $\mathfrak{q}$ es un ideal primario algún exponente s tal que $(b^s)^r \in \mathfrak{q}$ esto se cumple para algún entero positivo, tomando un exponente apropiado tenemos que $b \in \mathfrak{p}$.
Por lo tanto $\mathfrak{p}$ es primo.

Probemos que $\mathfrak{q} \subseteq \mathfrak{p}$. Sea $x \in \mathfrak{p}$, como $\mathfrak{p}$ es el conjunto de todos los elementos x tal que $x^n \in \mathfrak{q}$ entonces $x^n \in \mathfrak{q}$, tomando un valor apropiado para n , es decir, con $n = 1$ tenemos que $x \in \mathfrak{q}$ y por lo tanto $\mathfrak{q} \subseteq \mathfrak{p}$.
Finalmente probemos que $\mathfrak{p} \subseteq \mathfrak{p}'$. Sea $\mathfrak{p}'$ cualquier otro ideal primo conteniendo a $\mathfrak{q}$ y sea $x \in \mathfrak{p}$, pero como $\mathfrak{p}$ es el conjunto de elementos x tal que $x^n \in \mathfrak{q}$ y supongamos que $\mathfrak{q} = \mathfrak{q}_1\mathfrak{q}_2...\mathfrak{q}_n \subseteq \mathfrak{p}'$, entonces por la *proposición 1.3.1* sabemos que $x^n \in \mathfrak{q} = \mathfrak{q}_1\mathfrak{q}_2...\mathfrak{q}_n \subseteq \mathfrak{p}'$ entonces $\mathfrak{q}_i \subseteq \mathfrak{p}'$ para al menos un valor de i, con $i = 1, 2, ..., n$, tomando un valor apropiado para i tenemos que $\mathfrak{q} \subseteq \mathfrak{p}'$ además $x^n \in \mathfrak{q} \subseteq \mathfrak{p}'$ entonces $x^n \in \mathfrak{p}'$ para al menos un exponente positivo entonces tomando apropiadamente tenemos que $x \in \mathfrak{p}'$ y por lo tanto $\mathfrak{p} \subseteq \mathfrak{p}'$.

1.6. Ideales con una Descomposición Primaria

Definición 1.6.1 *Si un ideal* $\mathfrak{a}$ *se puede expresar de la siguiente forma:*

$$\mathfrak{a} = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap ... \cap \mathfrak{q}_n,$$

donde cada $\mathfrak{q}_i$ *es un ideal primario, diremos que tenemos una descomposición primaria de* $\mathfrak{a}$ *y cada* $\mathfrak{q}_i$ *se llamará componente primaria de la descomposición primaria del ideal* $\mathfrak{a}$.

Hay un tipo importante de anillo el cuál es el *Anillo Notheriano* en el que todo ideal tiene una descomposición primaria y es principalmente en los anillos que trabajaremos.

Definición 1.6.2 *Sean* $\mathfrak{p}$ y $\mathfrak{q}$ *ideales en el anillo* R *y si* $\mathfrak{p} = r(\mathfrak{q})$*, entonces diremos que* $\mathfrak{q}$ *es* $\mathfrak{p}$*-primario*

Definición 1.6.3 *Diremos que ideal* $\mathfrak{a}$ *es descomponible si tiene una una descomposición primaria.*

Ejemplo 1.6.1 *Encontrar una descomposición primaria del ideal* $\mathfrak{a} = (xy, y^2)$.

Solución: Podemos descomponer al ideal $\mathfrak{a}$ como:

$$\begin{aligned} \mathfrak{a} &= (xy, y^2) \\ &= (x) \cap (x, y^2). \end{aligned}$$

Por lo tanto la descomposición primaria del ideal $\mathfrak{a}$ es $(x) \cap (x, y^2) = (xy, y^2)$.

Teorema 1.6.1 *Sea* $\mathfrak{a} = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap ... \cap \mathfrak{q}_n$*, donde* $\mathfrak{q}_i$ *es* $\mathfrak{p}_i$*-primario para* $1 \leq i \leq n$*. Entonces cualquier ideal primo que este contenido en* $\mathfrak{a}$ *debe contener al menos uno de los* $\mathfrak{p}_i$*; el ideal primo minimal de* $\mathfrak{a}$ *son precisamente los ideales primos* $\mathfrak{p}_i$ *que no contienen estrictamente cualquier otro* $\mathfrak{p}_j$*, es decir, el* $r(\mathfrak{a}) = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap ... \cap \mathfrak{q}_n$*, y más precisamente , el radical de* $\mathfrak{a}$ *es la intersección de todos los ideales primos minimales.*

Demostración:
Supongamos que $\mathfrak{p}$ un ideal primo contenido en $\mathfrak{a}$, entonces

$$\begin{aligned} \mathfrak{q}_1\mathfrak{q}_2...\mathfrak{q}_n &= \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap ... \cap \mathfrak{q}_n \\ &= \mathfrak{a} \subseteq \mathfrak{p} \end{aligned}$$

consecuentemente, por la proposición 1.1.1 literal 3.2) y por la proposición 1.3.2, podemos escoger un i tal que $\mathfrak{q}_i \subseteq \mathfrak{p}$, por la proposición 1.5.1 tenemos que $\mathfrak{p}_i \subseteq \mathfrak{p}$, aplicando la definición de ideales primos minimales de un ideal tenemos que $\mathfrak{p}_i \subseteq \mathfrak{a}$ y $\mathfrak{p}_j \nsubseteq \mathfrak{a} \subseteq \mathfrak{p}$.
Ahora, sea $x \in r(\mathfrak{a})$, y m un entero adecuado tal que $x^m \in \mathfrak{a} \subseteq \mathfrak{q}_i \subseteq \mathfrak{p}_i$, con $x \in \mathfrak{p}_i$ para $1 \leq i \leq n$, entonces $x \in \cap_{i=1}^{n} \mathfrak{p}_i$ y por lo tanto tenemos que

$$r(\mathfrak{a}) \subseteq \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap ... \cap \mathfrak{q}_n \tag{1.7}$$

Sea $y \in \mathfrak{a} = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap ... \cap \mathfrak{q}_n$, entonces para cada i, tenemos que $y \in \mathfrak{p}_i$, entonces podemos encontrar m_i tal que $y^{m_i} \in \mathfrak{q}_i$ y tomando a $m = max(m_1, m_2, ..., m_n)$,
$y^m \in \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap ... \cap \mathfrak{q}_n = \mathfrak{a}$ y entonces tenemos que $y \in r(\mathfrak{a})$ y por lo tanto

$$r(\mathfrak{a}) \quad \supseteq \quad \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap ... \cap \mathfrak{q}_n \tag{1.8}$$

De 1.7 y 1.8 tenemos $r(\mathfrak{a}) = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap ... \cap \mathfrak{q}_n$.

Corolario 1.6.1 *Si* $\mathfrak{q}$ *es* $\mathfrak{p}$*-primario,* $ab \in \mathfrak{q}$*, y* $a \notin \mathfrak{p}$ *entonces* $b \in \mathfrak{q}$.

Demostración:

Supongamos que $ab \in \mathfrak{q}$ y que $a \notin \mathfrak{p}$, como $\mathfrak{q}$ es un ideal $\mathfrak{p}$-primario entonces $\mathfrak{p} = r(\mathfrak{q})$ y necesitamos probar que $\mathfrak{q} = \mathfrak{p}$ entonces sea $x \in \mathfrak{p} = r(\mathfrak{q})$, entonces $x^n \in \mathfrak{q}$, para algún entero positivo $n > 0$, tomando el menor entero tenemos que $x \in \mathfrak{q}$, así $\mathfrak{p} \subseteq \mathfrak{q}$.
Luego para toda $x \in \mathfrak{q}$ tendremos que $x^1 \in \mathfrak{q}$, con $1 \in \mathbb{N}$, entonces $x \in r(\mathfrak{q}) = \mathfrak{p}$ por ser $\mathfrak{q}$ $\mathfrak{p}$-primario. Entonces $\mathfrak{q} \subseteq \mathfrak{p}$ y por lo tanto $\mathfrak{q} = \mathfrak{p}$.
Y como por hipótesis $ab \in \mathfrak{q}$ y $a \notin \mathfrak{q} = \mathfrak{p}$, entonces $a \notin \mathfrak{p}$ y por definición de ideal primo, no le queda de otra que $b \in \mathfrak{q}$.

Corolario 1.6.2 *Si* $\mathfrak{q}$ *es* $\mathfrak{p}$*-primario,* $\mathfrak{ab} \subseteq \mathfrak{q}$*, y* $\mathfrak{a} \nsubseteq \mathfrak{p}$ *, entonces* $\mathfrak{b} \subseteq \mathfrak{q}$.

Demostración:

Podemos elegir un $a_0 \in \mathfrak{a}$ de modo que $a_0 \notin \mathfrak{p}$ y si ahora b es un elemento cualquiera de $\mathfrak{b}$, tenemos que $a_0 b \in \mathfrak{q}$, ya que $\mathfrak{ab} \subseteq \mathfrak{q}$ y que $a_0 \notin \mathfrak{p}$ entonces $b \in \mathfrak{q}$ por el corolario 1.6.1, y como b es un elemento cualquiera de $\mathfrak{b}$ entonces $\mathfrak{b} \subseteq \mathfrak{q}$.

Corolario 1.6.3 *Si* $\mathfrak{q}$ *es* $\mathfrak{p}$*-primario y si* $\mathfrak{a} \nsubseteq \mathfrak{p}$ *entonces* $(\mathfrak{q} : \mathfrak{a}) = \mathfrak{q}$.

Demostración:

Sabemos que $\mathfrak{a}(\mathfrak{q} : \mathfrak{a}) \subseteq \mathfrak{q}$, por la proposición 1.1.1 literal 4). Dado que $\mathfrak{a} \nsubseteq \mathfrak{q}$, por el corolario 1.6.2 tenemos:

$$(\mathfrak{q} : \mathfrak{a}) \quad \subseteq \quad \mathfrak{q} \tag{1.9}$$

por el corolario 1.6.2 .

La otra inclusión es inmediata utilizando la proposición 1.1.1 literal 4.1 .

Así

$$\mathfrak{q} \subseteq (\mathfrak{q} : \mathfrak{a}) \tag{1.10}$$

De 1.9 y 1.10 tenemos que $(\mathfrak{q} : \mathfrak{a}) = \mathfrak{q}$.

Lema 1.6.1 *Supongamos que* $\mathfrak{p}'$ *y* $\mathfrak{q}'$ *son ideales para los cuales se satisfacen las siguientes condiciones:*

1) $\mathfrak{p}' \supseteq \mathfrak{q}'$

2) *Si* $x \in \mathfrak{p}'$*, entonces existe algún exponente positivo de* x *que está en* $\mathfrak{q}'$.

3) *Si* $ab \in \mathfrak{q}'$ *y* $a \notin \mathfrak{p}'$*, entonces* $b \in \mathfrak{q}'$.

Entonces $\mathfrak{p}'$ *es un ideal primo, y* $\mathfrak{q}'$ *es un ideal primario que está incluido en* $\mathfrak{p}'$.

Demostración:

Comenzamos por mostrar que $\mathfrak{q}'$ es un ideal primario. Asumamos que $ab \in \mathfrak{q}'$ y que $b \notin \mathfrak{q}'$, entonces, por 3), $a \notin \mathfrak{p}'$, además por 2), existe un entero n tal que $a^n \in \mathfrak{q}'$ entonces para algún entero positivo n, el elemento a está en $\mathfrak{q}'$ por lo tanto q' es primario.

Probemos que $\mathfrak{p}'$ es un ideal primo. Sea $ab \in \mathfrak{p}'$ entonces por 2) existe algún exponente positivo s tal que $(ab)^s \in \mathfrak{q}'$, pero como $(ab)^s = a^s b^s \in \mathfrak{q}'$ y $a^s \notin \mathfrak{q}'$ por 3) se tiene que $b^s \in \mathfrak{q}' \subseteq \mathfrak{p}'$; por 1) $b^s \in \mathfrak{p}'$ luego tomando un entero positivo apropiado tenemos que $b \in \mathfrak{p}'$, por lo tanto $\mathfrak{p}'$ es un ideal primo.

Sea $\mathfrak{q}'$ $\mathfrak{p}$-primario, para cualquier ideal $\mathfrak{p}$ demostremos que $\mathfrak{p}' \subseteq \mathfrak{p}$ ya que si tomamos $x \in \mathfrak{p}'$ entonces existe exponente n positivo n tal que $x^n \in \mathfrak{p}$, para un entero conveniente tenemos que $x \in \mathfrak{p}$ y entonces $\mathfrak{p}' \subseteq \mathfrak{p}$.

Ahora probemos que $\mathfrak{p} \subseteq \mathfrak{p}'$, sea $x \in \mathfrak{p}$, por ser $\mathfrak{q}'$ $\mathfrak{p}$-primario por definición 1.6.2 $\mathfrak{p} = r(\mathfrak{q}')$, es decir, $x \in r(\mathfrak{q}')$ entonces existe un entero i positivo tal que $x^i \in \mathfrak{q}'$. Por un lado, si $i = 1$ tenemos que $x \in \mathfrak{q}' \subseteq \mathfrak{p}'$, por 1) y por el otro lado, si $i > 1$ entonces $x^i = xx^{i-1} \in \mathfrak{q}'$ y $x^{i-1} \notin \mathfrak{q}'$, por consiguiente utilizando 3) tenemos que $x \in \mathfrak{q}' \subseteq p'$ por 1), entonces $x \in \mathfrak{p}'$. Por lo tanto $\mathfrak{p} = \mathfrak{p}'$.

Por lo tanto $\mathfrak{q}' \subseteq \mathfrak{p}'$.

Proposición 1.6.1 *Si* $\mathfrak{q}_1, \mathfrak{q}_2, ..., \mathfrak{q}_n$ *son todos ideales* $\mathfrak{p}$*-primarios, entonces* $\mathfrak{q} = \bigcap_{i=1}^{n} \mathfrak{q}_i$ *es también un ideal* $\mathfrak{p}$*-primario.*

Demostración:

Sea $\mathfrak{q}$ y $\mathfrak{p}$ ideales donde $\mathfrak{q} = \cap_{i=1}^{n} \mathfrak{q}_i$ y como cada q_i es $\mathfrak{p}$-primario, por hipótesis $\mathfrak{q}_i$ está en $\mathfrak{p}$ y por lo tanto $\mathfrak{q} \subseteq \mathfrak{p}$.

Ahora sea $x \in \mathfrak{p}$ entonces para cada i podemos encontrar enteros m_i talque $x^{m_i} \in \mathfrak{q}_i$ y tomando $m = max(m_1, m_2, ..., m_n)$ tendremos que $x^m \in \mathfrak{q}_i$ para cada $1 \leq i \leq n$, es decir, $x^m \in \mathfrak{q}$. Supongamos que $ab \in \mathfrak{q}$ y $a \notin \mathfrak{p}$, como $\mathfrak{q} = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap ... \cap \mathfrak{q}_n$ entonces $ab \in \mathfrak{q} = \cap_{i=1}^{n} \mathfrak{q}_i$ entonces $ab \in \mathfrak{q}_i$ para todo i y $a \notin \mathfrak{p}$, por lo tanto $b \in \mathfrak{q}_i$ para todo i , entonces $b \in \mathfrak{q}$ y del lema 1.6.1 deducimos que $\mathfrak{q}$ es $\mathfrak{p}$-primario.

Proposición 1.6.2 *Si* $\mathfrak{q}$ *es* $\mathfrak{p}$*-primario y si* $\mathfrak{a}$ *es un ideal no conteniendo* $\mathfrak{q}$*, entonces* $(\mathfrak{q} : \mathfrak{a})$ *es* $\mathfrak{p}$*-primario. Pero si* $\mathfrak{a} \subseteq \mathfrak{q}$ *entonces* $(\mathfrak{q} : \mathfrak{a}) = (1)$.

Demostración:

Supongamos que $\mathfrak{a} \subseteq \mathfrak{q}$ y supongamos que $\mathfrak{q}' = (\mathfrak{q} : \mathfrak{a})$, como $\mathfrak{a} \subseteq \mathfrak{q}$ podemos encontrar $a_0 \in \mathfrak{a}$ tal que $a_0 \notin \mathfrak{q}$. Si tomamos $y \in \mathfrak{q}'$ entonces $a_0 y \in \mathfrak{q}$ y $a_0 \notin \mathfrak{q}$ por lo tanto $y \in \mathfrak{p}$ y entonces $\mathfrak{q}' \subseteq \mathfrak{p}$.

Si $x \in \mathfrak{p}$ entonces con un entero m apropiado tenemos que $x^m \mathfrak{q} \subseteq \mathfrak{q}'$ por ser $\mathfrak{q}$ $\mathfrak{p}$-primario, supongamos que $\alpha\beta \in \mathfrak{q}'$ y que $\alpha \notin \mathfrak{p}$, entonces para cualquier $a \in \mathfrak{a}$ tenemos que

$a(\alpha\beta) = a(\beta\alpha) = (a\beta)\alpha \in \mathfrak{q}$ y como $\alpha \notin \mathfrak{p}$ entonces $a\beta \in \mathfrak{q}$ y por lo tanto $\beta \in (\mathfrak{q} : \mathfrak{a}) = \mathfrak{q}'$ y luego del lema 1.6.1 deducimos que $\mathfrak{q}'$ es $\mathfrak{p}$-primario. Dado que $\mathfrak{q}' = (\mathfrak{q} : \mathfrak{a})$, entonces $(\mathfrak{q} : \mathfrak{a})$ es $\mathfrak{p}$-primario.

Ahora si $\mathfrak{a} \subseteq \mathfrak{q}$ entonces todos los elementos del anillo R están en $(\mathfrak{q} : \mathfrak{a})$, de modo que

$(\mathfrak{q} : \mathfrak{a}) = R = (1)$.

Proposición 1.6.3 *Sea* $\mathfrak{a}$ *un ideal y sean* $\mathfrak{p}_1, \mathfrak{p}_2, ..., \mathfrak{p}_n$ *ideales primos ninguno de los cuales están contenidos en* $\mathfrak{a}$*, entonces existe un elemento* $a \in \mathfrak{a}$ *tal que no está contenido en* $\mathfrak{p}_i$ *para todo* $i = 1, 2, ..., n$*.*

Demostración:

Usemos inducción sobre el número n de ideales primos.

Si $n = 1$ entonces $\mathfrak{p}_1 \nsubseteq \mathfrak{a}$ entonces $a_i \in \mathfrak{a}$ talque $\mathfrak{p}_1 \nsubseteq \mathfrak{a}$.

si $n = k - 1$ entonces $\mathfrak{p}_1, \mathfrak{p}_2, ..., \mathfrak{p}_{k-1} \nsubseteq \mathfrak{a}$ entonces para cada i $(1 \leq i \leq k - 1)$ existe un elemento $a_i \in \mathfrak{a}$ que no está contenido en cualquier $\mathfrak{p}_1, \mathfrak{p}_2, ..., \mathfrak{p}_{k-1}$ es decir que $\mathfrak{p}_1, \mathfrak{p}_2, ..., \mathfrak{p}_{k-1} \nsubseteq a$.

Si $n = k$ entonces $\mathfrak{p}_1, \mathfrak{p}_2, ..., \mathfrak{p}_{k-1}, \mathfrak{p}_k \nsubseteq \mathfrak{a}$ entonces para cada i $(1 \leq i \leq k)$ existe un elemento

$a_i \in \mathfrak{a}$ que no está contenido en cualquier $\mathfrak{p}_1, \mathfrak{p}_2, ..., \mathfrak{p}_{i-1}, \mathfrak{p}_{i+1}..., \mathfrak{p}_{k-1}$,$\mathfrak{p}_k$. Entonces para al menos un i tenemos que $a_i \notin \mathfrak{p}_i$ y en este caso no hay nada que probar. Por lo tanto probaremos el caso donde $a_i \in \mathfrak{p}_i$ para todo i. Supongamos que $a = \sum_{i=1}^{n}(a_1a_2...a_{i-1}a_{i+1}...a_k)$, entonces el término j-ésimo en la sumatoria no pertenece a $\mathfrak{p}_j$, supongamos que $i \neq j$ entonces $a_1a_2...a_{i-1}a_{i+1}...a_k \in \mathfrak{p}_j$ ya que a_j está en el producto. Y esto demuestra que $a \notin \mathfrak{p}$, independientemente del valor de j y como $a \in \mathfrak{a}$ porque todos los $a_1a_2...a_{i-1}a_{i+1}...a_k \in \mathfrak{a}$.

Capítulo 2

Los Anillos Noetherianos Conmutativos

2.1. Definiciones y Condiciones en anillos Noetherianos

Recordamos que un ideal $\mathfrak{a}$ es finito, si podemos encontrar un conjunto finito $a_1, a_2, ..., a_n$ de elementos, tal que

$$\mathfrak{a} = Ra_1 + Ra_2 + ... + Ra_n$$

Ra_i es sólo otra manera de escribir el ideal principal (a_i), que utilizaremos cuando hagamos hincapié en que (a_i) se compone de todos los elementos de la forma ra_i donde r es un elemento arbitrario de R.

Definición 2.1.1 *Un anillo R se llama Noetheriano si todo ideal de R es finito.*

Con el fin de poner la condición Noetheriana de formas alternativas, damos dos definiciones más.

Definición 2.1.2 *Una cadena ascendente en R dice que, si cada vez que tenemos una secuencia infinita de ideales que cada vez es mayor, es decir,*

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq ...$$

entonces, existe un entero m tal que $\mathfrak{a}_n = \mathfrak{a}_m$ para todo $n \geq m$.

Definición 2.1.3 *La condición maximal, dice que R tiene un maximal, si dado cualquier conjunto no vacío $\mathfrak{S}$ de ideales, existe un ideal $\mathfrak{a}$, en el conjunto $\mathfrak{S}$, y tal que si $\mathfrak{b}$ pertenece a $\mathfrak{S}$ y $\mathfrak{a} \subseteq \mathfrak{b}$, entonces $\mathfrak{a} = \mathfrak{b}$.*

En otras palabras, cada conjunto $\mathfrak{S}$ no vacío de ideales, contiene un ideal, es decir, un ideal $\mathfrak{b}$, que es maximal.

Esto, sin embargo, no significa que el ideal $\mathfrak{a}$, que es maximal, contiene todos los ideales del conjunto $\mathfrak{S}$; sólo significa que el ideal $\mathfrak{a}$ no está contenido por cualquier otro ideal del conjunto.

Teorema 2.1.1 *Los siguientes tres enunciados son equivalentes:*

(1) La condición de la cadena ascendente se tiene en R;

(2) La condición maximal, para ideales, se tiene en R;

(3) Todo ideal en R es generado finitamente; y cada uno de ellos es equivalente a decir que: R es noetheriano.

Demostración:

$(1) \Rightarrow (2)$: Supongamos que se cumple la condición de la cadena, y sea $\mathfrak{S}$ un conjunto no vacío de ideales. Vamos a suponer que ningún miembro de $\mathfrak{S}$ es maximal y por lo tanto derivar una contradicción. Esto demostrará (1) implica (2). Dado que $\mathfrak{S}$ no es vacío, contiene al menos un ideal; sea $\mathfrak{a}_1 \in \mathfrak{S}$ tal ideal, por hipótesis, $\mathfrak{a}_1$ no puede ser maximal; por lo tanto podemos encontrar $\mathfrak{a}_2 \in \mathfrak{S}$ tal que $\mathfrak{a}_2 \supset \mathfrak{a}_1$.

Una vez más, ya que $\mathfrak{a}_2$ no es maximal, entonces existe un $\mathfrak{a}_3 \in \mathfrak{S}$ tal que $\mathfrak{a}_3 \supset \mathfrak{a}_2$ y así sucesivamente. Esto da una contradicción , porque en la secuencia $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, ...$ viola la condición de cadena ascendente, definición 2.1.2.

$(2) \Rightarrow (3)$: Ahora supongamos que la condición de maximal se mantiene, y sea $\mathfrak{a}$ un ideal dado. Denotemos por $\mathfrak{S}$ el conjunto de todos los ideales finitamente generados que estan contenidos en $\mathfrak{a}$ entonces $\mathfrak{S}$ no es vacío porque contiene (0). Si $\mathfrak{a}^* = Ra_1 + Ra_2 + ... + Ra_n$ es un ideal del conjunto $\mathfrak{S}$ que es maximal, entonces $\mathfrak{a}^* \subseteq \mathfrak{a}$. Vamos a demostrar que $\mathfrak{a}^* = \mathfrak{a}$ del cual se sigue que $\mathfrak{a}$ es finito, y, por tanto, demostraríamos (2) implica (3).

Ahora si $\mathfrak{a}^* \neq \mathfrak{a}$, entonces podemos encontrar un $b \in \mathfrak{a}$ tal que $b \notin \mathfrak{a}^*$, y luego el ideal

$$\mathfrak{a} = Ra_1 + Ra_2 + ... + Ra_n + Rb$$

pertenecerán a $\mathfrak{S}$, y contienen estrictamente a $\mathfrak{a}^*$. Esto, sin embargo, es imposible por la elección de $\mathfrak{a}^*$.

$(3) \Rightarrow (1)$: Vamos a completar la demostración del teorema al mostrar que (3) implica (1). Para esto,

supongamos que todo ideal es finitamente generado, y sea $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq ...$ una sucesión creciente de ideales.

Si denotamos por $\mathfrak{a}$ la unión de todos los ideales $\mathfrak{a}_i$, entonces $\mathfrak{a}$ es un ideal.

Sean $x_1, x_2 \in \mathfrak{a}$ y $r \in R$, entonces podemos encontrar un entero l talque x_1 y x_2 ambos están en $\mathfrak{a}_l$ entonces $x_1 + x_2$ y $x_1 - x_2$ están todos en $\mathfrak{a}_l$ y luego $rx_1 \in \mathfrak{a}_l$ porque $x_1 \in \mathfrak{a}_l$ de manera que, con mayor razón, todos están en $\mathfrak{a}$. Por lo tanto $\mathfrak{a}$ es un ideal, por hipótesis, se tiene una base finita. Sea $\mathfrak{a} = (a_1, a_2, ..., a_n)$ y para cada i elijamos m_i así que $a_i \in \mathfrak{a}_{m_i}$, entonces todos los a_i están en $\mathfrak{a}_m$, donde

$$m = max(m_1, m_2, ..., m_n)$$

Ahora si $n > m$ tenemos

$$\mathfrak{a} = (a_1, a_2, ..., a_n) \subseteq \mathfrak{a}_m \subseteq \mathfrak{a}_n \subseteq \mathfrak{a};$$

así $\mathfrak{a}_m = \mathfrak{a}_n$ única condición de que $n > m$.

Proposición 2.1.1 *Sean R un anillo noetheriano con unidad, y sea $\mathfrak{a} \neq R$, entonces existe un ideal maximal de R que contiene a $\mathfrak{a}$*

Demostración:

Sea $\mathfrak{B}$ el conjunto de todos los ideales en R, en otras palabras,

$$\mathfrak{B} = \{\mathfrak{a} / \mathfrak{a} \neq R,\ \mathfrak{a}\ es\ un\ ideal\ de\ R\}$$

donde $\mathfrak{B}$ es no vacío, puesto que $0 \in \mathfrak{a}$.

Ahora por ser R un anillo noetheriano por el teorema 2.1.1 entonces la condición de cadena ascendente y la condición maximal se mantiene en R.

Sea pues $\mathfrak{S}$ una cadena de ideales en $\mathfrak{B}$, por lo tanto $\mathfrak{S}$ es una cadena de ideales en R y veamos que $\mathfrak{a} = \bigcup_{\mathfrak{a} \in \mathfrak{S}} \mathfrak{b}$ es un ideal, efectivamente, $\mathfrak{a} \neq 0$ ya que $0 \in \mathfrak{b}$, para toda $\mathfrak{b} \in \mathfrak{B}$.

Si $x, y \in \mathfrak{a}$, entonces existen $\mathfrak{b}_1, \mathfrak{b}_2 \in \mathfrak{S}$ de modo que $x \in \mathfrak{b}_1$, $y \in \mathfrak{b}_2$, pero como $\mathfrak{S}$ cumple con la condición de cadena ascendente por ser R noetheriano, entonces $\mathfrak{b}_1 \subseteq \mathfrak{b}_2$, entonces $x, y \in \mathfrak{b}_2$ entonces $x + y \in \mathfrak{b}_2 \subseteq \mathfrak{a}$.

por lo tanto $x + y \in \mathfrak{a}$.

De manera similar probamos que $x - y \in \mathfrak{a}$.

Si $x \in \mathfrak{a}$ y para $r \in R$, existe un $\mathfrak{b}_1 \in \mathfrak{S}$ tal que $x \in \mathfrak{b}_1$, entonces $rx \in \mathfrak{b}_1 \subset \mathfrak{a}$ en consecuencia $rx \in \mathfrak{a}$.

Por tanto $\mathfrak{a} = \bigcup_{\mathfrak{a}\in\mathfrak{S}} \mathfrak{b}$ es un ideal y por ser R noetheriano entonces la condición maximal se cumple, es decir que $\mathfrak{a} \subseteq \mathfrak{b}$ y $\mathfrak{b}$ es maximal.

2.2. Descomposición Primaria en Anillos Noetherianos

Llegamos ahora a una de las propiedades fundamentales de los anillos noetherianos. Para probar este resultado, vamos a introducir un concepto auxiliar y hacer uso de los siguientes dos lemas.

Definición 2.2.1 *Vamos a decir que un ideal $\mathfrak{a} \subset R$ es irreducible, si $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$ donde $\mathfrak{b}$ y $\mathfrak{c}$ son ideales, entonces bien $\mathfrak{a} = \mathfrak{b}$ ó $\mathfrak{a} = \mathfrak{c}$.*

En otras palabras, *el ideal $\mathfrak{a}$ es irreducible si no se puede escribir como la intersección de dos ideales estrictamente mayores.*

Lema 2.2.1 *Si R es noetheriano, entonces todo ideal se puede representar como la intersección de un número finito de ideales irreducibles.*

Demostración:

Sea $\mathfrak{S}$ el conjunto de todos los ideales que no son intersecciones finitas de los ideales irreducibles. Tenemos que demostrar que $\mathfrak{S}$ es vacío.
Asumiendo lo contrario y por el Teorema 2.1.1, podemos encontrar un ideal $\mathfrak{a} \in \mathfrak{S}$ que es maximal para el conjunto $\mathfrak{S}$. Dado que $\mathfrak{a} \in \mathfrak{S}$, no es una intersección finita de ideales irreducibles, de manera que, en particular, $\mathfrak{a}$ no es irreducible. Así $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$, donde $\mathfrak{b}$ y $\mathfrak{c}$ son ideales, que contienen estrictamente a $\mathfrak{a}$. Por la condición maximal aplicado a $\mathfrak{a}, \mathfrak{b} \in \mathfrak{S}$ y $\mathfrak{c} \notin \mathfrak{S}$, tenemos que $\mathfrak{b}$ y también $\mathfrak{c}$ son intersecciones finitas de los ideales irreducibles. De esto se deduce que $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$ es también una intersección finita de ideales irreducibles; pero esto es imposible porque $\mathfrak{a} \in \mathfrak{S}$, entonces es una contración.
Por lo tanto R se puede representar como la intersección de un número finito de ideales irreducibles.

Lema 2.2.2 *Si R es Noetheriano, entonces todo ideal irreducible es primario.*

Demostración:

Vamos a suponer que $\mathfrak{a}$ es un ideal no primario en el anillo noetheriano R, y vamos a deducir que $\mathfrak{a}$ debe ser reducible.

Dado que $\mathfrak{a}$ no es primario, existen elementos b, c tal que $bc \in \mathfrak{a}$, $c \notin \mathfrak{a}$, y ningún exponente de b está en $\mathfrak{a}$.

De $bc \in \mathfrak{a}$ y $c \notin \mathfrak{a}$, se sigue que a $\mathfrak{a} \subset (\mathfrak{a} :(b))$, de que la inclusión es estricta. Usando (4.1) y (6) de la proposición 1.1.1 obtenemos

$$\begin{aligned} \mathfrak{a} :(b^r) &\subseteq ((\mathfrak{a} :(b^r)) : (b)) \\ &= (\mathfrak{a} : (b^{r+1})) \end{aligned}$$

por lo tanto

$$\mathfrak{a} \subset (\mathfrak{a} : (b)) \subseteq (\mathfrak{a} : (b^2)) \subseteq (\mathfrak{a} : (b^3)) \subseteq ...$$

Por la condición de cadena ahora demostramos que existe un entero m tal que $(\mathfrak{a} : (b^n)) = (\mathfrak{a} : (b^m))$ siempre que $n > m$.

Vamos a demostrar que

$$\mathfrak{a} = (\mathfrak{a} : (b^m)) \cap [\mathfrak{a} + (b^m)]$$

y con esto demostramos el lema. Ya que, por construcción, ambos $(\mathfrak{a} : (b^m))$ y $\mathfrak{a}+(b^m)$ están contenidos en el ideal $\mathfrak{a}$, entonces

$$((\mathfrak{a} : b^m)) \cap [\mathfrak{a} + (b^m)] \subseteq \mathfrak{a}.$$

Sea $x \in (\mathfrak{a} : (b^m)) \cap [\mathfrak{a} + (b^m)]$ entonces si demostramos que $x \in \mathfrak{a}$ hemos probamos que $\mathfrak{a} = (\mathfrak{a} : (b^m)) \cap [\mathfrak{a}+(b^m)]$. Ahora bien, como $x \in (\mathfrak{a} : (b^m)) \cap [\mathfrak{a}+(b^m)]$, entonces $x \in (\mathfrak{a} : (b^m))$ y $x \in \mathfrak{a}+(b^m)$, si $x \in \mathfrak{a} + (b^m)$ tenemos que $x = a + rb^m$, donde $a \in \mathfrak{a}$ y $r \in R$. También tenemos $x \in (\mathfrak{a} : (b^m))$ y como $x = a + rb^m$ entonces, al multiplicar la ecuación anterior a ambos lados por b^m tenemos

$$\begin{aligned} xb^m &= (a + rb^m)b^m \\ &= ab^m + b^{2m} \end{aligned}$$

en consecuencia $xb^m = ab^m + rb^{2m}$ pertenece a $\mathfrak{a}$, lo que demuestra que $rb^{2m} \in \mathfrak{a}$, y por tanto, que $r \in (\mathfrak{a} : (b^{2m}))$. Con la elección del entero m, apropiado $(\mathfrak{a} : (b^{2m})) = (\mathfrak{a} : (b^m))$, por lo tanto $r \in (\mathfrak{a} : (b^m))$ y $rb^m \in \mathfrak{a}$. Así $x = a + rb^m \in \mathfrak{a}$, que es lo que queríamos probar.

El siguiente teorema nos afirma que cada ideal diferente del ideal generado por uno en un anillo Noetheriano tiene una descomposición primaria.

Teorema 2.2.1 *En un anillo noetheriano R cada ideal tiene una descomposición primaria.*

Demostración:

Sea $\mathfrak{a}$ un ideal en R y como por hipótesis el anillo R es Noetheriano por el lema 2.2.1 tenemos

$$\begin{aligned} \mathfrak{a} &= \bigcap_{i=1}^{n} \mathfrak{a}_i \\ &= \mathfrak{a}_1 \bigcap \mathfrak{a}_2 \bigcap \ldots \bigcap \mathfrak{a}_n \end{aligned}$$

donde cada $\mathfrak{a}_i$ es irreducible.

Luego como cada $\mathfrak{a}_i$ es irreducible por el lema 2.2.2 tenemos que cada $\mathfrak{a}_i$ es primario y luego por la definición 1.6.1 el ideal $\mathfrak{a}$ tiene una descomposición primaria.

Por ser el ideal $\mathfrak{a}$ un ideal cualesquiera cada ideal tiene una descomposición primaria.

Por lo tanto cada ideal tiene una descomposición primaria en un anillo Noetheriano R.

2.3. Propiedades Adicionales de los Anillos Noetherianos

Proposición 2.3.1 *En un anillo noetheriano R, cada ideal contiene una potencia de su radical.*

Demostración:

Sea $\mathfrak{a}$ un ideal de un anillo noetheriano y sea $\mathfrak{b} = r(\mathfrak{a})$, entonces $\mathfrak{b}$ es generado finitamente, es decir, $\mathfrak{b} = Rb_1 + Rb_2 + \ldots + Rb_n$.

Luego $b_i \in r(\mathfrak{a})$, podemos encontrar un entero m_i tal que $b_i^{m_i} \in \mathfrak{a}$.

Pongamos a m como

$$m = m_1 + m_2 + \ldots + m_n$$

y vamos a demostrar que $\mathfrak{b}^m \subseteq \mathfrak{a}$.

Luego como sabemos que $\mathfrak{b}^m$ es generado por los elementos $b_1^{\mu_1} b_2^{\mu_2} \ldots b_n^{\mu_n}$, donde los μ_i son números enteros no negativos tales que

$$\mu_1 + \mu_2 + \ldots + \mu_n = m_1 + m_2 + \ldots + m_n$$

pero si $\mu_1 + \mu_2 + ... + \mu_n = m_1 + m_2 + ... + m_n$, entonces por lo menos para un valor de i se cumple que $\mu_i \geq m_i$, en consecuencia $b_1^{\mu_1} b_2^{\mu_2} ... b_n^{\mu_n} \in \mathfrak{a}$.

Entonces todos los generadores de $\mathfrak{b}^m$ están en $\mathfrak{a}$, es decir, que $\mathfrak{b}^m \subseteq \mathfrak{a}$.

Por lo tanto, el ideal $\mathfrak{a}$ contiene una potencia de su radical.

Proposición 2.3.2 *Sea R un anillo noetheriano, $\mathfrak{m}$ un ideal maximal de R, $\mathfrak{q}$ un ideal cualquiera de R, entonces las siguientes condiciones son equivalentes:*

(1) $\mathfrak{q}$ *es* $\mathfrak{m}$*-primario;*

(2) $r(\mathfrak{q}) = \mathfrak{m}$*;*

(3) $\mathfrak{m}^n \subseteq \mathfrak{q} \subseteq \mathfrak{m}$ *para algún* $n > 0$.

Demostración:

1) implica 3)

Como $\mathfrak{q}$ es $\mathfrak{m}$-primario, entonces por definición tenemos que $\mathfrak{m} = r(\mathfrak{q})$ y por la proposición 1.3.1 tenemos que $\mathfrak{m}^n \subseteq \mathfrak{q}$, para algún entero positivo $n > 0$, pero como también $\mathfrak{q} \subseteq \mathfrak{m}$ por ser $\mathfrak{m}$ un ideal maximal de R y $\mathfrak{q}$ un ideal cualquiera de R entonces tenemos

$$\mathfrak{m}^n \subseteq \mathfrak{q} \subseteq \mathfrak{m}$$

para algún $n > 0$.

3) implica 2). Partamos de $\mathfrak{m}^n \subseteq \mathfrak{q} \subseteq \mathfrak{m}$ para algún $n > 0$ y tomando radicales en la relación tenemos:

$$\begin{aligned}
\mathfrak{m}^n \subseteq \quad & \mathfrak{q} \quad \subseteq \quad \mathfrak{m} \\
r(\mathfrak{m}^n) \subseteq \quad & r(\mathfrak{q}) \quad \subseteq \quad r(\mathfrak{m}) \\
r(\underbrace{\mathfrak{m}\mathfrak{m}...\mathfrak{m}}_{n-veces}) \subseteq \quad & r(\mathfrak{q}) \quad \subseteq \quad r(\mathfrak{m}) \\
r(\bigcap_{i=1}^{n} \mathfrak{m}) \subseteq \quad & r(\mathfrak{q}) \quad \subseteq \quad r(\mathfrak{m}) \\
\bigcap_{i=1}^{n} r(\mathfrak{m}) \subseteq \quad & r(\mathfrak{q}) \quad \subseteq \quad r(\mathfrak{m}) \\
r(\mathfrak{m}) \subseteq \quad & r(\mathfrak{q}) \quad \subseteq \quad r(\mathfrak{m}).
\end{aligned}$$

Luego por la proposición 1.4.1 sabemos que $\mathfrak{m} \subseteq r(\mathfrak{m})$ y como llegamos a tener $r(\mathfrak{m}) \subseteq r(\mathfrak{q}) \subseteq r(\mathfrak{m})$, entonces tenemos que

$$\mathfrak{m} \subseteq r(\mathfrak{q}) \quad y \quad \mathfrak{m} \supseteq r(\mathfrak{q})$$

Por lo tanto $r(\mathfrak{q}) = \mathfrak{m}$.

2) implica 1).

Por definición 1.6.2 es claro que si $r(\mathfrak{q}) = \mathfrak{m}$, entonces $\mathfrak{q}$ es $\mathfrak{m}$-primario.

Corolario 2.3.1 *Si R es un anillo Noetheriano y si $\mathfrak{q}$ es $\mathfrak{p}$-primario, entonces $\mathfrak{p}^{\alpha} \subseteq \mathfrak{q}$ para algún entero positivo α.*

Desmostración:

Como $\mathfrak{q}$ es $\mathfrak{p}$-primario entonces $\mathfrak{p} = r(\mathfrak{q})$, donde

$$r(\mathfrak{q}) \;\; = \;\; \Big\{ \mathfrak{q} \in R/ \; x^n \in \mathfrak{q}; \; n > 0 \; ; n \in \mathbb{N} \Big\},$$

es decir, que $\mathfrak{q} \subseteq R$ por definición del radical de un ideal y por ser R un anillo Noetheraino entonces $\mathfrak{p}$ es generado finitamente, tal que

$$\mathfrak{p} \;\; = \;\; Rp_1 + Rp_2 + ... + Rp_n$$

Dado que $p_i \in r(\mathfrak{q})$, por ser $\mathfrak{p} = r(\mathfrak{q})$, entonces podemos encontrar un α_i tal que $\alpha_i \in \mathfrak{p}$ y pongamos a $\alpha = \alpha_1 + \alpha_2 + ... + \alpha_n$.

Ahora que sabemos que $\mathfrak{p}^{\alpha}$ es generado por los elementos

$$p_1^{\beta_1} p_2^{\beta_2} \quad ... \quad p_n^{\beta_n}$$

donde los β_i son números enteros positivos tales que

$$\beta_1 + \beta_2 + ... + \beta_n \;\; = \;\; \alpha_1 + \alpha_2 + ... + \alpha_n,$$

entonces por lo menos para un valor de i, se cumple que $\beta_i \geqslant \alpha_i$ y por lo tanto

$$p_1^{\beta_1} p_2^{\beta_2} \quad ... \quad p_n^{\beta_n} \in \mathfrak{q}$$

Entonces todos los generadores de $\mathfrak{p}^{\alpha}$ están en $\mathfrak{q}$.

Por lo tanto $\mathfrak{p}^{\alpha} \subseteq \mathfrak{q}$ para algún entero positivo α.

El corolario anterior muestra que si $\mathfrak{p}$ es un ideal primario en un anillo Noetheriano, una condición necesaria para que un ideal dado debe ser $\mathfrak{p}$-primario es que el ideal deberá contener una potencia de $\mathfrak{p}$. Hay una situación importante en la que la condición es suficiente asi como es necesaria, que es el siguiente resultado.

Proposición 2.3.3 *Sea R un anillo Noetheriano y sea $\mathfrak{p}$ un ideal maximal primo de R, entonces un ideal propio $\mathfrak{a}$ es $\mathfrak{p}$-primario si y sólo si, contiene un exponente de $\mathfrak{p}$.*

Demostración:
Supongamos que un ideal propio $\mathfrak{a}$ es $\mathfrak{p}$-primario, entonces debemos probar que $\mathfrak{p}$ contiene un exponente de $\mathfrak{a}$.
Pero como $\mathfrak{a}$ es $\mathfrak{p}$-primario y R es un anillo Noetheriano por el corolario 2.3.1, existe un exponente m tal que

$$\mathfrak{p}^m \subseteq \mathfrak{a}$$

Por lo tanto para algún exponente de $\mathfrak{a}$ está contenido en $\mathfrak{p}$.
Recíprocamente, supongamos que $\mathfrak{a}$ contiene un exponente de $\mathfrak{p}$, es decir, $\mathfrak{p}^r \subseteq \mathfrak{a}$, para algún $r > 0$ entonces, probemos que $\mathfrak{a}$ es $\mathfrak{p}$-primario.
Sea $\mathfrak{p}'$ un ideal primo tal que

$$\mathfrak{a} \subseteq \mathfrak{p}'$$

Tenemos que $\mathfrak{p}^r \subseteq \mathfrak{a} \subseteq \mathfrak{p}'$, de modo que $\mathfrak{p} \subseteq \mathfrak{p}'$ y, por tanto, ya que $\mathfrak{p}$ es maximal, entonces $\mathfrak{p} = \mathfrak{p}'$. Así $\mathfrak{p}$ es el único ideal primo que pertenece a $\mathfrak{a}$.
Como tenemos que

$$\mathfrak{p}^r \subseteq \mathfrak{a} \subseteq \mathfrak{p}$$

por la proposición 2.3.2, 3) implica 1), entonces tenemos que $\mathfrak{a}$ es $\mathfrak{p}$-primario.
Por lo tanto un ideal propio $\mathfrak{a}$ es $\mathfrak{p}$-primario si y sólo si, contiene un exponente de $\mathfrak{p}$.

2.4. Teorema de la Base de Hilbert

Si R es un anillo dado, podemos considerar expresiones formales de la clase $a_0 + a_1x + a_2x^2 + ... + a_nx^n$, donde los a_i son elementos de R, y donde x es un símbolo, que se conoce como una variable.

Una expresión como $a_0 + a_1x + a_2x^2 + ... + a_nx^n$ es llamado un polinomio en la variable x.
El coeficiente de x^i en este polinomio es a_i, si $i \geq n$ y cero si $i > n$. Dos polinomios

$$a_0 + a_1x + a_2x^2 + ... + a_nx^n \text{ y } b_0 + b_1x + a_2x^2 + ... + b_px^p$$

se consideran iguales, si y sólo si, los coeficientes de x^i es el mismo en ambos polinomios para todos los valores de i. La suma y la multiplicación de polinomios se definen ahora en la forma natural, y esto convierte el conjunto de todos los polinomios en x (con coeficientes en R) en un anillo, que es costumbre denotar por $R[x]$. El elemento cero de este nuevo anillo es llamado la nula polinómica, que tiene todos sus coeficientes igual a cero. Los polinomios constantes, en la que nos referimos a los polinomios que tienen el coeficiente de x^i igual a cero para todos los $i \geq 1$, forman por sí mismos un anillo. Para cada elemento $a \in R$ le corresponde un polinomio constante que es única $a + 0x + 0x^2 + ...$, y esta correspondencia muestra que el anillo de polinomios constante es sólo una copia del anillo R. Por lo tanto podemos identificar a R con el anillo de polinomios constantes, y decir que $R[x]$ contiene R. El elemento unitario de $R[x]$ es la constante de un polinomio 1, o de acuerdo con nuestras identificaciones, es simplemente el elemento unidad de R. Por el coeficiente principal de $f(x) = a_0+a_1x+a_2x^2+...+a_nx^n$ nos referimos al último coeficiente distinto de cero, y por el grado de $f(x)$ nos referimos al mayor valor de i para el cual el coeficiente de x^i que no es cero. El grado de $f(x)$ se denota por $\partial^0 f(x)$, o por $\partial^0 f$. Hasta ahora, sólo hemos hablado de polinomios en una variable. También podemos considerar polinomios en n variables $x_1, x_2, ..., x_n$ con coeficientes en R, en cuyo caso se obtiene el anillo que se denota por $R[x_1, x_2, ..., x_n]$.

Teorema 2.4.1 *(Teorema de la Base de Hilbert). Si R es un anillo noetheriano, entonces el anillo de polinomios $R[x]$ es noetheriano.*

Demostración:

Vamos a suponer que $\mathfrak{U}$ es un ideal de $R[x]$ y además supongamos que $\mathfrak{U}$ es generado finitamente. Los elementos de $\mathfrak{U}$ son polinomios. Formemos un conjunto $\mathfrak{a}$, de elementos de R, tomando el coeficiente principal de todos los polinomios en $\mathfrak{U}$ junto con el elemento cero. Ahora probemos que $\mathfrak{a}$ es un ideal de R. Supongamos que $\alpha_1, \alpha_2 \in \mathfrak{a}$, entonces existen polinomios $\alpha_1x^m + ...$ y $\alpha_2x^n + ...$ que están en $\mathfrak{U}$. Y sea $p = m + n$, multipliquemos el primer polinomio por x^n y el secundo polinomio por x^m, de este modo, obtenemos dos polinomios los cuales son

$$\alpha_1x^p + ... \quad y \quad \alpha_1x^p + ...$$

ambos están en $\mathfrak{U}$ y cuando sumamos tenemos

$$(\alpha_1 x^p + ...) + (\alpha_2 x^p + ...) \;\; = \;\; (\alpha_1 + \alpha_2)x^p + ... \in \mathfrak{U}$$

y cuando hacemos la resta tenemos

$$(\alpha_1 x^p + ...) - (\alpha_2 x^p + ...) \;\; = \;\; (\alpha_1 - \alpha_2)x^p + ... \in \mathfrak{U}$$

entonces $\alpha_1 + \alpha_2 \in \mathfrak{a}$ y $\alpha_1 - \alpha_2 \in \mathfrak{a}$.
Además, si $r \in R$, entonces

$$r(\alpha_1 x^p + ...) \;\; = \;\; (r\alpha_1)x^p + ... \in \mathfrak{U}$$

y por lo tanto $r\alpha_1 \in \mathfrak{a}$. Así $\mathfrak{a}$ es un ideal.
Como R es Noetheriano, $\mathfrak{a}$ es generado finitamente, es decir, $\mathfrak{a} = (\alpha_1, \alpha_2, ..., \alpha_h)$, de modo que existen polinomios $f_1 = f_1(x), f_2 = f_2(x), ..., f_h = f_h(x)$ tal que $f_i \in \mathfrak{U}$ tiene coeficiente principal α_i. Multiplicando cada uno de los $f_i(x)$ por un exponente adecuado de x, podemos arreglar que todos tengan el mismo grado, es decir, de grado N, para obtener

$$f_i \in \mathfrak{U}; \;\; f_i(x) = \alpha_i x^N + ... \quad (1 \leq i \leq h).$$

Consideremos todos los polinomios en $\mathfrak{U}$ cuyos grados no exceden de $N - 1$. Los coeficientes de x^{N-1} en estos polinomios forman un ideal $\mathfrak{b}$ de R, es decir, $\mathfrak{b} = (\beta_1, \beta_2, ..., \beta_k)$ y podemos elegir los polinomios $g_1 = g_1(x), g_2 = g_2(x), ..., g_k = g_k(x)$ tal que

$$g_i \in \mathfrak{U}; \;\; g_i(x) = \beta_i x^{N-1} + ... \;\; (1 \leq i \leq k).$$

De la misma forma, si consideramos los polinomios en $\mathfrak{U}$ cuyos grados no exceden de $N - 2$, entonces los coeficientes de x^{N-2} en estos polinomios forman un ideal $\mathfrak{c} = (\gamma_1, \gamma_2, ..., \gamma_l)$. También existen polinomios $h_1(x), h_2(x), ..., h_l(x)$ tal que

$$h_i \in \mathfrak{U}; \;\; h_i(x) = \gamma_i x^{N-2} + ... \;\; (1 \leq i \leq l).$$

Mediante este método, eventualmente obtenemos cierto conjunto finito $f_1, ..., f_h, g_1, ..., g_k, h_1, ..., h_l, ...$ de polinomios. Estos polinomios están todos en $\mathfrak{U}$. Vamos a demostrar que estos polinomios generan $\mathfrak{U}$. Supongamos que $\phi(x) = \alpha x^P + ...$ pertenece a $\mathfrak{U}$, entonces $\alpha \in \mathfrak{a}$, es decir,

$$\alpha = \omega_1\alpha_1 + \omega_2\alpha_2 + ... + \omega_h\alpha_h,$$

donde $\omega_i \in R$.

Si $P > N$, entonces

$$\phi - \omega_1 x^{P-N} f_1 - \omega_2 x^{P-N} f_2 - ... - \omega_h x^{P-N} f_h$$

está de nuevo en $\mathfrak{U}$, pero tiene un grado menor que ϕ. Si el grado del polinomio nuevo sigue siendo no menos de N, se puede reducir aún más por el mismo mecanismo. De esta manera tenemos que existen polinomios $A_1(x), A_2(x), ..., A_h(x)$, tal que

$$\phi(x) = A_1(x)f_1(x) + A_2(x)f_2(x) + ... + A_h(x)f_h(x) + \psi(x),$$

donde $\psi(x) \in \mathfrak{U}$, y el grado de este polinomio es $\partial^0\psi \leq N - 1$. Vamos a completar la prueba, demostrando que:

$$\psi(x) = \mu_1(x)g_1(x) + \mu_2(x)g_2(x) + ... + \mu_k(x)g_k(x) + \nu_1 h_1(x) + ... + \nu_l h_l(x) + ...,$$

donde $\mu_1, ..., \mu_k, \nu_1, ..., \nu_l, ...$ están todos en R. Para probarlo, primero elijamos $\mu_1, \mu_2, ..., \mu_k$ de modo que $\psi(x)$ y $\mu_1(x)g_1(x) + \mu_2(x)g_2(x) + ... + \mu_k(x)g_k(x)$ tienen el mismo coeficiente de x^{N-1}. Esto es posible, ya que $\psi(x) \in \mathfrak{U}$ y que $\partial^0\psi \leq N - 1$, por definición de los $g_i(x)$. Luego Elijamos $\nu_1, \nu_2, ..., \nu_l$ de modo que el coeficiente de x^{N-2} es la misma en

$$\psi(x) - \mu_1 g_1(x) - \mu_2 g_2(x) - ... - \mu_k g_k(x)$$

como es en

$$v_1 h_1(x) + v_2 h_2(x) + ... + v_l h_l(x).$$

por lo tanto $\psi(x) = \mu_1(x)g_1(x) + \mu_2(x)g_2(x) + ... + \mu_k(x)g_k(x) + \nu_1 h_1(x) + ... + \nu_l h_l(x) + ...$, y como

$$\phi \;\; = \;\; A_1(x)f_1(x) + A_2(x)f_2(x) + ... + A_h(x)f_h(x) + \psi(x)$$

donde $\psi(x) = \mu_1(x)g_1(x) + \mu_2(x)g_2(x) + ... + \mu_k(x)g_k(x) + \nu_1 h_1(x) + ... + \nu_l h_l(x) + ...$, y como lo hemos escrito como una combinación lineal de los polinomios $f_1, ..., f_h$, $g_1, ..., g_k$, $h_1, ..., h_l, ...$ por definición 1.1.8 de un ideal generado por un conjunto entonces estos polinomios generan finitamente a $\mathfrak{U}$.

Y por definición de anillo noetheriano entonces $R[x]$ es noetheriano.
Si $P \leq N$, entonces obtenemos un polinomio $\phi - \omega_1 f_1 - \omega_2 f_2 - ... - \omega_h f_h$ de grado menor que P, que está de nuevo en $\mathfrak{U}$, con lo que se concluye igualmente, pero si el grado del polinomio nuevo sigue siendo no menos de N, se puede reducir aún más por el mismo método.
Y por lo tanto $R[x]$ es noetheriano.

Ejemplo 2.4.1 *El anillo $\mathbb{Z}[x]$, es un anillo Noetheriano.*

Solución:
Como $\mathbb{Z}$ es noetheriano, entonces es una consecuencia inmediata del teorema de la base de Hilbert.

Corolario 2.4.1 *Si R es un anillo noetheriano, entonces el anillo de polinomios $R[x_1, x_2, ..., x_n]$ también es noetheriano.*

Demostración:
Supongamos que $R_0 = R$, y que $R_i = R[x_1, x_2, ..., x_i]$ para $1 \leq i \leq n$.
Puesto que cada polinomio en $x_1, x_2, ..., x_{i+1}$ puede considerarse, precisamente de una manera, como un polinomio en x_{i+1} cuyos coeficientes son polinomios en $x_1, x_2, ..., x_i$, en el anillo R_{i+1} que no es otro que el anillo de polinomios $R_i[x_{i+1}]$.
En consecuencia, por el teorema anterior, Teorema de la Base de Hilbert, R_{i+1} es noetheriano siempre R_i es northeriano. Por hipótesis, como $R_0 = R$, entonces R_0 es noetheriano, consecuentemente todos los R_i son noetherianos, en particular, esto es cierto para $R_n = R[x_1, x_2, ..., x_n]$, es decir, que R_n es noetheriano.
Por lo tanto $R[x_1, x_2, ..., x_n]$ es noetheriano.

2.5. Homomorfirmos e Isomorfismos

Definición 2.5.1 *Si una asignación σ de un anillo R sobre un anillo R' es talque $\sigma(a+b) = \sigma(a) + \sigma(b)$ y que $\sigma(ab) = \sigma(a)\sigma(b)$ para todo par de elementos a, b de R, entonces decimos que "σ es un homomorfismo de R sobre R'".*

Supongamos que σ mapea a R homomórficamente sobre R', entonces, puesto que $a + (-a) = 0$ y que $\sigma(0)$ es el elemento cero de R', entonces deducimos que $\sigma(-a) = -\sigma(a)$.

Podemos, por supuesto, tener un homomorfismo σ de un anillo R sobre un anillo $R^{'}$. Debemos notar que, aunque $\sigma(0)$ debe ser el elemento cero de $R^{'}$, y puede suceder que $\sigma(1)$ no es el elemento unidad de $R^{'}$.

Definición 2.5.2 *Si σ es un homomorfismo de R sobre $R^{'}$ es tal que σ establece una correspondencia uno a uno entre los elementos de R y los de $R^{'}$, entonces decimos que σ mapea a R isomórficamente sobre $R^{'}$ y decimos también que R y $R^{'}$ son isomorfos y lo denotaremos $R \cong R^{'}$.*

Si σ es un isomorfismo de R sobre $R^{'}$, entonces también la asignación inversa, σ^{-1}, se asignará $R^{'}$ isomórficamente sobre R. Dos anillos que son isomorfos son copias fieles el uno del otro, y, en consecuencia, tienen las mismas propiedades algebraicas.

Definición 2.5.3 *Sea $\mathfrak{a}$ un ideal propio de el anillo R, y supongamos que x_1 y x_2 dos elementos de R. Si $x_1 - x_2 \in \mathfrak{a}$, es decir, que x_2 es congruente con x_1 módulo $\mathfrak{a}$ y lo escribimos de la siguiente menera*

$$x_1 \equiv x_2(mod\ \mathfrak{a})\ \acute{o}\ x_1 \equiv x_2(\mathfrak{a})$$

Esta relación entre los elementos es reflexiva, simétrica y transitiva.

Vamos a decir que es $reflexiva$ cuando cumple que $x \equiv x(mod\ \mathfrak{a})$ para todo $x \in R$, Vamos a entender por *simétrica* cuando se cumpla que $x \equiv y(mod\ \mathfrak{a})$ entonces $y \equiv x(mod\ \mathfrak{a})$ para todo $x, y \in R$ y por $transitividad$ cuando $x \equiv y(mod\ \mathfrak{a})$ y $y \equiv z(mod\ \mathfrak{a})$ entonces tenemos que $x \equiv z(mod\ \mathfrak{a})$ para todo $x, y, z \in R$.

Vamos a recoger los elementos de R en las clases de elementos mutuamente congruentes, de modo que dos elementos de la misma clase serán congruentes entre sí, pero si primero tenemos un elemento de una clase y después tomamos un elemento de una clase diferente, estos dos elementos no serán congruentes. Las clases de elementos se conocen como *las clases de residuos de* $\mathfrak{a}$. Puesto que estamos suponiendo que $\mathfrak{a}$ es un ideal propio, entonces 1 y 0 no puede estar en la clase de un mismo residuo, por lo tanto, existen al menos dos clases de residuos. El siguiente lema, hace a un anillo de las clases de residuos.

Lema 2.5.1 *Sean $x_1 \equiv x_2(mod\ \mathfrak{a})$ y si $y_1 \equiv y_2(mod\ \mathfrak{a})$, entonces tenemos que $x_1 + y_1 \equiv x_2 + y_2(mod\ \mathfrak{a})$, $x_1 - y_1 \equiv x_2 - y_2(mod\ \mathfrak{a})$ y que $x_1 y_1 \equiv x_2 y_2(mod\ \mathfrak{a})$*

Demostración:

Como tenemos que $x_1 \equiv x_2 (mod\ \mathfrak{a})$ y si $y_1 \equiv y_2 (mod\ \mathfrak{a})$ entonces tenemos que $x_1 - x_2 \in \mathfrak{a}$ y que $y_1 - y_2 \in \mathfrak{a}$. Vamos ha demostrar que $(x_1+y_1)-(x_2+y_2) \in \mathfrak{a}$. Entonces partiendo de $(x_1+y_1)-(x_2+y_2)$ y agrupando de manera conveniente tenemos:

$$\begin{aligned} (x_1 + y_1) - (x_2 + y_2) &= x_1 + y_1 - x_2 - y_2 \\ &= (x_1 - x_2) + (y_1 - y_2) \end{aligned}$$

Ahora ocupando la hipótesis $x_1 - x_2 \in \mathfrak{a}$ y que $y_1 - y_2 \in \mathfrak{a}$ entonces tenemos que

$$(x_1 + y_1) - (x_2 + y_2) \quad \in \quad \mathfrak{a}$$

Luego probemos que $(x_1 - y_1) - (x_2 - y_2) \in \mathfrak{a}$.
Haciendo un proceso similar al anterior tenemos:

$$\begin{aligned} (x_1 - y_1) - (x_2 - y_2) &= (x_1 - y_1) - x_2 + y_2 \\ &= (x_1 - x_2) - (y_1 - y_2). \end{aligned}$$

Como tenemos por hipótesis $x_1 - x_2 \in \mathfrak{a}$ y que $y_1 - y_2 \in \mathfrak{a}$, entonces tenemos que

$$(x_1 - y_1) - (x_2 - y_2) \in \mathfrak{a}.$$

Para probar que $x_1y_1 \equiv x_2y_2 (mod\ \mathfrak{a})$ tenemos que probar que

$$x_1y_1 - x_2y_2 \quad \in \quad \mathfrak{a} \tag{2.1}$$

Entonces a la ecuación 1.9 sumemos y restemos al mismo tiempo el termino x_2y_1 y agrupamos de manera conveniente para poder aplicar la hipótesis entonces tenemos

$$\begin{aligned} (x_1y_1) - (x_2y_2) &= x_1y_1 - x_2y_2 - x_2y_1 + x_2y_1 \\ &= (x_1 - x_2)y_1 + x_2(y_1 - y_2). \end{aligned}$$

Pero como $x_1 - x_2 \in \mathfrak{a}$ y $y_1 - y_2 \in \mathfrak{a}$ entonces $(x_1 - x_2)y_1$ y $x_2(y_1 - y_2)$ están todos en $\mathfrak{a}$.
Por lo tanto $(x_1 + y_1) - (x_2 + y_2), (x_1 - y_1) - (x_2 - y_2)$ y $(x_1y_1) - (x_2y_2)$ están todos en $\mathfrak{a}$.
Y esto es lo que queríamos demostrar.

Proposición 2.5.1 *El mapeo que asigna a cada elemento en su clase de residuos módulo* $\mathfrak{a}$*, es un homomorfismo.*

Demostración:

Sea σ una asignación de R sobre $R/\mathfrak{a}$ tal que tomamos un elemento x y me lleva a la clases de residuo $x + \mathfrak{a}$, es decir, $\sigma(a) = x + \mathfrak{a}$.
Probemos que σ es un homomorfismo. Sean x y y elementos de R entonces

$$\sigma(x) = x + \mathfrak{a} \ \ y \ \ \sigma(y) = y + \mathfrak{a}.$$

Tenemos que demostrar que $\sigma(x + y) = \sigma(x) + \sigma(y)$ y partamos de $\sigma(x + y) = (x + y) + \mathfrak{a} \in R/\mathfrak{a}$ y aplicando la suma de clases de residuos tenemos

$$\begin{aligned} \sigma(x + y) &= (x + y) + \mathfrak{a} \\ &= (x + \mathfrak{a}) + (y + \mathfrak{a}) \\ &= \sigma(x) + \sigma(y). \end{aligned}$$

Por lo tanto tenemos

$$\sigma(x + y) = \sigma(x) + \sigma(y).$$

Ahora probemos que se cumple para el producto, es decir, que $\sigma(xy) = \sigma(x)\sigma(y)$.

$$\begin{aligned} \sigma(xy) &= (xy) + \mathfrak{a} \\ &= (x + \mathfrak{a})(y + \mathfrak{a}) \\ &= \sigma(x)\sigma(y). \end{aligned}$$

Por lo tanto tenemos que $\sigma(xy) = \sigma(x)\sigma(y)$.
Por consiguiente σ es un homomorfismo, y lo llamaremos el homomorfismo natural de R sobre $R/\mathfrak{a}$.

Proposición 2.5.2 *Una imagen de cocientes de un anillo noetheriano es de nuevo noetheriano.*

Demostración: Sea σ un homomorfismo de un anillo Noetheriano R sobre un anillo $R^{'}$, y sea $\mathfrak{a}^{'}$ un ideal del anillo $R^{'}$.
Además pongamos que $\mathfrak{a} = \sigma^{-1}(\mathfrak{a}^{'})$, entonces $\mathfrak{a}$ es un ideal de R y por lo tanto es finitamente generado, es decir,

$$\mathfrak{a} = (a_1, a_2, ..., a_n).$$

Al aplicarle el homomorfismo al ideal $\mathfrak{a}$ que es generado finitamente tenemos

$$\sigma(\mathfrak{a}) \quad = \quad (\sigma(a_1), \sigma(a_2), \sigma(a_3), ..., \sigma(a_n))$$

Entonces $\sigma(a_1), \sigma(a_2), \sigma(a_3), ..., \sigma(a_n)$ generará a $\sigma(\mathfrak{a}) = \mathfrak{a}^{'}$, entonces $\mathfrak{a}^{'}$ es generado finitamente.
Por lo tanto $\sigma(\mathfrak{a})$ es Noetheriano.

Capítulo 3

Variedades Algebraicas Afines

3.1. Ideales y Variedades

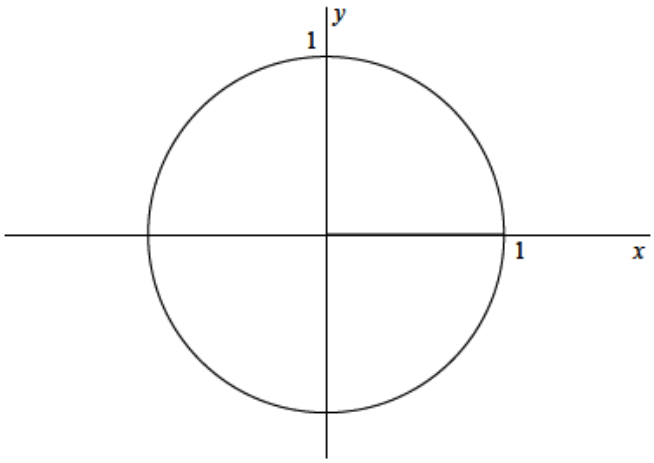
Trabajamos con k un cuerpo algebraicamente cerrado y $k[x] = k[x_1, x_2, ..., x_n]$ el anillo Noetheriano de polinomios en n variables con coeficientes en k.

Definición 3.1.1 *Denotamos k^n al espacio afín n-dimensional sobre k, es decir, al conjunto de $x = (x_1, x_2, ..., x_n)$ con $x_i \in k$, con la estructura de espacio afín.*
Sea $X \subset k[x]$. Definimos

$$U = V(X) = \Big\{ x \in k^n / \ f(x) = 0; \ para\ todo\ f \in X \Big\}$$

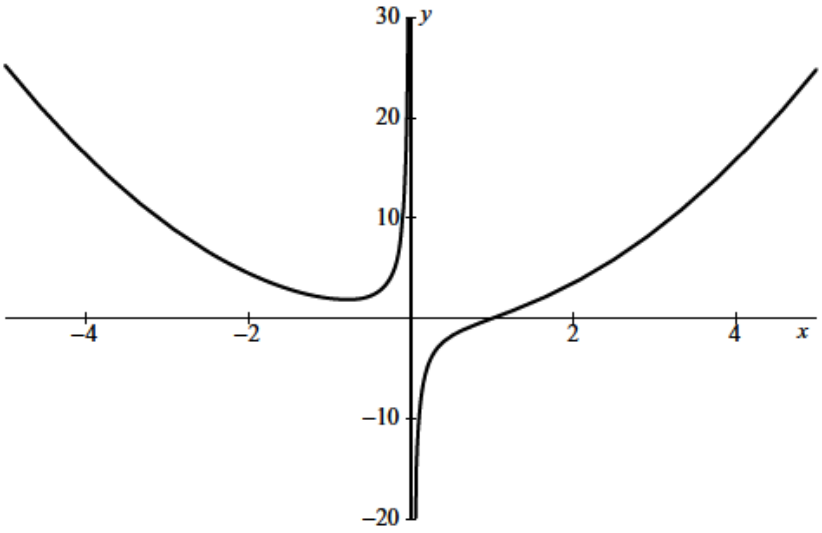
llamaremos a U la variedad algebraica afín definida por X.
En general, decimos que un conjunto de puntos $U \subset k^n$ es una variedad algebraica afín, si existe $X \subset k[x]$ tal que $U = V(X)$.

En otras palabras una variedad algebraica afín $V(X) \subset k^n$ es el conjunto de todas las soluciones del sistemas de ecuaciones $f_1(x_1, x_2, ..., x_n) = f_2(x_1, x_2, ..., x_n) = ... = f_n(x_1, x_2, ..., x_n) = 0$, con $f_1, f_2, ..., f_n \in X$.
Ejemplo, tomando $k = \mathbb{R}$ y $n = 2$, entonces $k^n = \mathbb{R}^2$ se tiene que la variedad $V(x^2 + y^2 - 1)$ no es más que el circulo unitario.



Las secciones cónicas estudiadas en geometría análitica (circulo, elipses, hipérbolas y parábolas) definen variedades afines. Al igual que el gráfico de las funciones polinómicas son variedades afines. Así el gráfico de $y = f(x)$ es $V(y - f(x))$.

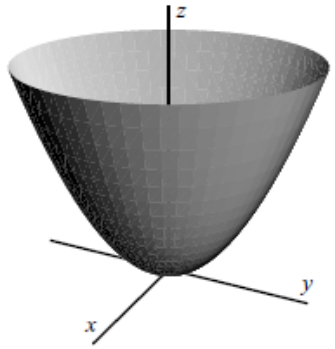
Aunque no siempre es obvio, el gráfico de una función racional también define una varieda algebraica afín. Por ejemplo, considere el gráfico de $y = \frac{x^3-1}{x}$.



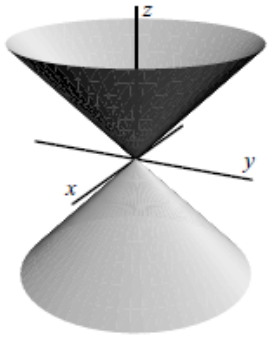
Es fácil ver que esta ecuación define la variedad algebraica afín $V(xy - x^3 + 1)$.

A continuación en el espacio real tridimensional $\mathbb{R}^3$, una variedad algebraica afín puede ser la dada por el paraboloide de revolucón $V(z - x^2 - y^2)$, el cual se obtiene de rotar la parábola $z = x^2$ alrededor

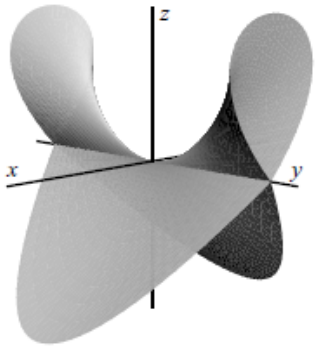
del eje z.



El cono $V(z^2 - x^2 - y^2)$:

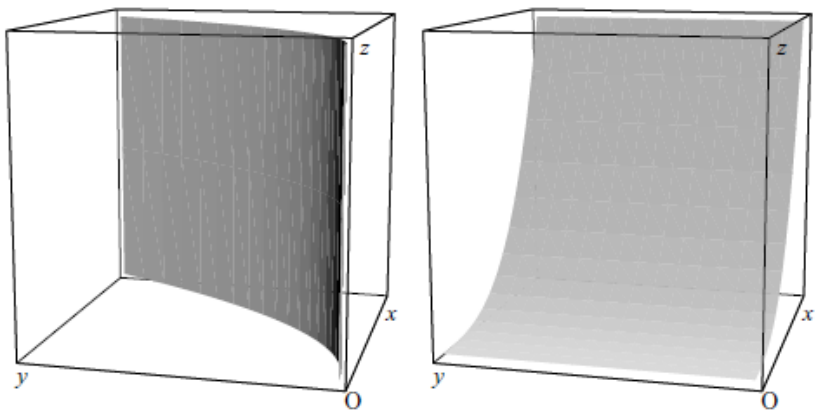


Mucho más complicada es la superficie dada por $V(x^2 - y^2z^2 + z^3)$:



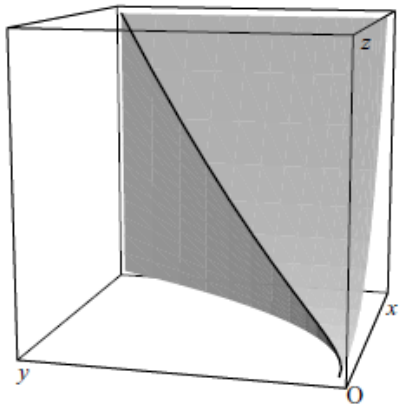
En estos dos últimos ejemplos, las superficies no son uniformes en todas partes: el cono tiene un punto fuerte en el origen, y el último ejemplo se cruza a lo largo de todo el eje. Estos son ejemplos de puntos singulares.

Un ejemplo interesante de una curva en $\mathbb{R}^3$ es el "cubo retorcido", el cual se define por la variedad $V(y - x^2, z - x^3)$. Para simplificar, nos limitaremos a la parte que se encuentra en el primer octante. Y observamos las superficies $y = x^2$ y $z = x^3$ por separado:



$y = x^2$ $\qquad$ $z = x^3$

Entonces su intersección da el cubo retorcido:



A continuación algunos ejemplos de variedades de mayor dimensión. Un concepto familiar se obtiene del álgebra lineal. Supongamos k es un cuerpo, y consideremos un sistema de m ecuaciones lineales en n incógnitas $x_1, ..., x_n$ con coeficientes en k:

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n &= b_1 \\ &\vdots \\ a_{1m}x_1 + \cdots + a_{mn}x_n &= b_m \end{aligned} \qquad (1)$$

Las soluciones de estas ecuaciones forman una variedad algebraica afín en k^n, que recibe el nombre de variedad lineal. Así, las líneas y los planos son variedades lineales, pero también se pueden considerar ejemplos de dimensiones arbitrariamente grandes. Las variedades lineales se relacionan muy bien con nuestra discusión de la dimensión. Es decir, si $V \subset k^n$ es la variedad lineal definida por (1), entonces V no necesita tener dimensión $n - m$, a pesar de que V se define por las m ecuaciones. De hecho, cuando V es no vacío, el álgebra lineal nos dice que V tiene dimensión $n - r$, donde r es el rango de la matriz (a_{ij}). Así que para las variedades lineales, la dimensión se determina por el número de ecuaciones independientes.

Algunos ejemplos complicados en dimensiones más altas provienen de cálculo. Supongamos, por ejemplo, que queremos encontrar los valores mínimo y máximo de $f(x, y, z) = x^3 + 2xyz - z^2$ sujeta a la restricción $g(x, y, z) = x^2 + y^2 + z^2 = 1$. El método de los multiplicadores de Lagrange establece que $\nabla f = \lambda \nabla g$ es un mínimo o máximo local [recordar que el gradiente de f es el vector de derivadas

parciales $\nabla f = (Fx, Fy, Fz)$]. Esto da el siguiente sistema de cuatro ecuaciones con cuatro incógnitas, x, y, z, λ, a resolver:

$$\begin{aligned} 3x^2 + 2yz &= 2x\lambda \\ 2xz &= 2y\lambda \qquad (2) \\ 2xy - 2z &= 2z\lambda \\ x^2 + y^2 + z^2 &= 1 \end{aligned}$$

Estas ecuaciones definen una variedad afín en $\mathbb{R}^4$.

Hay que mencionar también que las variedades afines puede ser el conjunto vacío. Por ejemplo, cuando $k = \mathbb{R}$, es obvio que $V(x^2 + y^2 + 1) = \emptyset$ ya que $x^2 + y^2 = -1$ no tiene soluciones reales (aunque hay soluciones cuando $k = \mathbb{C}$).
Otro ejemplo es $V(xy, xy - 1)$, que es vacío, sin importar que campo sea k, para un x e y dados no se puede satisfacer tanto $xy = 0$ y $xy = 1$.

Para estudiar los conjuntos de polinomios que definen a una variedad, usamos la estructura de ideal.

Definición 3.1.2 *Decimos que un subconjunto $\mathfrak{a} \subset k[x]$ es un ideal si cumple las siguientes condiciones:*

1. $0 \in \mathfrak{a}$
2. *Si $f, g \in \mathfrak{a}$, entonces $f \pm g \in \mathfrak{a}$.*
3. *Si $f \in \mathfrak{a}$ y $g \in k[x]$, entonces $gf \in \mathfrak{a}$*

El objetivo aquí es introducir al lector en algunos ejemplos de ideales de origen natural, para ver cómo los ideales se relacionan con las variedades afines. De hecho esa es la verdadera importancia de los ideales en este trabajo.
El primer ejemplo natural de un ideal es el ideal generado por un número finito de polinomios.

Definición 3.1.3 *Sea $X \subset k[x]$. Definimos el ideal generado por X como*

$$\mathfrak{a} = (f_\lambda / \ f_\lambda \in X) = \left\{ \textstyle\sum_{f_\lambda \in X} h_\lambda f_\lambda / \ h_\lambda \in k[x] \right\}$$

donde cada suma contiene una cantidad finita de términos.

Este ideal tiene una excelente interpretación en términos de ecuaciones polinómicas. Para X, se tiene el sistema de ecuaciones:

$$\begin{aligned} f_1 &= 0 \\ &\vdots \\ f_\lambda &= 0 \end{aligned}$$

Luego podemos ver que si multiplicamos la primera ecuación por $h_1 \in k[x]$, la segunda por $h_2 \in k[x]$, etc. Así al sumarlas se tiene

$$h_1 f_1 + h_2 f_2 + \cdots + h_\lambda f_\lambda = 0$$

que es una combinación de nuestro sistema original. Observe que el lado izquierdo de la esta ecuación es exactamente un elemento del ideal $\mathfrak{a}$. Por lo tanto, podemos expresar al ideal $\mathfrak{a}$ como el conjunto de todos los polinomios que son combinación de las ecuaciones $f_1 = f_2 = \cdots = f_\lambda = 0$.

Para ver lo que esto significa en la práctica, considere el ejemplo de representación paramétrica

$$\begin{aligned} x &= 1 + t \\ y &= 1 + t^2 \end{aligned}$$

Eliminando t se obtiene

$$y = x^2 - 2x + 2$$

Empezamos por escribir las ecuaciones como

$$\begin{aligned} x - 1 - t &= 0 \qquad (3) \\ y - 1 - t^2 &= 0 \end{aligned}$$

Para cancelar el parámetro t, multiplicamos la primera ecuación por $x - 1 + t$ y la segunda por -1:

$$\begin{aligned} (x-1)^2 - t &= 0 \\ -y + 1 + t^2 &= 0 \end{aligned}$$

Al sumar obtenemos

$$(x-1)^2 - y + 1 = x^2 - 2x + 2 - y = 0$$

En términos del ideal generado por las ecuaciones (3), podemos escribir esto como

$$\begin{aligned} x^2 - 2x + 2 - y &= (x - 1 + t)(x - 1 - t) + (-1)(y - 1 - t^2) \\ &\in \left\langle x - 1 - t, y - 1 - t^2 \right\rangle \end{aligned}$$

De manera similar, cualquier otra combinación del sistema (3) conduce a un elemento de este ideal.

Decimos que un ideal es finitamente generado si existen $f_1, ..., f_\lambda \in k[x]$ de tal manera que $\mathfrak{a} = \langle f_1, ..., f_\lambda \rangle$, y decimos que $\langle f_1, ..., f_\lambda \rangle$, son la base de la $\mathfrak{a}$, incluso podemos mencionar el hecho asombroso de que todos los ideales de $k[x]$ son finitamente generados (esto se conoce como el Teorema de la base de Hilbert). Se debe de tener en cuenta que un ideal dado puede tener muchas bases diferentes. Se puede demostrar que se puede elegir un tipo de base especialmente útil, llamada base de Groebner. Que no se tratará ese tema en este trabajo y le dejamos esa inquietud al lector.

Aquí podemos establecer una bonita analogía con el álgebra lineal. La definición de un ideal es similar a la definición de un sub-espacio: ambos tienen que ser cerrados bajo la adición y multiplicación, con la diferencia que, para un sub-espacio, se multiplica por escalares, mientras que para un ideal, se multiplica por polinomios. Además, observe que el ideal generado por los polinomios $f_1, \ldots, f_\lambda$ es similar al sub-espacio generado por un número finito de vectores $v_1, \ldots, v_\lambda$. En cada caso, se tiene combinaciones lineales, utilizando los respectivos coeficientes del campo, escalares y polinomios.

Otro papel que desempeñado por los ideales es la siguiente proposición, que demuestra que una variedad depende sólo del ideal generado y no por las ecuaciones que lo definen.

Proposición 3.1.1 *Si $f_1, \ldots, f_\lambda$ y $g_1, \ldots, g_\mu$ son bases del mismo ideal en $k[x]$, de modo que $\langle f_1, \ldots, f_\lambda \rangle$ = $\langle g_1, \ldots, g_\mu \rangle$, entonces tenemos que $V(f_1, \ldots, f_\lambda) = V(g_1, \ldots, g_\mu)$.*

Demostración:
Sea $x \in V(f_1, \ldots, f_\lambda)$ entonces $f_i(x) = 0$ para todo $1 \leq i \leq \lambda$, es decir, $f_1(x) = f_2(x) = \ldots = f_\lambda(x) = 0$
Luego si $f_1(x) = 0$, le multiplicamos por $h_1(x) \in k[x]$, tenemos $h_1(x)f_1(x) = 0$
Así sucesivamente, si $f_2(x) = 0$, le multiplicamos por $h_2(x) \in k[x]$, tenemos $h_2(x)f_2(x) = 0$

$\vdots$

Hasta llegar a $f_\lambda(x) = 0$, le multiplicamos por $h_\lambda(x) \in k[x]$, tenemos $h_\lambda(x)f_\lambda(x) = 0$.
Al sumarlas tenemos $h_1(x)f_1(x) + h_2(x)f_2(x) + \cdots + h_\lambda(x)f_\lambda(x) = 0$, llegamos a expresarlo como el conjunto de todos los polinomios que son combinaciónes lienales, es decir, que es generado por $\langle f_1, \ldots, f_\lambda \rangle$, pero por hipótesis $\langle f_1, \ldots, f_\lambda \rangle$ = $\langle g_1, \ldots, g_\mu \rangle$ entonces $t(x) = \sum_{i=1}^{\lambda} h_i(x)f_i(x) = 0 = \sum_{i=1}^{\mu} q_i(x)g_i(x)$ donde $h_i, q_i \in k[x]$, entonces $x \in V(g_1, \ldots, g_\mu)$
La otra inclusión es análoga.

Como ejemplo, considere la variedad $V(2x^2 + 3y^2 - 11, x^2 - y^2 - 3)$. Es fácil demostrar que $\langle 2x^2 + 3y^2 - 11, x^2 - y^2 - 3 \rangle = \langle x^2 - 4, y^2 - 1 \rangle$, por lo que

$$V(2x^2 + 3y^2 - 11, x^2 - y^2 - 3) = V(x^2 - 4, y^2 - 1) = (\pm 2, \pm 1)$$

por la proposición anterior.
Así, al cambiar la base del ideal, se hizo más fácil determinar la variedad.

La capacidad de cambiar la base, sin afectar la variedad es muy importante. Esto da lugar a la observación de que las variedades afines son determinadas por los ideales, no por ecuaciones. Y este hecho es fundamental para poder comprender la correspondencia entre los ideales y las variedades.

Ahora definimos la variedad asociada a un ideal:

Definición 3.1.4 *Sea* $\mathfrak{a} \subset k[x]$ *un ideal, definimos la variedad del ideal* $\mathfrak{a}$ *como*

$$V(\mathfrak{a}) = \Big\{ x \in k^n / \ f(x) = 0, \ para\ todo\ f \in \mathfrak{a} \Big\}$$

El Teorema de la base de Hilbert nos asegura que $V(\mathfrak{a})$ es en realidad una variedad afín, ya que nos dice que existe un conjunto finito de polinomios $f_1, \ldots f_\lambda \in \mathfrak{a}$ tales que $\mathfrak{a} = \langle f_1, \ldots f_\lambda \rangle$, además $\mathfrak{a}$ es el conjunto de las raíces comunes de estos polinomios. Por lo tanto, tenemos un mapeo:

$$\begin{array}{ccc} \mathfrak{a} & \longrightarrow & V(\mathfrak{a}) \\ \text{ideales} & & \text{variedades afines} \end{array}$$

De lo cual ya mencionamos antes que existe esa correspondencia entre ideales y variedades afines. Sin embargo es de notar que no es una correspondencia uno a uno, ya que diferentes ideales pueden dar la misma variedad. Por ejemplo, $\langle x \rangle$ y $\langle x^2 \rangle$ son dos ideales diferentes en $k[x]$ pero tienen la misma variedad $V(x) = V(x^2) = \{0\}$. De hecho, los problemas más graves pueden ocurrir si el cuerpo k no

es algebraicamente cerrado. De esto se ve la necesida de que k sea algebraicamente cerrado.

Consideremos el siguiente lema.

Lema 3.1.1 *Sean* $\mathfrak{a}$, $\mathfrak{b}$ *ideales en* $k[x]$ *tales que* $\mathfrak{a} \subset \mathfrak{b}$ *entonces* $V(\mathfrak{a}) \supset V(\mathfrak{b})$.

Demostración: Sea $x \in V(\mathfrak{b})$, por definición de una variedad para un ideal tenemos que $f(x) = 0$ para todo $f \in \mathfrak{b}$.
Como $\mathfrak{a} \subset \mathfrak{b}$, $g(x) = 0$ para todo $g \in \mathfrak{a}$ y en consecuencia $x \in V(\mathfrak{a})$.
Por tanto $V(\mathfrak{a}) \supset V(\mathfrak{b})$.

Tenemos la siguiente proposición.

Proposición 3.1.2 *Sea* $X \subset k[x]$ *y sea* $\mathfrak{a} = (f_\lambda / f_\lambda \in X)$, *entonces* $V(\mathfrak{a}) = V(X)$.

Demostración:

Sea $x \in V(\mathfrak{a})$, entonces $f(x) = 0$, para todo $f \in \mathfrak{a}$. Por hipótesis $\mathfrak{a} = (f_\lambda / f_\lambda \in X)$, entonces $f(x) = 0$, para todo $f \in X$ y por definición de variedad afín tenemos que $x \in V(X)$. Por lo tanto $V(\mathfrak{a}) \subseteq V(X)$.

Sea $y \in V(X)$, entonces $f(y) = 0$, para todo $f \in X$, entonces y es un cero común de todos los polinomios de X (que también lo es de cualquier elemento que sea una combinación lineal de X con coeficientes en $k[x]$), entonces tenemos que para toda $f \in \mathfrak{a}$,

$$f(y) \quad = \quad \sum_{f_\lambda \in X} h_\lambda f_\lambda(y) = 0.$$

donde $h_\lambda \in k[x]$, entonces $y \in V(\mathfrak{a})$, y por lo tanto $V(X) \subseteq V(\mathfrak{a})$.
Por tanto $V(\mathfrak{a}) = V(X)$.

Proposición 3.1.3 *Sean* $\mathfrak{a} = (f_1, f_2, ..., f_n)$ *y* $\mathfrak{b} = (g_1, g_2, ..., g_n)$ *ideales en* $k[x]$. *Entonces*

i) $V(\mathfrak{a} + \mathfrak{b}) = V(\mathfrak{a}) \cap V(\mathfrak{b})$,

ii) $V(\mathfrak{a}\mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$,

iii) $V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{a}\mathfrak{b})$.

Demostración:

i) Sea $x \in V(\mathfrak{a}+\mathfrak{b})$, entonces por definición de variedad afín para todo $h \in \mathfrak{a}+\mathfrak{b}$, $h(x) = 0$ pero como $h \in \mathfrak{a}+\mathfrak{b}$ por definición de suma de ideales tenemos que $h = f_i + g_j$ donde $f_i \in \mathfrak{a}$ y $g_j \in \mathfrak{b}$, pero como $h(x) = 0$ entonces $f_i(x) + g_j(x) = 0$ para toda $f_i \in \mathfrak{a}$ y toda $g_j \in \mathfrak{b}$ entonces $f_1(x) = f_2(x) = ... = f_n(x) = g_1(x) = g_2(x) = ... = g_m(x) = 0$ para todo $f_i \in \mathfrak{a}$ y $g_j \in \mathfrak{b}$. En consecuencia, $x \in V(\mathfrak{a})$ y $x \in V(\mathfrak{b})$, por la definición de la variedad de un ideal, y por lo tanto $V(\mathfrak{a}+\mathfrak{b}) \subseteq V(\mathfrak{a}) \cap V(\mathfrak{b})$.

Recíprocamente, sea $x \in V(\mathfrak{a}) \cap V(\mathfrak{b})$, entonces $x \in V(\mathfrak{a})$ y $x \in V(\mathfrak{b})$ por definición de una variedad afín para toda $f \in \mathfrak{a}$ y toda $g \in \mathfrak{b}$, $f(x) = 0$ y $g(x) = 0$ entonces para toda $h = f + g \in \mathfrak{a}+\mathfrak{b}$,

$h(x) = f(x) + g(x) = 0$ entonces $h(x) = 0$ y por lo tanto $x \in V(\mathfrak{a}+\mathfrak{b})$, entonces

$V(\mathfrak{a}) \cap V(\mathfrak{b}) \subseteq V(\mathfrak{a}+\mathfrak{b})$

Entonces $V(\mathfrak{a}+\mathfrak{b}) = V(\mathfrak{a}) \cap V(\mathfrak{b})$.

ii) Sea $x \in [V(\mathfrak{a}) \cup V(\mathfrak{b})]$, entonces $x \in V(\mathfrak{a})$ ó $x \in V(\mathfrak{b})$, es decir, que $f(x) = 0$ para todo $f \in \mathfrak{a}$ ó $g(x) = 0$ para todo $g \in \mathfrak{b}$. Podemos suponer que $x \in V(\mathfrak{a})$, entonces $f(x) = 0$ para todo $f \in \mathfrak{a}$, y para todo polinomio en $\mathfrak{b}$ tenemos

$$\begin{aligned} f(x)g(x) &= 0 \\ (fg)(x) &= 0 \end{aligned}$$

por que $f(x) = 0$ para todo $f \in \mathfrak{a}$.

Como tenemos que $(fg)(x) = 0$ para todo $f \in \mathfrak{a}$ y $g \in \mathfrak{b}$ entonces $x \in V(\mathfrak{ab})$.

Por tanto $V(\mathfrak{a}) \cup V(\mathfrak{b}) \subseteq V(\mathfrak{ab})$.

Recíprocamente supongamos que $x \in V(\mathfrak{ab})$ y que $x \notin [V(\mathfrak{a}) \cup V(\mathfrak{b})]$, entonces existe un $f \in \mathfrak{a}$ tal que $f(x) \neq 0$ y un $g \in \mathfrak{b}$ tal que $g(x) \neq 0$, entonces tenemos

$$\begin{aligned} f(x)g(x) &\neq 0 \\ (fg)(x) &\neq 0 \end{aligned}$$

y por lo tanto $x \notin V(\mathfrak{ab})$ teniendo una contración ya que $x \in V(\mathfrak{ab})$.

En consecuencia $V(\mathfrak{ab}) \subseteq V(\mathfrak{a}) \cup V(\mathfrak{b})$ y por tanto, $V(\mathfrak{ab}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$.

iii) Vamos a demostrar que $V(\mathfrak{a} \cap \mathfrak{b}) \subseteq V(\mathfrak{a}) \cup V(\mathfrak{b}) \subseteq V(\mathfrak{ab}) \subseteq V(\mathfrak{a} \cap \mathfrak{b})$.

Primero probemos que $V(\mathfrak{a} \cap \mathfrak{b}) \subseteq V(\mathfrak{a}) \cup V(\mathfrak{b})$, veamos la prueba por el contrarrecíproco, sea $x \notin [V(\mathfrak{a}) \cup V(\mathfrak{b})]$, entonces existe un $f \in \mathfrak{a}$ tal que $f(x) \neq 0$ y un $g \in \mathfrak{b}$ tal que $g(x) \neq 0$.

Luego formemos el polinomio fg que está en $\mathfrak{a}$ y en $\mathfrak{b}$, por lo que $fg \in \mathfrak{a} \cap \mathfrak{b}$ entonces tenemos

$$\begin{aligned} f(x)g(x) &\neq 0 \\ \underbrace{(fg)(x)}_{=h} &\neq 0 \\ h(x) &\neq 0. \end{aligned}$$

para toda $h \in \mathfrak{a} \cap \mathfrak{b}$, $x \notin V(\mathfrak{a} \cap \mathfrak{b})$. Por tanto $V(\mathfrak{a} \cap \mathfrak{b}) \subseteq V(\mathfrak{a}) \cup V(\mathfrak{b})$.
Sabemos por ii) de la misma proposición que $V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{ab})$, entonces $V(\mathfrak{a}) \cup V(\mathfrak{b}) \subseteq V(\mathfrak{ab})$.
Finalmente supongamos que $x \in V(\mathfrak{ab})$ y que $x \notin V(\mathfrak{a} \cap \mathfrak{b})$, entonces existe $f \in \mathfrak{a} \cap \mathfrak{b}$ tal que $f(x) \neq 0$.
Pero por la proposición 1.1.1, 3.1) tenemos que $\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b}$ entonces también existe $f \in \mathfrak{ab}$ tal que $f(x) \neq 0$ y por lo tanto $x \notin V(\mathfrak{ab})$, lo cual es una contradicción ya que $x \in V(\mathfrak{ab})$.
Por tanto $V(\mathfrak{ab}) \subseteq V(\mathfrak{a} \cap \mathfrak{b})$.

3.2. El Ideal de una Variedad

Vamos a analizar los ideales que se obtienen a partir de variedades.

Definición 3.2.1 *Sea $X \subset k^n$ una variedad afín y consideremos el conjunto de todos los polinomios $g \in k[x] = k[x_1, x_2, ..., x_n]$ y definamos el conjunto $\mathfrak{a}(X)$ como*

$$\mathfrak{a}(X) = \Big\{ g \in k[x] / g(x) = 0 \ para \ todo \ x \in X \Big\}$$

Este conjunto es un ideal $\mathfrak{a}(X)$ en el anillo de polinomios y lo llamaremos el ideal de la variedad X.

Lema 3.2.1 *Para cualquier variedad $X \subset k^n$, se cumple que $V(\mathfrak{a}(X)) = X$.*

Demostración:
Si $x \in X$, todos los polinomios de $\mathfrak{a}(X)$ se anulan en x, y por lo tanto $x \in V(\mathfrak{a}(X))$, es decir que $X \subseteq V(\mathfrak{a}(X))$.
Para la otra inclusión, tomemos funciones polinómicas $g_1, g_2, ..., g_n$ tales que

$$X = V(g_1, g_2, ..., g_n) = \Big\{ x \in k^n / \ g_i(x) = 0 \ para \ todo \ 1 \leq i \leq s \Big\}.$$

Entonces $g_1, g_2, ..., g_n \in \mathfrak{a}(X)$.
Sea $x \in V(\mathfrak{a}(X))$, entonces se cumple que $g_1(x) = g_2(x) = ... = g_s(x) = 0$.

En consecuencia, $x \in X$ y entonces $V(\mathfrak{a}(X)) \subseteq X$.

Por lo tanto $V(\mathfrak{a}(X)) = X$.

Lema 3.2.2 *Sean $X,\ Y$ variedades en k^n tales que $X \subset Y$. Entonces*

$$\mathfrak{a}(X) \ \supset \ \mathfrak{a}(Y).$$

Demostración:

Sea $f \in \mathfrak{a}(Y)$, entonces $f(x) = 0$ para todo $x \in Y$.

Pero como $X \subset Y$, $f(x) = 0$ para todo $x \in X$ y en consecuencia $f \in \mathfrak{a}(X)$.

Por lo tanto $\mathfrak{a}(Y) \subset \mathfrak{a}(X)$.

Proposición 3.2.1 *Sea $V_1 \supset V_2 \supset V_3 \supset ...$, una cadena descendente de variedades en k^n. Entonces existe un $N \geq 1$ tal que*

$$V_N = V_{N+1} = V_{N+2} = ...$$

Demostración:

Partamos de la cadena descendente de variedades

$$V_1 \supset V_2 \supset V_3 \supset ...$$

Tomando los ideales que generan esas variedades por el lema 3.2.2 obtenemos

$$\mathfrak{a}(V_1) \subset \mathfrak{a}(V_2) \subset \mathfrak{a}(V_3) \subset ...$$

Por la condición de cadenas ascendentes de ideales está cadena es estacionaria, es decir, existe un N tal que

$$\mathfrak{a}(V_N) = \mathfrak{a}(V_{N+1}) = ...$$

para algún $N \in \mathbb{N}$.

Tomando ahora las variedades de estos ideales, tenemos

$$V(\mathfrak{a}(V_N)) = V(\mathfrak{a}(V_{N+1})) = ...$$

pero por el lema 3.2.1 tenemos que $V(\mathfrak{a}(V_N)) = V_N$. Por lo tanto existe un $N \geq 1$ tal que

$$V_N = V_{N+1} = V_{N+2} = ...$$

Proposición 3.2.2 *Sea* $(\mathfrak{a}_\alpha)_{\alpha\in R}$ *una familia cualesquiera de ideales que están en el anillo* $R \subseteq k[x]$ *entonces:*

1) *Si* $V_\alpha = V(\mathfrak{a}(V_\alpha))$ *para todo* $\alpha \in R$ *entonces* $\bigcap_{\alpha\in R} V\alpha = V(\bigcup_{\alpha\in R} \mathfrak{a}(V_\alpha))$.

2) *Si* $V_j = V(\mathfrak{a}(V_j))$, *para todo* $j = 1, 2, ..., r$ *entonces* $\bigcup_{j=1}^{r} V_j = V(\prod_{i=1}^{r} \mathfrak{a}(V_j))$.

3) $V(0) = k^n$ *y* $V(1) = \emptyset$.

4) $V(\mathfrak{a}) = V(r(\mathfrak{a}))$.

Demostración:

1)($\subseteq$) Sea $x \in \bigcap_{\alpha\in R} V\alpha$ y sea $f \in \bigcup_{\alpha\in R} \mathfrak{a}(V_\alpha)$, debemos probar que $f(x) = 0$.

Como $f \in \bigcup_{\alpha\in R} \mathfrak{a}(V_\alpha)$, entonces existe un $\alpha_i \in R$ tal que $f \in \mathfrak{a}(V_{\alpha_i})$. Además, como $x \in \bigcap_{\alpha\in R} V_\alpha$, entonces $x \in V_{\alpha_i}$ para todo $\alpha_i \in R$. Luego por el lema 3.2.1 tenemos que $V_{\alpha_i} = V(\mathfrak{a}(V_{\alpha_i}))$, entonces $x \in V(\mathfrak{a}(V_{\alpha_i}))$, por lo que $f(x) = 0$, entonces $x \in V(\bigcup_{\alpha\in R} \mathfrak{a}(V_\alpha))$

Por tanto $\bigcap_{\alpha\in R} V\alpha \subseteq V(\bigcup_{\alpha\in R} \mathfrak{a}(V_\alpha))$.

($\supseteq$) Sea $x \in V(\bigcup_{\alpha\in R} \mathfrak{a}(V_\alpha))$ entonces para todo $f \in \bigcup_{\alpha\in R} \mathfrak{a}(V_\alpha)$, tememos que $f(x) = 0$, ahora como para todo α, $\mathfrak{a}(V_\alpha) \subset \bigcup_{\alpha\in R} \mathfrak{a}(V_\alpha)$, tenemos que $f(x) = 0$ para todo $f \in \mathfrak{a}(V_\alpha)$ y en consecuencia $x \in V(\mathfrak{a}(V_\alpha))$ para todo $\alpha \in R$.

Así $x \in \bigcap_{\alpha\in R} V(\mathfrak{a}(V_\alpha))$. De nuevo por el lema 3.2.1 $x \in \bigcap_{\alpha\in R} V\alpha$. Por tanto $\bigcap_{\alpha\in R} V\alpha \supseteq V(\bigcup_{\alpha\in R} \mathfrak{a}(V_\alpha))$.

2)($\subseteq$) Sea $x \in \bigcup_{j=1}^{r} V_j$ entonces existe un $j \in 1, 2, ..., r$ tal que $x \in V_j$, pero por el lema 3.2.1 tenemos que $V_j = V(\mathfrak{a}(V_j))$, $x \in V(\mathfrak{a}(V_j))$, entonces para todo $f_j \in \mathfrak{a}(V_j)$, $f_j(x) = 0$ y en consecuencia el producto de polinomios

$$f_1(x)f_2(x)...f_r(x) = 0$$

porque para $f_j \in \mathfrak{a}(V_j)$.

Por lo tanto, $x \in V(\prod_{i=1}^{r} \mathfrak{a}(V_j))$.

($\supseteq$) Hagamos la prueba por el contrarrecíproco.

Supongamos que $x \notin \bigcup_{j=1}^{r} V_j$, por el lema 3.2.1 para todo $V(\mathfrak{a}(V_j)) = V_j$, entonces $x \notin \bigcup_{j=1}^{r} V(\mathfrak{a}(V_j))$ entonces $x \notin V(\mathfrak{a}(V_j))$, entonces:

- Para $V(\mathfrak{a}(V_1))$, entonces existe un $f_1 \in \mathfrak{a}(V_1)$ tal que $f_1(x) \neq 0$;
- Para $V(\mathfrak{a}(V_2))$, entonces existe un $f_2 \in \mathfrak{a}(V_2)$ tal que $f_2(x) \neq 0$;

y así sucesivamente hasta r, es decir, que

- Para $V(\mathfrak{a}(V_r))$, existe un $f_r \in \mathfrak{a}(V_r)$ tal que $f_r(x) \neq 0$.

Luego si consideramos el producto

$$f_1(x)f_2(x)...f_r(x)$$

tenemos que este polinomio es no nulo, con lo que $x \notin V(\prod_{j=1}^{r} \mathfrak{a}(V_j))$ ya que $\mathfrak{a}(V_i) = \{\prod_{j=1}^{r} f_j / f_j \in \mathfrak{a}(V_i), j \in 1, 2, ..., r\}$. Por lo tanto $\bigcup_{j=1}^{r} V_j \supseteq V(\prod_{i=1}^{r} \mathfrak{a}(V_j))$

3)($\subseteq$) Sea $x \in V(0)$, entonces por definición de una variedad $x \in k^n$. Por lo que $V(0) \subseteq k^n$

($\supseteq$) Sea $x \in k^n$, por definición de polinomio nulo, tenemos que $0(x) = 0$.

Entonces, $x \in V(0)$ y por tanto, $k^n \subseteq V(0)$.

Finalmente, veamos que $V(1) = \emptyset$.

$V(1) = \left\{ x \in k^n / \ f(x) = 0; \ para \ todo \ f \in 1 \right\}$

Como $1(x) = 1$ para todo $x \in k^n$ (ya que el polonomio constante e igual a 1 no se anula nunca), entonces $V(1) = \emptyset$.

4) Sea $x \in V(\mathfrak{a})$ entonces por definición 3.1.4 $f(x) = 0$ para toda $f \in \mathfrak{a}$, sabemos que $\mathfrak{a} \subseteq r(\mathfrak{a})$, entonces $f \in r(\mathfrak{a})$, y por definición 3.1.4, $x \in V(r(\mathfrak{a}))$

Como consecuencia $V(\mathfrak{a}) \subseteq V(r(\mathfrak{a}))$.

Sea $y \in V(r(\mathfrak{a}))$ entonces $f(y) = 0$ para toda $f \in r(\mathfrak{a})$, es decir, que existe un $n > 0$ tal que $f^n \in \mathfrak{a}$. Luego en particular para $n = 1$ tenemos que $f \in \mathfrak{a}$, por ende $f(y) = 0$ para toda $f \in \mathfrak{a}$, por definición 3.1.4 tenemos $V(r(\mathfrak{a})) \subseteq V(\mathfrak{a})$

Por tanto $V(\mathfrak{a}) = V(r(\mathfrak{a}))$.

Como consecuencia de está proposición, existe una topología definida sobre k^n, llamada Topología de Zarisky, en la que los conjuntos cerrados y las variedades coinciden.

3.3. El Anillo Coordenado de las Variedades

Definición 3.3.1 *El anillo cociente*

$$P(X) = k[x_1, x_2, ..., x_n]/\mathfrak{a}(X)$$

es el anillo de funciones polinómicas en X, puesto que dos polinomios g, h definen la misma función polinomio en X, si y sólo si $g - h$ se anula en cada punto de X.

Proposición 3.3.1 *Dados dos polinomios h y g definen la misma función polinomio en X, si y sólo si $g - h \in \mathfrak{a}(X)$, en otras palabras si $g - h$ se anula en cada punto de X.*

Demostración:

Sean h y g dos polinomios que definen la misma función polinomio en X, entonces $g(x) = h(x)$, para toda $x \in X$ entonces tenemos

$$\begin{aligned} g(x) &= h(x) \\ g(x) - h(x) &= 0 \\ (g-h)(x) &= 0 \end{aligned}$$

para toda $x \in X$ entonces $g - h \in k[x]$. Por definición de ideal de una variedad X, $g - h \in \mathfrak{a}(X)$.

Ahora sea $g - h \in \mathfrak{a}(X)$ entonces $(g - h)(x) = 0$, para toda $x \in X$, es decir que

$$\begin{aligned} (g-h)(x) &= 0 \\ g(x) - h(x) &= 0 \\ g(x) &= h(x) \end{aligned}$$

para todo $x \in X$. Por lo tanto h y g dos polinomios que definen la misma función polinomio en X.

Sea ξ_i la imagen de x_i en $P(X)$. Y las $\xi_i (1 \leq i \leq n)$ son las las funciones coordenadas en X.

Definición 3.3.2 *El anillo cociente $P(X)$ es generado como una k-álgebra por las funciones coordenadas y se denomina el anillo coordenado de X.*

3.4. Descomposición de Variedades

Retomemos la idea de descomponer variedades.

Definición 3.4.1 *Una variedad algebraica afín $V \subseteq k^n$, es irreducible si dadas V_1 y V_2 variedades afines tales que $V = V_1 \cup V_2$ entonces $V = V_1$ ó $V = V_2$*

Proposición 3.4.1 *Sea $V \subseteq k^n$ una variedad algebraica afín, entonces V se puede escribir como una unión finita*

$$V = V_1 \cup V_2 \cup ... \cup V_t,$$

donde cada V_i es una variedad irreducible.

Demostración:
Supongamos que existe una variedad V que no puede escribir como unión de variedades irreducibles, en particular, V no es irreducible y se puede escribir como

$$V \;=\; V_1 \cup V_1^{'},\;\; con\;\; V_1 \neq V \;\; y \;\; V_1^{'} \neq V.$$

Si podemos descomponer a V_1 y $V_1^{'}$ como unión de irreducibles, obtenemos una descomposición de V en variedades irreducibles, por lo tanto, podemos suponer que V_1 no es unión de irreducibles, es decir,

$$V_1 \;=\; V_2 \cup V_2^{'},\;\; con\;\; V_2 \neq V_1 \;\; y \;\; V_2^{'} \neq V_1.$$

Por el mismo argumento podemos suponer que V_2 no es unión de irreducibles, es decir,

$$V_2 \;=\; V_3 \cup V_3^{'},\;\; con\;\; V_3 \neq V_2 \;\; y \;\; V_3^{'} \neq V_2.$$

Continuando este proceso, obtenemos una sucesión infinita de variedades

$$V \supsetneq V_1 \supsetneq V_2 \supsetneq V_3 \supsetneq ...$$

Como las inclusiones son estrictas, esto contradice la proposición 3.2.1 .
Por tanto $V = V_1 \cup V_2 \cup ... \cup V_t$.

Lema 3.4.1 *Sea $\mathfrak{a} \subset k[x]$ un ideal y sean f, g polinomios que pertenecen a $k[x]$, entonces*

$$V(\mathfrak{a}, f) \cup V(\mathfrak{a}, g) = V(\mathfrak{a}, fg)$$

.

Demostración:
Sea $x \in V(\mathfrak{a}, f) \cup V(\mathfrak{a}, g)$, entonces $x \in V(\mathfrak{a}, f)$ ó $x \in V(\mathfrak{a}, g)$. Podemos suponer que $x \in V(\mathfrak{a}, f)$, por lo tanto f se anula en x y los polinomios del ideal $\mathfrak{a}$ también se anulan en x, por definición de una variedad, además supongamos que g es un ideal de $\mathfrak{a}$, entonces $g(x) = 0$, es decir, que

$$\begin{aligned} f(x)g(x) &= 0 \\ (fg)(x) &= 0 \end{aligned}$$

y como $(fg)(x) = 0$, obtenemos que $x \in V(\mathfrak{a}, fg)$

Recíprocamente, sea $x \in V(\mathfrak{a}, fg)$, entonces $(fg)(x) = 0$, pero como

$$(fg)(x) = f(x)g(x) = 0$$

en consecuencia $f(x) = 0$ ó $g(x) = 0$.

Suponiendo que $f(x) = 0$, obtenemos que $x \in V(\mathfrak{a}, f)$.

Y suponiendo que $g(x) = 0$, obtenemos que $x \in V(\mathfrak{a}, g)$.

Por lo tanto, $x \in V(\mathfrak{a}, f) \cup V(\mathfrak{a}, g)$.

El concepto de ideal primo es el análogo algebraico de variedades irreducibles. La relación está dada por la proposición siguiente.

Proposición 3.4.2 *Sea $V \subset k[x]$ una variedad algebraica afín, entonces V es irreducible si y solo si $\mathfrak{a}(V)$ es un ideal primo.*

Demostración:

("⇒") Supongamos que $\mathfrak{a}(V)$ no es primo, entonces existen f y g en $k[x]$ tales que $fg \in \mathfrak{a}(V)$, pero $f \notin \mathfrak{a}(V)$ y $g \notin \mathfrak{a}(V)$, es decir, que existen puntos x y y en V tales que $f(x) \neq 0$ y $g(y) \neq 0$.

Por el lema 3.4.1, se tiene que

$$V(\mathfrak{a}(V), fg) \;=\; V(\mathfrak{a}(V), f) \cup V(\mathfrak{a}(V), g)$$

pero por ser $f(x) \neq 0$ y $g(y) \neq 0$, tenemos que $V(\mathfrak{a}(V), f) \neq V$ y $V(\mathfrak{a}(V), g) \neq V$, es decir, que V no es igual a ninguna de las dos variedades, entonces V no es irreducible.

Por lo tanto $\mathfrak{a}(V)$ es primo.

("⇐") Para la otra implicación supongamos que V no es irreducible, entonces $V = V_1 \cup V_2$, con $V_1 \neq V$ y $V_2 \neq V$, es decir, que $V_1 \subset V$ y $V_2 \subset V$.

Por el lema 3.2.2 podemos elegir un $f \in \mathfrak{a}(V_1)$, tal que $f \notin \mathfrak{a}(V)$ y $g \in \mathfrak{a}(V_2)$, tal que $g \notin \mathfrak{a}(V)$.

Demostremos que $fg \in \mathfrak{a}(V)$.

Sea $x \in V$, pero como V no es irreducible,$V = V_1 \cup V_2$, es decir, para toda $x \in V_1$ o $x \in V_2$, $f(x) = 0$ o $g(x) = 0$ pues $f \in \mathfrak{a}(V_1)$ y $g \in \mathfrak{a}(V_2)$.

Consideramos fg vemos que fg se anula en los puntos de V, porque f se anula en los puntos de V_1 y g se anula en los puntos de V_2, es decir,

$$(fg)(x) \;=\; 0 \;\; para \;\; toda \;\; x \in V$$

por lo tanto $fg \in \mathfrak{a}(V)$.

En consecuencia, existen $f, g \notin \mathfrak{a}(V)$, pero tales que $fg \in \mathfrak{a}(V)$, por definición de un ideal primo, $\mathfrak{a}(V)$ no es un ideal primo.

Por tanto V es irreducible.

Capítulo 4

EL teorema de los ceros de Hilbert

4.1. Lema de Normalización de Noether

Definición 4.1.1 *Sea R un anillo, $R^{'}$ un sudanillo de R tal que $1 \in R^{'}$. Un elemento x de R se dice que es un entero sobre $R^{'}$ si x esa una raíz de un polinomio mónico con coeficientes en $R^{'}$, es decir, si x satisface una ecuación de la forma*

$$x^n + a_1 x^{n-1} + ... + a_n \quad = \quad 0$$

donde las a_i son elementos de $R^{'}$.

Es evidente que cada elemento de $R^{'}$ es entero sobre $R^{'}$

Definición 4.1.2 *Sea k un subgrupo de R. Diremos que el elemento $a \in R$ es algebraico sobre k, si existe un polinomio no constante f en $k[x]$ tal que $f(x) = 0$.*

Lema 4.1.1 (Lema de Normalización de Noether) *Sea k un cuerpo y sea $R \neq 0$ una k-álgebra con generación finita . Entonces existen elementos $y, y_1, y_2, ..., y_r \in R$ que son algebraicamente independientes sobre k y tales que R es un entero sobre $k[y, y_1, ..., y_r]$.*

Demostracción:
Supongamos que k es infinito.
Sean $x_1, x_2, ..., x_n$ generadores de R como R-álgebra, es decir, existen finitos elementos $x_1, x_2, ..., x_n$ que generan a R.

Luego tomemos $x_1, x_2, ..., x_r$un subconjunto de $x_1, x_2, ..., x_n$ algebraicamente independiente sobre k y cada una de las $x_{r+1}, x_{r+2}, ..., x_n$ sean algebraicas sobre $k[x_1, x_2, ..., x_r]$.

Procedamos ahora por inducción respecto a n.

Si $n = r$ no hay nada que probar, pues tomando $y_i = x_i$ para toda i donde los x_i generan a R y si $a \in R$, entonces existe un $f \in k[x_1, x_2, ..., x_n]$ tal que $f(x_1, x_2, ..., x_n) = a$ entonces $a \in k[x_1, x_2, ..., x_n]$ y donde $x - a$ es un polinomio mónico con coeficientes en $k[x_1, x_2, ..., x_n]$ en donde a es una raíz y por lo tanto R es un entero sobre $k[y_1, y_2, ..., y_r]$.

Si $n > r$ y suponiendo que el resultado es cierto para $n - 1$ generadores, probaremos para n generadores.

Supongamos que $n > 1$, ya que si $n = 1$, $R = k[x_1]$, $r = 0$, y tomando $y_1, y_2, ..., y_r = \emptyset$.

Como $x_1, x_2, ..., x_n$ son generadores de R como R-álgebra resulta que $x_1, x_2, ..., x_n$ son algebraicamente independientes sobre k, en otras palabras el generador x_n es algebraico sobre $k[x_1, x_2, ..., x_{n-1}]$[1], por lo tanto existe un polinomio $f \neq 0$, en n variables tal que

$$f(x_1, x_2, ..., x_{n-1}, x_n) = 0.$$

Sea F la parte homogénea de mayor grado en f, digamos que el grado es d, $\partial^0 F = d$, puesto que k es infinito, existen elementos $\lambda_1, \lambda_2, ..., \lambda_{n-1} \in k$ con coeficientes en el anillo de polinomios $k[\lambda_1, \lambda_2, ..., \lambda_{n-1}]$ tales que $F[\lambda_1, \lambda_2, ..., \lambda_{n-1}, 1] \neq 0$.

Definamos $x_i^{'} = x_i - \lambda_i x_n$, donde $i = 1, 2, ..., n-1$ y probemos que x_n es un entero sobre $R^{'}[x_i^{'}, ..., x_{n-1}^{'}]$.

Como $x_i^{'} = x_i - \lambda_i x_n$, para toda $i = 1, 2, ..., n-1$ entonces tenemos

$$\begin{aligned} x_1 &= x_1^{'} - \lambda_1 x_n \\ x_2 &= x_2^{'} - \lambda_2 x_n \\ &\vdots \\ x_{n-1} &= x_{n-1}^{'} - \lambda_{n-1} x_n \end{aligned}$$

y sustituyendo cada x_i en $f(x_1, x_2, ..., x_{n-1}) = 0$ tenemos

$$f(x_1^{'} - \lambda_1 x_n, x_2^{'} - \lambda_2 x_n, ..., x_{n-1}^{'} - \lambda_{n-1} x_n) = 0 \tag{4.1}$$

$$F(\lambda_1, \lambda_2, ..., \lambda_{n-1}, 1) x_n^d + \underbrace{H(x_1^{'}\lambda_1, x_2^{'}\lambda_2, ..., x_{n-1}^{'}\lambda_{n-1}, 1) x_n^{d-i}}_{\partial^0 H < \partial^0 F} = 0 \tag{4.2}$$

[1] Recordemos que si x_n es algebraico sobre $k[x_1, x_2, ..., x_{n-1}]$, entonces existe un polinomio f no nulo tal que $f(x_1, x_2, ..., x_n) = 0$

En otras palabras H es un polinomio de grado menor que F.

Siendo $F[\lambda_1, \lambda_2, ..., \lambda_{n-1}, 1] \neq 0$, podemos dividir el polinomio (4.2) entre $F(\lambda_1, \lambda_2, ..., \lambda_{n-1}, 1)$ y obtenemos un polinomio mónico

$$\frac{F(\lambda_1, \lambda_2, ..., \lambda_{n-1}, 1)x_n^d}{F(\lambda_1, \lambda_2, ..., \lambda_{n-1}, 1)} + \frac{H(x_1^{'}\lambda_1, x_2^{'}\lambda_2, ..., x_{n-1}^{'}\lambda_{n-1}, 1)x_n^{d-i}}{F(\lambda_1, \lambda_2, ..., \lambda_{n-1}, 1)} = 0 \quad (4.3)$$

$$x_n^d + \frac{H(x_1^{'}\lambda_1, x_2^{'}\lambda_2, ..., x_{n-1}^{'}\lambda_{n-1}, 1)x_n^{d-i}}{F(\lambda_1, \lambda_2, ..., \lambda_{n-1}, 1)} = 0 \quad (4.4)$$

Por definición 4.1.1 x_n es raíz del polinomio mónico (4.4) con coeficientes en $R^{'}[x_i^{'}, ..., x_{n-1}^{'}]$ y por en consecuencia R es un entero sobre $R^{'}$.

Por hipótesis inductiva, existen $y_1, y_2, ..., y_r$ algebraicamente independiente sobre k tal que $R^{'}$ es un entero sobre $k[y_1, y_2, ..., y_r]$. Pero como los x_i, (con $i < n$) son enteros sobre $R^{'}$ pues $x_i = x_i^{'} + \lambda_i x_n$ entonces $x_1, x_2, ..., x_r$ son un entero sobre $k[y_1, y_2, ..., y_r]$.

Por lo tanto R es un entero sobre $k[y_1, y_2, ..., y_r]$.

4.2. Teorema de los ceros de Hilbert en su forma débil

Proposición 4.2.1 *Sea k un campo algebraicamente cerrado y sean $a_1, a_2, ..., a_n$ elementos que pertenecen a k, entonces*

$$(x_1 - a_1, x_2 - a_2, ..., x_n - a_n)$$

es un ideal maximal.

Demostración:

Supongamos que $\mathfrak{a} = (x_1 - a_1, x_2 - a_2, ..., x_n - a_n)$ y que existe un ideal $\mathfrak{b}$ tal que $\mathfrak{a} \subseteq \mathfrak{b} \subseteq k$.

Debemos probar que $\mathfrak{a} = \mathfrak{b}$ ó $\mathfrak{b} = k$.

Sea $f \in \mathfrak{b} - \mathfrak{a}$, luego aplicando el algoritmo de la división, entre $x_1 - a_1$ tenemos [2]

$$f = q_1(x_1 - a_1) + r_1 \ \ donde \ \ q_1 \in k[x_1, ..., x_n], r_1 \in k[x_2, ..., x_n] \ \ y \ \ r_1 \neq 0$$

[2]El algoritmo de la división: Sean $f(x)$ y $g(x)$ polinomios en $k[x]$ y el $\partial^0 g(x) \geq 1$. Entonces existen dos únicos polinomios $q(x)$ y $r(x)$ tales que $f(x) = q(x)g(x) + r(x)$ y $r(x) = 0$ ó $\partial^0 r(x) < \partial^0 g(x)$

donde $r_1 \neq 0$ por que $f \in \mathfrak{b} - \mathfrak{a}$, pues de lo contrario $f \in \mathfrak{a}$.

Luego a r_1 le aplicamos el algoritmo de la división entre $x_2 - a_2$, obteniendo:

$$\begin{aligned} r_1 &= q_2(x_2 - a_2) + r_2, \ \ con \ \ q_2 \in k[x_2, ..., x_n], r_2 \in k[x_3, ..., x_n] \ \ y \ \ r_2 \neq 0 \\ r_2 &= q_3(x_3 - a_3) + r_3, \ \ con \ \ q_3 \in k[x_3, ..., x_n], r_3 \in k[x_4, ..., x_n] \ \ y \ \ r_3 \neq 0 \\ &\vdots \\ r_{n-1} &= q_n(x_n - a_n) + r_n, \ \ con \ \ q_n \in k[x_n], r_n \in k \ \ y \ \ r_n \neq 0 \end{aligned}$$

Ahora sustituyendo todos los residuos en f tenemos

$$f = q_1(x_1 - a_1) + q_2(x_2 - a_2) + ... + q_n(x_n - a_n) + r_n \tag{4.5}$$

donde los $q_i \in k[x_1, ..., x_n]$, $r_n \in k$ y $r_n \neq 0$

Ahora como $\mathfrak{a} \subseteq \mathfrak{b}$ entonces

$$f - r_n = q_1(x_1 - a_1) + q_2(x_2 - a_2) + ... + q_n(x_n - a_n) \ \in \ \mathfrak{b} \tag{4.6}$$

Como (4.5) está en $\mathfrak{b} - \mathfrak{a}$ y tenemos que (4.6) está en $\mathfrak{b}$ entonces llegamos a que $r_n \in \mathfrak{b}$.

Dado que r_n es un inversible de $\mathfrak{b}$,[3] ya que r_n es un elemento no nulo del cuerpo escalar k, asi que por tener el ideal $\mathfrak{b}$ un elemento inversible, entonces $\mathfrak{b} = k[x_1, x_2, ..., x_n]$.

Por lo tanto $(x_1 - a_1, x_2 - a_2, ..., x_n - a_n)$ es un ideal maximal.

Teorema 4.2.1 *Sea k un cuerpo algebraicamente cerrado y sea $\mathfrak{a}$ un ideal maximal de $k[x_1, x_2, ..., x_n]$, entonces existen elementos $a_1, a_2, ..., a_n$ en k tal que*

$$\mathfrak{a} = (x_1 - a_1, x_2 - a_2, ..., x_n - a_n).$$

Demostración:

Sea

$$\phi : k[x_i] \longmapsto k[x_1, x_2, ..., x_n]$$

un homomorfismo en el anillo k.

Sea $\mathfrak{a} \subseteq k[x_1, x_2, ..., x_n]$ un ideal tomado en la imagen, luego como $k[x_1, x_2, ..., x_n]$ es un anillo noetheriano, tenemos que $k[x_1, x_2, ..., x_n]$ es finitamente generado, entonces la pre-imagen $\phi^{-1}(\mathfrak{a}) = k[x_i] \cap \mathfrak{a}$

[3] Si $\mathfrak{a}$ contiene un elemento inversible, entonces $\mathfrak{a} = R$, en particular si R es un anillo unitario y si $\mathfrak{a}$ es un ideal que contiene a 1 entonces $\mathfrak{a} = R$

es también un ideal maximal, para cada $i = 1, 2, 3, ..., n$.

Además como $k[x_i]$ es un dominio de ideales principales, entonces $k[x_i] \cap \mathfrak{a} = (f_i)$, con f_i polinomio irreducible. Pero por ser k algebraicamente cerrado, tenemos que $k[x_i] \cap \mathfrak{a} = (f_i) = (x_i - a_i)$ con $a_i \in k$.

Así tenemos que existen elementos $a_1, a_2, ..., a_n \in k$ tal que $x_i - a_i \in \mathfrak{a}$ ya que $k[x_i] \cap \mathfrak{a} = (x_i - a_i)$

Entonces tenemos que $(x_1 - a_1, x_2 - a_2, ..., x_n - a_n) \subseteq \mathfrak{a}$. Pero $\mathfrak{a}$ es un ideal maximal entonces $(x_1 - a_1, x_2 - a_2, ..., x_n - a_n) = \mathfrak{a}$.

Por tanto

$$(x_1 - a_1, x_2 - a_2, ..., x_n - a_n) = \mathfrak{a}$$

Teorema 4.2.2 (Teorema de los ceros de Hilbert forma débil) *Sea X una variedad algebraica afín en k^n, donde k es un cuerpo algebraicamente cerrado y sea $\mathfrak{a}(X)$ el ideal de X en el anillo de polinomios $k[x_1, x_2, ..., x_n]$, y si $\mathfrak{a}(X) \neq (1)$ entonces X es no vacío.*

Otra forma de escribir el teorema:

X una variedad algebraica afín en k^n, donde k es un cuerpo algebraicamente cerrado y sea $\mathfrak{a}(X)$ el ideal de X en el anillo de polinomios $k[x_1, x_2, ..., x_n]$, y si $X(\mathfrak{a}) = \emptyset$ entonces $\mathfrak{a} = k[x_1, x_2, ..., x_n]$.

Demostración:

Sea $\mathfrak{a}$ un ideal propio de $k[x_1, x_2, ..., x_n]$, siendo k un anillo conmutativo con unidad y $\mathfrak{a} \neq k[x_1, x_2, ..., x_n]$, luego por la proposición 2.1.1 existe un ideal maximal $\mathfrak{b}$ de k tal que $\mathfrak{a} \subseteq \mathfrak{b}$.

Ahora como k es un cuerpo algebraicamente cerrado y $\mathfrak{b}$ es un ideal maximal de $k[x_1, x_2, ..., x_n]$ entonces por el teorema 4.2.1 existen elementos $a_1, a_2, ..., a_n$ en k, es decir, que $a = (a_1, a_2, ..., a_n) \in k$ tal que $\mathfrak{b} = (x_1 - a_1, x_2 - a_2, ..., x_n - a_n)$ que es maximal.

Luego por estar $\mathfrak{a} \subseteq \mathfrak{b}$ por el lema 3.1.1 tenemos que $X(\mathfrak{a}) \supseteq X(\mathfrak{b})$.

Como $X(\mathfrak{b}) \subseteq X(\mathfrak{a})$, luego para ver que $X(\mathfrak{a}) \neq \emptyset$, bastará probar que $X(\mathfrak{b}) \neq \emptyset$.

Sea $f \in \mathfrak{b} = (x_1 - a_1, x_2 - a_2, ..., x_n - a_n)$, luego existen $q_1, q_2, ..., q_n \in k[x_1, x_2, ..., x_n]$ tal que

$$f = q_1(x_1 - a_1) + q_2(x_2 - a_2) + ... + q_n(x_n - a_n) \tag{4.7}$$

Evaluando el polinomio (4.7) en $a = (a_1, a_2, ..., a_n) \in k$ tenemos

$$\begin{aligned} f(a) &= q_1(a)((a_1 - a_1) + q_2(a)(a_2 - a_2) + ... + q_n(a)(a_n - a_n) \\ &= q_1(a)(0_k) + q_2(a)(0_k) + ... + q_n(a)(0_k) \\ &= 0_k \end{aligned}$$

Luego como $f(a) = 0_k$ para toda $f \in \mathfrak{b}$ por definición 3.1.4, tenemos que $a \in X(\mathfrak{b})$, por lo tanto $X(\mathfrak{b}) \neq \emptyset$ ya que $(a_1, a_2, ..., a_n) \in X(\mathfrak{b})$.
Como $X(\mathfrak{b}) \subseteq X(\mathfrak{a})$ entonces $a \in \mathfrak{a}$, es decir que, $a = (a_1, a_2, ..., a_n) \in \mathfrak{a}$.
Por tanto $X(\mathfrak{a}) \neq \emptyset$.

4.3. Teorema de los ceros de Hilbert en su forma fuerte

Teorema 4.3.1 *Sea R el anillo de polinomios $k[x_1, x_2, ..., x_n]$ donde k es un cuerpo algebraicamente cerrado y sea V la variedad en k^n definida por el ideal $\mathfrak{a}$ que está en R, y sea $\mathfrak{b}(V)$ el ideal de V, entonces $\mathfrak{b}(V) = r(\mathfrak{a})$.*

Demostración:
($\subseteq$) Sea $f \in r(\mathfrak{a})$, $x \in V(\mathfrak{a})$ entonces como $f \in r(\mathfrak{a})$, existe un $n \in \mathbb{N}$ tal que $f^n \in \mathfrak{a}$.
Ahora como $x \in V(\mathfrak{a})$, entonces para todo $g \in \mathfrak{a}$, $g(x) = 0$.
Ya que $g(x) = 0$, para toda $g \in \mathfrak{a}$, entonces como $f^n \in \mathfrak{a}$, vale en particular, que $f^n = 0$ para algún $n > 0$ donde $n \in \mathbb{N}$, luego para un n apropiado $f(x) = 0$, para toda $f \in \mathfrak{a}$ y por definición 3.2.1, $f \in \mathfrak{b}(V)$.
Por tanto $r(\mathfrak{a}) \subseteq \mathfrak{b}(V)$.
($\supseteq$) Sea $f \in \mathfrak{b}(V)$, como $\mathfrak{a}$ es un ideal de $R = k[x_1, x_2, ..., x_n]$ y como R es un anillo Noetheriano, entonces $\mathfrak{a}$ es finitamente generado, es decir, que $\mathfrak{a} = (f_1, f_2, ..., f_m)$.
Introduzcamos una variable adicional Y, y trabajemos en $k[x_1, x_2, ..., x_n, Y]$.
Sea $\mathfrak{a}^*$ el ideal de $k[x_1, x_2, ..., x_n, Y]$, generado por

$$\mathfrak{a}^* = (\mathfrak{a}, (1 - Yf))$$

Vamos a probar que $V(\mathfrak{a}^*) = \emptyset$.
Sea $(a_1, a_2, ..., a_n, a_{n+1}) \in V(\mathfrak{a}^*) \subseteq k^{n+1}$, y $(a_1, a_2, ..., a_n) \in V(\mathfrak{a})$ y resultando que para toda $f \in \mathfrak{a}$ $f(a_1, a_2, ..., a_n) = 0$. Evaluaremos el polinomio $1 - Yf$ en $(a_1, a_2, ..., a_n, a_{n+1})$.

$$\begin{aligned}(1 - Yf)(a_1, a_2, ..., a_n, a_{n+1}) &= 1 - a_{n+1} f(a_1, a_2, ..., a_n) \\ &= 1 - a_{n+1}(0_k) \\ &= 1\end{aligned}$$

Lo que es una contradicción, pues $(a_1, a_2, ..., a_n, a_{n+1}) \in V(\mathfrak{a}^*)$ y por lo tanto $V(\mathfrak{a}^*) = \emptyset$.

Aplicando el Teorema de Hilbert en su forma débil resulta que $\mathfrak{a}^* = k[x_1, x_2, ..., x_n, Y]$.

Como hemos visto que $\mathfrak{a}^* = k[x_1, x_2, ..., x_n, Y]$, entonces en particular $1 \in \mathfrak{a}^*$.

Recordando que $\mathfrak{a}^*$ esta generado por $(f_1, f_2, ..., f_m, (1 - Yf))$, por lo que existen una combinación lineal para 1 tal que

$$1 = \sum_{i=1}^{m} g_i f_i + h(1 - Yf) \ \ donde \ \ g_i, h \in k[x_1, x_2, ..., x_n, Y] \ \ y \ \ f_i \in \mathfrak{a} \tag{4.8}$$

Haciendo $Y = \frac{1}{f}$[4] y evaluando la igualdad (4.8) en $(x_1, x_2, ..., x_n, Y)$ tenemos

$$\begin{aligned}
1 &= \sum_{i=1}^{m} g_i f_i + h(1 - Yf)(x_1, x_2, ..., x_n, Y) \\
&= \sum_{i=1}^{m} (g_i f_i)(x_1, x_2, ..., x_n, Y) + h(1 - Yf)(x_1, x_2, ..., x_n, Y) \\
&= \sum_{i=1}^{m} g_i(x_1, x_2, ..., x_n, Y) f_i(x_1, x_2, ..., x_n, Y) + h(x_1, x_2, ..., x_n, Y) - \\
&\quad h(x_1, x_2, ..., x_n, Y) \frac{1}{f(x_1, x_2, ..., x_n)} f(x_1, x_2, ..., x_n, Y)
\end{aligned}$$

$$\begin{aligned}
&= \sum_{i=1}^{m} g_i(x_1, x_2, ..., x_n, Y) f_i(x_1, x_2, ..., x_n) + h(x_1, x_2, ..., x_n, Y) - \\
&\quad h(x_1, x_2, ..., x_n, Y) \frac{1}{f(x_1, x_2, ..., x_n)} f(x_1, x_2, ..., x_n) \\
&= \sum_{i=1}^{m} g_i(x_1, x_2, ..., x_n, Y) f_i(x_1, x_2, ..., x_n) + h(x_1, x_2, ..., x_n, Y) - \\
&\quad h(x_1, x_2, ..., x_n, Y) \\
&= \sum_{i=1}^{m} g_i(x_1, x_2, ..., x_n, Y) f_i(x_1, x_2, ..., x_n).
\end{aligned}$$

Llegamos a expresar a 1 como una suma finita de funciones racionales cuyos denominadores son potencias de f, es decir,

$$1 = \sum_{i=1}^{m} g_i(x_1, x_2, ..., x_n, \frac{1}{f(x_1, x_2, ..., x_n)}) f_i(x_1, x_2, ..., x_n) \tag{4.9}$$

[4]Este truco especial fue inventado por S. Rabinowitch en 1,929 y en su honor fué bautizado como truco de Rabinowitch, para mas detalles ver R. MILES A. (1995), Undergraduate Conmutative Álgebra, Cambridge University Press.

Multiplicando a ambos lados de la igualdad (4.9) por $f^r(x_1, x_2, ..., x_n)$ tenemos:

$$\begin{aligned} f^r(x_1, x_2, ..., x_n) &= f^r(x_1, x_2, ..., x_n)(\sum_{i=1}^{m} g_i(x_1, x_2, ..., x_n, Y) f_i(x_1, x_2, ..., x_n)) \\ &= \sum_{i=1}^{m} f^r(x_1, x_2, ..., x_n) g_i(x_1, x_2, ..., x_n, Y) f_i(x_1, x_2, ..., x_n) \end{aligned}$$

donde el producto de las funciones $f^r g_i \in k[x_1, x_2, ..., x_n]$ y las $f_i \in \mathfrak{a}$ entonces $f^r \in \mathfrak{a}$ y por definición 1.4.1 $f \in \mathfrak{a}$.

Por lo tanto $\mathfrak{b}(V) \subseteq r(\mathfrak{a})$.

Entonces $\mathfrak{b}(V) = r(\mathfrak{a})$.

Capítulo 5

Aplicación: Espacios Topológicos Noetherianos

5.1. Topologia de Zarisky

Trabajamos con k un cuerpo algebraicamente cerrado y $k[x] = k[x_1, x_2, ..., x_n]$ el anillo Noetheriano de polinomios en n variables con coeficientes en k.

Definición 5.1.1 *Sea k un campo y llamaremos topología de Zarisky en k^n a la Topología cuyos cerrados son de la forma $V(X)$, para un subconjunto $X \subseteq k[x_1, ..., x_n]$.*

Definición 5.1.2 *Sea U una variedad algebraica afín y $f \in k[x] = k[x_1, ..., x_n]$ entonces el conjunto*

$$U_f = \Big\{ x \in k[x] / f(x) \neq 0 \Big\}$$

es un abierto de U para la Topología de Zarisky.

Proposición 5.1.1 *Sea U una variedad algebraica afín. Probar que el conjunto U_f forman una base de conjuntos abiertos para la topología de Zarisky.*

Demostración:
Sea $B = \Big\{ U_f \Big\}_{f \in k[x]}$ un abierto de $U = V(X)$, es decir $U_f = k^n - U$, donde $U = V(X) = V(\langle X \rangle) = V(f_1, f_2, \ldots, f_n)$, debemos probar que B es una base para U.

Luego $V(X) = V(\bigcup_{\alpha \in X \subseteq k[x]} \{\alpha\})$. Partamos de

$$\begin{aligned} U_f &= k^n - V(X) \\ &= k^n - V(\bigcup_{\alpha \in X \subseteq k[x]} \{\alpha\}) \\ &= k^n - \bigcap_{\alpha \in X \subseteq k[x]} V(\{\alpha\}) \\ &= \bigcup_{\alpha \in X \subseteq k[x]} (k^n - V(\{\alpha\})) \\ &= \bigcup_{\alpha \in X \subseteq k[x]} U_\alpha \end{aligned}$$

por lo tanto $B = \left\{U_f\right\}_{f \in k[x]}$ forman una base de U para la Topología de Zarisky.

Proposición 5.1.2 *Sea k un cuerpo algebraicamente cerrado. Supongamos que k^n es cubierto por conjunto abiertos con la topología de Zarisky y sea $\mathfrak{a}$ un ideal generado por los $\mathfrak{a}_i$. Entonces $1 \in \mathfrak{a}$.*

Demostración:
Supongamos que $k^n = \bigcup_{i \in k[x]} (k^n - V(\mathfrak{a}_i)) = \bigcup_{i \in k[x]} (V(\mathfrak{a}_i))^c$ con $(V(\mathfrak{a}_i))^c$ abiertos en la topología de Zarisky.
Tomando complemento ambos lados tenemos:

$$\begin{aligned} (k^n)^c &= (\bigcup_{i \in k[x]} (V(\mathfrak{a}_i))^c)^c \\ \emptyset &= \bigcap_{i \in k[x]} (V(\mathfrak{a}_i)) \end{aligned}$$

$$\begin{aligned} &= V(\bigcup_{i \in k[x]} \mathfrak{a}_i) \\ &= V(\langle \bigcup_{i \in k[x]} \mathfrak{a}_i \rangle) \\ \emptyset &= V(\mathfrak{a}). \end{aligned}$$

Luego, por el teorema de los ceros de Hilbert forma débil , $\mathfrak{a} = k[x_1, , x_2, ..., x_n]$, es decir, el ideal $\mathfrak{a}$ tiene un elemento inversible, por lo tanto $1 \in \mathfrak{a}$.

Teorema 5.1.1 *Sea k un cuerpo algebraicamente cerrado, en el anillo noetheriano $k[x_1, x_2, ..., x_n]$, entonces k^n es compacto con la topología de Zarisky.*

Demostración:
Sea $\left\{U_{i\in K[x]}\mathfrak{a}_i = (V(\mathfrak{a}_i))^c\right\}$ un cubrimiento de abiertos de la topología de Zarisky para k^n, sea $\mathfrak{a} = \langle\bigcup_{i\in k[x]}\mathfrak{a}_i\rangle = \sum_{i\in k[x]}\mathfrak{a}_i = \left\{x_{i_1}+x_{i_2}+, ..., +x_{i_n},\ \ con\ \ x_{i_j}\in\mathfrak{a}_{i_j}\right\}$ y por la proposición 5.1.2, sabemos que $1\in\mathfrak{a}$, y con lo cual se puede expresar como una suma finita, es decir, $1 = x_{i_1} + x_{i_2}+, ..., +x_{i_r}$ para acierto $x_{i_j}\in\mathfrak{a}_{i_j}$, entonces $1\in\sum_{j=1}^{r}\mathfrak{a}_{i_j}$.
Ahora, como el polinomio constante e igual a 1 no se anula nunca, podemos concluir que $V(1) = \emptyset = V(\sum_{j=1}^{r}\mathfrak{a}_{i_j})$, esto es:

$$\begin{aligned} V(\sum_{j=1}^{r}\mathfrak{a}_{i_j}) &= \emptyset \\ V(\langle\bigcup_{j=1}^{r}\mathfrak{a}_{i_j}\rangle) &= \emptyset \\ V(\bigcup_{j=1}^{r}\mathfrak{a}_{i_j}) &= \emptyset \end{aligned}$$

$$\begin{aligned} (\bigcap_{j=1}^{r}V(\mathfrak{a}_{i_j}))^c &= (\emptyset)^c \\ \bigcup_{j=1}^{r}(V(\mathfrak{a}_{i_j}))^c &= k^n \end{aligned}$$

Entonces todo cubrimiento de abiertos en la topología de Zarisky para k^n admite una subcubierta finita para k^n.
Por tanto k^n es compacto en la topología de Zarisky.

Proposición 5.1.3 *Sea $X\subset k^n$, la variedad afín $V(\mathfrak{a}(X))$ es el conjunto más pequeño que contiene a X, en el sentido de que si $W\subset k^n$ es una variedad afín que contiene a X, entonces*

$$V(\mathfrak{a}(X))\subset W$$

Demostración:
Si $X\subset W$, entonces $\mathfrak{a}(X)\supset\mathfrak{a}(W)$, luego $V(\mathfrak{a}(X))\subset V(\mathfrak{a}(W))$, de donde se obtiene el resultado.

$V(\mathfrak{a}(X)) \subset W$.

Definición 5.1.3 *La cerradura de Zarisky de un subconjunto de un espacio afín es la variedad algebraica afín más pequeña que contiene al subconjunto. Si $X \subset k^n$, la cerradura de Zarisky de X es denotada por $\overline{X}$ y es igual a $V(\mathfrak{a}(X))$*

5.2. Definición y Propiedades de los Espacios Topológicos Noetherianos

Definición 5.2.1 *Sea U un espacio Topológico, U es llamado espacio Noetheriano si los subconjuntos cerrados de U satisfacen la condición de cadena descendente, es decir, para subconjuntos cerrados $V_1, V_2, V_3, ... \subseteq U$ con $V_{i+1} \subseteq V_i$ para todo entero positivo i, existe un entero n tal que $V_i = V_n$ para todo $i \geq n$. Una condición para los subconjuntos abiertos es que deben satisfacer la condición de cadena ascendente.*

Teorema 5.2.1 *Sea k un campo en el anillo noetheriano $k[x_1, x_2, ..., x_n]$ y $U \subseteq k^n$ un subconjunto de puntos, apropiado con la topología de Zarisky, entonces U es espacio Noetheriano.*

Demostración:
Supongamos que $U = k^n$ y sea $Y_1, Y_2, Y_3, \cdots \subseteq k^n$ una cadena descendente de subconjuntos cerrados de U, es decir, $Y_1 \supseteq Y_2 \supseteq Y_3 \supseteq \cdots$
Tomando ideales que generan esas variedades por lema 3.2.2 tenemos

$$\mathfrak{a}(Y_1) \subseteq \mathfrak{a}(Y_2) \subseteq \mathfrak{a}(Y_3) \subseteq \cdots$$

Luego por la condición de cadena ascendente de ideales está cadena es estacionaria, entonces existe un entero n tal que $\mathfrak{a}(Y_i) = \mathfrak{a}(Y_n)$ par todo $i \geq n$.
Tomando variedades a estos ideales tenemos $V(\mathfrak{a}(Y_i)) = V(\mathfrak{a}(Y_n))$ par todo $i \geq n$ y por le lema 3.2.1, para todo i: $Y_i = V(\mathfrak{a}(Y_i))$, por lo tanto $Y_i = Y_n$, para todo $i \geq n$.
Entonces la cadena $Y_1 \supseteq Y_2 \supseteq Y_3 \supseteq \cdots$, es estacionaria.
Por lo tanto U es un espacio topológico noetheriano.

Proposición 5.2.1 *Supongamos que U es un espacio topológico. Entonces las siguientes condiciones son equivalentes:*

1) *U es un espacio topológico noetheriano.*

2) *Toda familia no vacía de subconjuntos cerrados tiene un elemento minimal.*

3) *U satisface la condición de cadana ascendente para conjuntos abiertos.*

4) *Toda familia no vacía de subconjuntos abiertos tiene un elemento maximal.*

Demostración:

$1)$ implica $2)$

Supongamos que U es un espacio noetheriano y sea S una familia no vacía de subconjuntos cerrados de U, entonces existe un conjunto $Y_1 \in S$, por ser $S \neq \emptyset$. Supongamos que S no posee elemento minimal, por tanto $Y_1 \in S$ no es minimal, entonces podemos encontrar otro conjunto $Y_2 \in S$ tal que $Y_1 \supsetneq Y_2$. Luego como Y_2 no es minimal, entonces existe un conjunto $Y_3 \in S$ tal que $Y_2 \supsetneq Y_3$.

Así sucesivamente tenemos una sucesión de elementos de S que cumple con

$$Y_1 \supsetneq Y_2 \supsetneq Y_3 \ldots,$$

Por lo tanto, hemos contruido una sucesión $\left\{Y_n\right\}_{n\in\mathbb{N}}$ que cumple $Y_1 \supsetneq Y_2 \supsetneq Y_3 \ldots$, pero esto es una contradicción, por ser U un espacio noetheriano.

Por tanto S debe tener un elemento minimal.

$2)$ implica $3)$

Tomemos $U_1 \subseteq U_2 \subseteq U_3 \subseteq \ldots$, una cadena ascendente de subconjuntos abiertos de U. Entonces $\left\{U_i^c\right\}$ es una familia no vacía de subconjuntos cerrados, la cual por hipótesis tiene un elemento minimal, digamos que es U_m^c, asi $U_m^c \subseteq U_i^c$, por la condición de minimalidad, se tiene que $U_m^c = U_i^c$, para todo $i \geq m$. Esto implica que la cadena ascendente de subconjuntos abiertos

$$U_1 \subseteq U_2 \subseteq U_3 \subseteq \ldots,$$

de U se estaciona para todo $i \geq m$.

$3)$ implica $4)$

Supongamos que U satisface la condición de cadena ascendente para conjuntos abiertos y sea T una familia no vacía de subconjuntos abiertos de U, y supongamos que T no posee elemento maximal y lleguemos a una contradicción.

Como T es una familia no vacía de subconjuntos abiertos de U, entonces existe un conjunto $Y_1 \in T$, ya

que $T \neq \emptyset$, pero como T no tiene elemento maximal, entonces Y_1 no puede ser maximal, por lo tanto podemos encontrar un conjunto $Y_2 \in T$ tal que $Y_1 \subsetneq Y_2$.
Una ves más, ya que $Y_2 \in T$ no es maximal entonces existe un conjunto $Y_3 \in T$ tal que $Y_2 \subsetneq Y_3$.
Así construimos una sucesión $\left\{Y_m\right\}_{m\in\mathbb{N}}$ que cumple:

$$Y_1 \subsetneq Y_2 \subsetneq Y_3 \subsetneq \dots,$$

por ser una cadena estricta no cumple la condición de cadena ascendente para conjuntos abiertos, generando asi una contradicción.
Por lo tanto T tiene que tener un elememto maximal.
$4)$ implica $1)$
Tomemos $U_1 \supseteq U_2 \supseteq U_3 \supseteq \dots$, una cadena descendente de subconjuntos cerrados de U.
Entonces $\left\{Y_i^c\right\}$ es una familia no vacía de subconjuntos abiertos, que tiene un elemento maximal, por nuestra hipótesis, digamos que es Y_m^c, asi por la condición maximal, tenemos que $Y_i^c \supseteq Y_m^c$, por lo que $Y_i^c = Y_m^c$ para todo $i \geq m$ y esto implica que la cadena original $U_1 \supseteq U_2 \supseteq U_3 \supseteq \dots$, es estacionaria.
Por lo tanto U es un espacio topológico noetheriano.

Definición 5.2.2 *Un espacio topológico noetheriano U es llamado compacto si para todo conjunto M de subconjuntos abiertos, $U = \bigcup_{U\in M} U_i$, existe $U_1, U_2, \dots, U_n \in M$ tal que $U = \bigcup_{i=1}^{n} U_i$.*

Lema 5.2.1 *Todo espacio topológico noetheriano es compacto.*

Demostración:
Sea U un espacio topológico noetheriano y sea $\Omega = \left\{U_f\right\}_{f\in k[x]}$ una cubierta abierta para U. Supongamos que $U \notin \Omega$ y tomemos $U_1 \in \Omega$ y pongamos a $Y_1 = U - U_1$.
Luego tomemos un $U_2 \in \Omega_1$, donde $\Omega_1 = \Omega - U_1$ con $U_2 \subseteq U_1$, y hagamos a $Y_2 = U - U_1 \cup U_2$.
Así sucesivamente, tomamos un $U_3 \in \Omega_2$, donde $\Omega_2 = \Omega - U_2$ con $U_3 \subseteq U_2$, y hagamos a $Y_3 = U - (U_1 \cup U_2 \cup U_3)$, de esta manera generamos una sucesión decreciente de conjuntos cerrados

$$Y_1 \supseteq Y_2 \supseteq Y_3 \supseteq \cdots,$$

ya que U es un espacio noetheriano, dicha sucesión es estacionaria, es decir, para todo $i \geq m$, $Y_i = Y_m$, donde $Y_m = U - (U_1 \cup U_2 \cup \cdots \cup U_m)$, esto significa que a todo el espacio noetheriano U lo podemos escribir como:

$$U = (U_1 \cup U_2 \cup \cdots \cup U_m) \cup Y_m$$

pero como la familia $\left\{U_f\right\}_{f\in k[x]}$ cubre a U, por lo tanto $Y_m = \emptyset$ y entonces $U = U_1 \cup U_2 \cup \cdots \cup U_m$. Por lo tanto U es compacto.

Proposición 5.2.2 *Cualquier subconjunto de un espacio topológico noetherianos es noetheriano con su topología inducida.*

Demostración:
Sea U un espacio topológico y sea $Y \subseteq U$, tomemos $\left\{U_f\right\}_{f\in k[x]}$ una cubierta abierta de Y. Como sabemos, que para toda $f \in k[x]$, existe un $T_f \subseteq U$ un subconjunto abierto tal que $U_f = T_f \cap Y$, entonces podemos contruir una sucesión decreciente de subconjuntos cerrados de U, es decir, tomemos U_{f_1} y si $U_{f_1} \neq Y$, entonces tomemos a $F_1 = U - U_{f_1}$, Luego tomemos U_{f_2} tal que $U_{f_2} \subseteq U_{f_1}$ y hacemos $F_2 = U - (U_{f_1} \cap U_{f_2})$, así sucesivamente tomemos un U_{f_3} tal que $U_{f_3} \subseteq U_{f_2}$ y hacemos $F_3 = U - (U_{f_1} \cap U_{f_2} \cap U_{f_3})$, continuando de esta menera, contruimos una sucesión

$$F_1 \supseteq F_2 \supseteq F_3 \supseteq \cdots ,$$

decreciente de subconjuntos cerrados en U, por ser noetheriano U, la cadena es estacionaria, es decir, para todo $j \geq m$,

$$F_m = U - \bigcup_{j=1}^{m} U_{f_j} = F_j$$

Luego $Y \subset \bigcup_{j=1}^{m} T_{f_j}$, ya que de lo contrario, tendríamos un $x \in Y$ con $x \notin \bigcup_{j=1}^{m} T_{f_j}$, entonces existe un $g \in k[x]$, $g \neq f_j$ tal que $x \in U_g$, asi tenemos que $F_m \supsetneq F_g$, donde $F_g = U - (\bigcup_{j=1}^{m} U_{f_j}) \cup T_g$, que contradice la minimalidad de F_m, por la proposición 5.2.1 por lo tanto $Y \subset \bigcup_{j=1}^{m} T_{f_j}$
Así tenemos que $Y = Y \cap (\bigcup_{j=1}^{m} T_{f_j}) = \bigcup_{j=1}^{m} (Y \cap T_{f_j}) = \bigcup_{j=1}^{m} U_{f_j}$ ya que $U_f = T_f \cap Y$, entonces $Y = \bigcup_{j=1}^{m} U_{f_j}$.
Entonces para todo $j \geq m$,

$$F_m = U - Y = F_j$$

es decir, la cadena que contruimos anteriormente se estaciona en el subconjunto Y.
Por lo tanto Y es Noetheriano.

Teorema 5.2.2 *Un espacio topológico U es noetheriano si y solo si, todo subconjunto abierto $Y \subseteq U$ es compacto.*

Demostración:

Sea U un espacio topológico noetheriano, entonces por la proposición 5.2.2 ya que $Y \subseteq U$, tenemos que Y es noetheriano con la topología inducida, ya que la proposición se cumple para cualquier subconjunto y luego por el lema 5.2.1 Y es compacto.

Por lo tanto Y es compacto.

Recíprocamente, sea $U_1 \subseteq U_2 \subseteq U_3 \subseteq \ldots$, una cadena ascendente de subconjuntos abiertos de U. Luego denotemos por U, la unión de todos los estos abiertos, es decir,

$$U = \bigcup_{U \in M} U_i$$

para cualquier conjunto M de subconjuntos abiertos, entonces U es un conjunto abierto, ya que la unión arbitraria de abiertos es abierto, y por hipótesis U es compacto, entonces existe una subcubierta finita de estos conjuntos abiertos, es decir, para toda $i \geq m$, $\ U = \bigcup_{i=1}^{m} U_i$.

Luego estos conjuntos forman una cadena, por lo que podemos concluir que U es uno de estos, por lo tanto la sucesión

$$U_1 \subseteq U_2 \subseteq U_3 \subseteq \ldots,$$

es estacionaria, luego por la proposición 5.2.1 U es noetheriano.

Por tanto U es un espacio topológico noetheriano.

BIOGRAFÍA

[1] T. W. HUNGERFORD . Abstract Algebra. Chicago. Editorial Cleveland.

[2] D. G. NORTHCOTT (1953). Ideal Theory. New York. U.S.A. Editorial Bentley House, N.W.I.

[3] M. F. ATIYAH (1969). Introducción al álgebra conmutativa. California. Editorial Addison Wes ley Publishing Compony.

[4] ZARISKY, O.(1958) Algebre Conmutative. New York. Editorial D. Van Nostrand Company.

[5] N. BOURBAKY (1961), Algebre Commutative. Hermann, Paris.

[6] R. MILES A. (1995), Undergraduate Conmutative Álgebra, Cambridge University Press.

[7] GREGOR KEMPER (2009), A Course in Commutative Algebra. Springer

[8] COX DAVID, LITTLE JOHN AND O. DONAL, (2006) An Introduction to Computational algebraic Geometry and Commutative Algebra. Springer

[9] ALVARO RITTATORE (2006), Introducción a la teoría de Invariantes.

[10] MAXIMILIANO RIDDICK AND PAULA VIZZARRI, (2008). Introducción a la geometría algebraica.