UNIVERSIDAD MAYOR DE SAN ANDRÉS
FACULTAD DE CIENCIAS PURAS Y NATURALES
CARRERA DE MATEMÁTICA

ANILLOS NOETHERIANOS Y EL TEOREMA DE LOS CEROS DE HILBERT

PROYECTO DE GRADO PRESENTADO PARA LA OBTENCIÓN DEL TITULO DE LICENCIADO EN MATEMÁTICA

Autor: Univ. Néstor Adrián Maydana Coela

Tutor: Lic. Rudy Wilfredo Mayta Callisaya

La Paz - Bolivia
2021

Dedicado a:

Mis padres Evaristo Maydana Roque, Martha Coela de Maydana

a mis hermanos Maria, Ruddy, Miriam y Sonia.

Agradecimientos

Primeramente mi agradecimiento de dirige a quien ha forjado mi camino y me ha dirigido por el sendero correcto, a Dios, él que en todo momento está conmigo ayudándome a aprender de mis errores y a no cometerlos nuevamente.

Agradecer a la Carrera de Matemática por existir simplemente, ya que gracias a esta institución logre conocer personas importantes en el transcurso de mi vida, a los docentes que me brindaron conocimiento y sapiencia, al personal administrativo en general que me colaboraron en mis diligencias, mis compañeros y amigos que se convirtieron en prácticamente mis hermanos; más que todo agradecer a la carrera por brindarme la oportunidad de conocer a mi esposa Sonia Soledad, con la que forme una familia e hijos Matías Adrián, Samantha Flavia y Leandro Gael.

No podría olvidar a mis tribunales Lic. Helder E. Lopez R. y Lic. Eugenio Castaños C. por su paciencia y colaboración empática hacia mi persona, muchas gracias.

Resumen

En el presente trabajo mostraremos en principio la teoría de anillos, puesto que es importante en Geometría algebraica, Teoría de números y otros, entendemos que satisface cierta condición de finitud la cual por lo general se expresan mejor siguiendo a Noether, en tal sentido el proyecto obedece a un interés de exponer las condiciones necesarias para que un anillo cumpla las condiciones para que sea noetheriano; sin embargo dada la amplitud y aplicabilidad de los anillos ya mencionados nuestro documento tendrá un alcance restringido de los anillos noetherianos. Desde un punto de vista algebraico se trata de dar una descomposición de ideales bajo una descomposición de ciertos ideales las cuales llamaremos ideales primarios.

En la Matemática moderna el conocimiento y dominio del álgebra conmutativa es primordial en la comprensión de la teoría de estructuras algebraicas y la geometría algebraica las cuales contribuyen al estudio principalmente de los anillos conmutativos en particular de los anillos noetherianos, las cuales se nos presenta como la unificación de la Aritmética y la Geometría afín, uno de los objetivos del presente trabajo es poder apreciar las propiedades básicas de los anillos noetherianos proporcionando un marco natural para desarrollar su estudio dentro el Álgebra Conmutativa, para poder así relacionar los conjuntos algebraicos con sus ideales lo cual realizaremos mediante un estudio de las herramientas necesarias como los anillos noetherianos conmutativos, variedades algebraicas afines, el Lema de normalización de Noether y el Teorema de la Base de Hilbert entre los principales; para posteriormente mostrar el Teorema de los Ceros de Hilbert en su forma débil y en su forma fuerte.

Introducción

La historia del álgebra conmutativa empieza en el siglo IX, más concretamente en el periodo 1920-1926 con las investigaciones que realiza Emmy Noether en torno a la Teoría de Anillos Conmutativos que en ese tiempo fue denominada La Teoría General de Ideales.

De todos los trabajos que realizó en esta área se destacan dos: Idealtheorie in Ringbereich de 1921 Abstrakter Aufbau del Idealtheorie in Algebraischen Zahl-und Funktionskörpern desarrollado en el año de 1926.

También hay que resaltar un artículo donde Noether demuestra el conocido "Lema de Normalización"; el cual apoya bastante con sus aplicaciones al estudio de la dimensión de variedades algebraicas. El primero de estos trabajos fue calificado posteriormente por I. Kaplansky de "revolucionario", por su influencia en el desarrollo de la teoría general de ideales. Gracias a ese trabajo, Noether comenzó a ser reconocida como profesor adjunto de matemática por derecho propio y no como ayudante de Hilbert o Klein. En ambos artículos presenta un elegante enfoque abstracto que fue muy novedoso por aquel tiempo, y en los que además obtuvo resultados nuevos y significativos que no habían sido probados en los casos particulares. Sus resultados indicaban de forma tangible el potencial del enfoque axiomático, así como presagiaban la riqueza de las nuevas matemáticas que iban a producirse. Los puntos de vista iniciados por Noether en estos trabajos y posteriormente desarrollados por W. Krull (alumno de Noether el cual estuvo un año académico en la Universidad de Göttingen) originaron los principios de la materia que llamamos hoy en día Algebra Conmutativa.

Así el Álgebra conmutativa es el estudio de los anillos conmutativos.

En la Teoría de Anillos Conmutativos se puede establecer como consecuencia de las definiciones de anillos los ideales, estos son, los subgrupos aditivos que son invariantes bajo la multiplicación por cualquier elemento arbitrario del anillo. Para el buen desarrollo del presente trabajo vamos a distinguir también ciertas clases de ideales: ideales primos, ideales primarios, ideales maximales, etc. Los ideales pueden ser sumados, multiplicados e interceptados, lo que nos da una nueva clase de estructura combinatoria del conjunto de ideales en un anillo; En particular los ideales primos juegan un rol importante en este conjunto de ideales.

En el anillo de los enteros $\mathbb{Z}$, cada ideal puede ser generado por un solo número, por el cual los conceptos de "ideal" y "número" son casi idénticos en $\mathbb{Z}$ (y en cualquier dominio de ideales princi-

pales). Cabe mencionar que en un anillo en general, el concepto “ideal” permite generalizar muchas propiedades de los enteros como por ejemplo, ideales primos en lugar de números primos. En ciertas clases de anillos importantes de la teoría de números, como son los dominios Dedekind, se tiene una nueva versión del teorema fundamental de la aritmética: Cada ideal distinto de cero tiene una descomposición única como un producto de ideales primos. Mencionar que muchos resultados importantes de la teoría de anillos conmutativos dependen de la condición de finitud, como en el caso de los anillos Noetherianos donde toda sucesión ascendente de ideales es estacionaria o termina; conocidos como la condición de cadena ascendente.

Mencionaremos el Teorema de la base de Hilbert ($A[x]$ es noetheriano si A lo es) la cual muestra la importancia de incluir en su demostración la condición de finitud. Posteriormente veremos un teorema en Geometría algebraica que relaciona variedades e ideales en anillos de polinomios sobre cuerpos algebraicamente cerrados llamado el Teorema de los ceros de Hilbert.

Índice general

1 Anillos e ideales

El concepto de anillo es una generalización de los números enteros, donde se definen dos operaciones: la suma y el producto son afines entre sí por una ley distributiva.

Por lo tanto, los anillos son estructuras algebraicas más completas que los grupos, pero en el estudio de sus propiedades más importantes nos apoyamos a lo largo de la exposición en los grupos. Ya que simplemente todo anillo es un grupo en sí mismo.

Definiremos las propiedades elementales de los anillos e ideales, fijando notaciones y convenios, para posteriormente ver las operaciones fundamentales de ideales primos e ideales maximales.

La palabra *anillo* denotará a un *anillo conmutativo* con elemento identidad y las letras alemanas $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \ldots$, etc, denotarán a los ideales y las letras minúsculas latinas y griegas a los elementos.

1.1. Anillos e ideales

Definición 1.1. Un conjunto $(R, +, \cdot)$ con dos operaciones binarias (adición y multiplicación) se llama *anillo* si satisface:

(i) $(R, +)$ es un grupo abeliano aditivo.

(ii) $(R, \cdot)$ la multiplicación es asociativa y distributiva respecto a la adición, tanto por la derecha como por la izquierda.

Ejemplo 1.1.

1. $(\mathbb{Z}, +, \cdot)$ es un anillo conmutativo y con unidad.
2. $(\mathbb{N}, +, \cdot)$ no es un anillo.
3. El conjunto $R[x]$ con la suma y el producto usual es un anillo conmutativo con unidad sobre el campo R.

Definición 1.2. Un subconjunto S de un anillo R es un subanillo de R, si S es cerrado respecto a la adición y multiplicación, además contiene el elemento identidad de R.

Ejemplo 1.2. El conjunto $\mathbb{Z}$ es un subanillo de $\mathbb{Q}$, de $\mathbb{R}$ y de $\mathbb{C}$.

Definición 1.3. Sea R un anillo, y sea $\mathfrak{a}$ un subconjunto no vacío de R, entonces $\mathfrak{a}$ se llama un *ideal* de R cuando satisface las siguientes condiciones:

(i) Si $a_1, a_2 \in \mathfrak{a}$, entonces $a_1 \pm a_2$ *pertenecen ambos* a $\mathfrak{a}$.

(ii) Si $a \in \mathfrak{a}$, entonces $ra \in \mathfrak{a}$ para todo $r \in R$.

Observación 1.1. Sea R un anillo, *ideal bilátero* de R es un subconjunto no vacío $\mathfrak{a}$ que es cerrada bajo la suma e inverso aditivo, y tal que para todo $r \in R$ se tiene $r\mathfrak{a} \subseteq \mathfrak{a}$ y $\mathfrak{a}r \subseteq \mathfrak{a}$.

Ejemplo 1.3.

1. Para todo entero relativo k, $k\mathbb{Z}$ es un ideal de $\mathbb{Z}$.
2. 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 llama *ideal propio* a todo ideal no trivial.
3. 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 con identidad, entonces $\mathfrak{a} = R$.
4. Los únicos ideales en un cuerpo k son los ideales triviales.

1.2. Operaciones con ideales

1.2.1. Suma de ideales

Definición 1.4. Sean $\mathfrak{a}$ y $\mathfrak{b}$ dos ideales en R, se define 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 $x_1, x_2 \in \mathfrak{a}+\mathfrak{b}$, 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 definición, $\mathfrak{a} + \mathfrak{b}$ es un ideal.

1.2.2. Producto de ideales

Definición 1.5. Sean $\mathfrak{a}$ y $\mathfrak{b}$ dos ideales en R, se define el *producto* de $\mathfrak{a}$ y $\mathfrak{b}$ como el conjunto

$$\mathfrak{ab} = \left\{ \sum_{i=1}^{n} a_i b_i : a_i \in \mathfrak{a},\ b_i \in \mathfrak{b} \right\}.$$

Este conjunto es un ideal. Veamos su prueba:

Supongamos que $x_1, x_2 \in \mathfrak{ab}$, entonces $x_1 = \sum_{i=1}^{p} a_i b_i$ 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:

$$\begin{aligned} x_1 + x_2 &= \sum_{i=1}^{p} a_i b_i + \sum_{j=1}^{q} a'_j b'_j \\ &= (a_1 b_1 + a_2 b_2 + \cdots + a_p b_p) + (a'_1 b'_1 + a'_2 b'_2 + \cdots + a'_q b'_q) \\ &= a_1 b_1 + \cdots + a'_q b'_q \in \mathfrak{ab} \end{aligned}$$

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:

$$\begin{aligned} x_1 - x_2 &= \sum_{i=1}^{p} a_i b_i + \sum_{j=1}^{q} a'_j b'_j \\ &= (a_1 b_1 + a_2 b_2 + \cdots + a_p b_p) - (a'_1 b'_1 + a'_2 b'_2 + \cdots + a'_q b'_q) \\ &= a_1 b_1 + \cdots + a_p b_p + (-a'_1) b'_1 + (-a'_2) b'_2 + \cdots + (-a'_q) b'_q \in \mathfrak{ab} \end{aligned}$$

Ahora, sea $r \in R$

$$\begin{aligned} rx_1 &= r\left(\sum_{i=1}^{p} a_i b_i\right) \\ &= r(a_1b_1 + a_2b_2 + \cdots + a_pb_p) \\ &= ra_1b_1 + ra_2b_2 + \cdots + ra_pb_p \\ &= (ra_1)b_1 + (ra_2)b_2 + \cdots + (ra_p)b_p \in \mathfrak{ab} \end{aligned}$$

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.

1.2.3. Intersección de ideales

Definición 1.6. Sean $\mathfrak{a}$ y $\mathfrak{b}$ dos ideales en R, podemos tomar la intersección de $\mathfrak{a}$ y $\mathfrak{b}$ y definir el conjunto

$$\mathfrak{a} \cap \mathfrak{b} = \left\{a \in R : \, a \in \mathfrak{a} \text{ y } a \in \mathfrak{b}\right\}$$

Y en forma general se puede mostrar que toda intersección de ideales resulta ser un ideal, se escribe una familia de ideales $\{\mathfrak{a}_i\}$ y queremos comprobar que

$$I = \bigcap_{i=1}^{n} \mathfrak{a}_i \text{ es un ideal.}$$

Supóngase que $x_1, x_2 \in I$ y que $r \in R$ entonces como x_1, x_2 pertenecen a la intersección de los $\mathfrak{a}_i$ entonces ambos están en cada $\mathfrak{a}_i$; es decir 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 $x_1 + x_2 \in I$ y $x_1 - x_2 \in I$. Luego probemos que $rx \in I$ para esto tomemos a $x_1 \in I$ y $r \in R$ y como $x_1 \in I$ 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 $rx_1 \in I$.

Ahora como $x_1 + x_2$, $x_1 - x_2$ y rx_1 pertenecen a I entonces el conjunto I es un ideal. En particular para dos ideales $\mathfrak{a}$ y $\mathfrak{b}$ la intersección también es un ideal.

1.2.4. Cociente de ideales

Definición 1.7. 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:

$$(\mathfrak{a} : \mathfrak{b}) = \left\{x \in R : \, xb \in \mathfrak{a}, \ \forall b \in \mathfrak{b}\right\}$$

Esa división residual es un ideal. Supóngase 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 se tiene que $r(x_1 b) \in \mathfrak{a}$ y $rx_1 \in (\mathfrak{a} : \mathfrak{b})$. Y por lo tanto $(\mathfrak{a} : \mathfrak{b})$ es un ideal.

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

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

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

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

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

(4.1) $\mathfrak{a} \subseteq (\mathfrak{a} : \mathfrak{b})$

(5) $\left(\bigcap \mathfrak{a}_i : \mathfrak{b}\right) = \bigcap (\mathfrak{a}_i : \mathfrak{b})$

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

(7) $\left(\mathfrak{a} : \sum_{i=1}^{n} \mathfrak{b}_i\right) = \bigcap_{i=1}^{n} (\mathfrak{a} : \mathfrak{b})$

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

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 está definida por $\mathfrak{a} + \mathfrak{b} = \big\{a + b : a \in \mathfrak{a},\ b \in \mathfrak{b}\big\}$, 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 $\mathfrak{a} + \mathfrak{b} \supseteq \mathfrak{b} + \mathfrak{a}$.

Por lo tanto, tenemos:

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

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

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

Por lo tanto, tenemos:

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

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

Es inmediato de la definición del producto de ideales:

$$\begin{aligned}
\mathfrak{ab} &= \left\{ \sum_{i=1}^{n} a_i b_i : a_i \in \mathfrak{a},\ b_i \in \mathfrak{b} \right\} \\
&= \{a_1 b_1 + a_2 b_2 + \cdots + a_n b_n : a_i \in \mathfrak{a},\ b_i \in \mathfrak{b}\} \\
&= \{b_1 a_1 + b_2 a_2 + \cdots + b_n a_n : b_i \in \mathfrak{b},\ a_i \in \mathfrak{a}\} \\
&= \mathfrak{ba}
\end{aligned}$$

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

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

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

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

luego

$$y = \sum_{i=1}^{p} a_i \left[\sum_{j=1}^{k_{i(p)}} c_j b_j \right]$$

claramente y es una suma de elementos de la forma

$$y = a_i(b_i c_i), \text{ para todo } a_i \in \mathfrak{a},\ b_i \in \mathfrak{b} \text{ y } c_i \in \mathfrak{c}, \text{ donde asociando se tendrá } y \in (\mathfrak{ab})\mathfrak{c},$$

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

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

Por lo tanto,

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

(3) Se probará 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 $a \in \mathfrak{a}$ entonces $x = a + 0$, donde $0 \in \mathfrak{b}$, está en $x \in \mathfrak{a} + \mathfrak{b}$.
Por lo tanto, $\mathfrak{a} \subseteq \mathfrak{a} + \mathfrak{b}$.
(3.1) Ahora se probará que $\mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b}$.
Sea $x \in \mathfrak{ab}$, entonces por la definición de producto de ideales tendrá la forma $x = \sum_{i=1}^{n} a_i b_i$, tal que $a_i \in \mathfrak{a}$ y $b_i \in \mathfrak{b}$. Es claro que $\mathfrak{ab}$ es el ideal generado por los productos ab con $a \in \mathfrak{a}$ y $b \in \mathfrak{b}$ está contenido en la intersección de $\mathfrak{a}$ y $\mathfrak{b}$, 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 $i = 1, 2, 3, \ldots, n$. Como $y_i \in (\mathfrak{a} : \mathfrak{b})$, por definición de división residual o cociente residual tenemos que $y_i\mathfrak{b} \subseteq \mathfrak{a}$, es decir, $y_i b \in \mathfrak{a}$ para todo $b \in \mathfrak{b}$ y para todo $i = 1, 2, 3, \ldots, n$, pero como $z_i \in \mathfrak{b}$ entonces $y_i z_i \in \mathfrak{a}$ para todo $i = 1, 2, 3, \ldots, n$ y entonces $x \in \mathfrak{a}$.
Por lo tanto se tiene $(\mathfrak{a} : \mathfrak{b}) \subseteq \mathfrak{a}$.

(4.1) Probemos que $\mathfrak{a} \subseteq (\mathfrak{a} : \mathfrak{b})$. Sea $x \in \mathfrak{a}$ y si se logra probar que $x\mathfrak{b} \subseteq \mathfrak{a}$, la prueba estaría completa. Como sabemos que $x\mathfrak{b} = \{xb : b \in \mathfrak{b}\}$ y por ser $\mathfrak{a}$ un ideal tenemos que $xb \in \mathfrak{a}$ 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 $\left(\bigcap \mathfrak{a}_i : \mathfrak{b}\right) = \bigcap (\mathfrak{a}_i : \mathfrak{b})$.
Probemos primero que $\left(\bigcap \mathfrak{a}_i : \mathfrak{b}\right) \subseteq \bigcap (\mathfrak{a}_i : \mathfrak{b})$.
Sea $x \in \left(\bigcap \mathfrak{a}_i : \mathfrak{b}\right)$ entonces $xb \in \bigcap \mathfrak{a}_i$ para todo $b \in \mathfrak{b}$ por definición de cociente residual. Luego $xb \in \mathfrak{a}_i$. Entonces $xb \in \mathfrak{a}_i$ para todo $b \in \mathfrak{b}$, es decir, $x \in (\mathfrak{a}_i : \mathfrak{b})$ para todo i, por lo tanto $x \in \bigcap (\mathfrak{a}_i : \mathfrak{b})$. Por tanto,

$$\left(\bigcap \mathfrak{a}_i : \mathfrak{b}\right) \subseteq \bigcap (\mathfrak{a}_i : \mathfrak{b}) \tag{1.1}$$

Sea $y \in \bigcap (\mathfrak{a}_i : \mathfrak{b})$, para cada i tenemos que $y \in (\mathfrak{a}_i : \mathfrak{b})$. Entonces $y\mathfrak{b} \in \mathfrak{a}_i$ para todo i. Por lo tanto tenemos que $y\mathfrak{b} \in \bigcap \mathfrak{a}_i$ para todo $b \in \mathfrak{b}$. Así, $y \in (\bigcap \mathfrak{a}_i : \mathfrak{b})$.

$$\bigcap (\mathfrak{a}_i : \mathfrak{b}) \subseteq \left(\bigcap \mathfrak{a}_i : \mathfrak{b}\right) \tag{1.2}$$

Por (1.1) y (1.2) tenemos que $\left(\bigcap \mathfrak{a}_i : \mathfrak{b}\right) = \bigcap (\mathfrak{a}_i : \mathfrak{b})$.

(6) Probemos que $\big((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}\big) = \big(\mathfrak{a} : (\mathfrak{b}\mathfrak{c})\big)$.
Sea $x \in \big((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}\big)$, 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 $b \in \mathfrak{b}$. Por tanto, se tiene $x(cb) \in \mathfrak{b}$.
Ahora, podemos conmutar los elementos b y c y se obtiene $x(bc) \in \mathfrak{a}$ y aplicando de nuevo la definición tenemos que $x \in \big(\mathfrak{a} : (\mathfrak{b}\mathfrak{c})\big)$:

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

Ahora, sea $x \in \big(\mathfrak{a} : (\mathfrak{b}\mathfrak{c})\big)$. 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 que $x \in \big((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}\big)$. Así,

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

Por (1.3) y (1.4) se tiene que $\big(\mathfrak{a} : (\mathfrak{b}\mathfrak{c})\big) = \big((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}\big)$.

(7) Ahora probemos que $\left(\mathfrak{a} : \sum_{i=1}^{n} \mathfrak{b}_i\right) = \bigcap_{i=1}^{n} (\mathfrak{a} : \mathfrak{b}_i)$.
Sea $x \in \left(\mathfrak{a} : \sum_{i=1}^{n} \mathfrak{b}_i\right)$, por la definición de cociente residual tenemos $x\left(\sum_{i=1}^{n} b_i\right) \in \mathfrak{a}$ 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 vez más nos da que $x \in (\mathfrak{a} : \mathfrak{b}_i)$ para todo i.

De esta forma $x \in \bigcap_{i=1}^{n}(\mathfrak{a} : \mathfrak{b}_i)$.
Por tanto tenemos:

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

Sea $x \in \bigcap_{i=1}^{n}(\mathfrak{a} : \mathfrak{b}_i)$, entonces $x \in (\mathfrak{a} : \mathfrak{b}_i)$ para todo i. Aplicando la definición de cociente residual tenemos $x\,b_i \in \mathfrak{a}$ para todo i y por ser para todo i, por lo tanto $x \sum_{i=1}^{n} b_i \in \mathfrak{a}$. Nuevamente por la definición de cociente residual, $x \in \left(\mathfrak{a} : \sum_{i=1}^{n} \mathfrak{b}_i\right)$.
Por lo tanto:

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

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

(8) Finalmente probemos $(\mathfrak{a} : \mathfrak{b}) = \big(\mathfrak{a} : (\mathfrak{a} + \mathfrak{b})\big)$.
Por (7) de la misma proposición sabemos que:

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

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

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

□

1.3. Ideales generados por un conjunto

Definición 1.8. Sea A un conjunto no vacío de elementos finitos arbitrarios 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, se llama el *ideal generado por un conjunto.*

Sea x_1 y x_2 que pertenecen al ideal generado por el conjunto finito A, distinto del vacío en el anillo R, entonces $x_1 = \sum_{i=1}^{n} r_i a_i$ y $x_2 = \sum_{i=1}^{m} r_i' a_i'$. Sin pérdida de generalidad $m > n$, veamos que la suma $x_1 + x_2$ está en el conjunto.

Sea $x_1, x_2 \in \sum_{i=1}^{n} r_i a_i$ 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 $x_1 + x_2$ está en el conjunto:

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

Así, $x_1 + x_2 \in \sum_{i=1}^{m} r_i a_i$.

Ahora vemos para la diferencia, bajo las mismas condiciones.

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

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

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

Dado que $a_i \in A$ y $kr_i \in R$, para todo $i = 1, \ldots, n$, entonces el conjunto $\sum_{i=1}^{n} (kr_i) a_i$ pertenece al ideal, por lo tanto el conjunto $\sum_{i=1}^{n} r_i a_i$ es un ideal

Definición 1.9. Si A consta de un número finito de elementos $a_1, a_2, \ldots, a_n$, entonces el ideal generado por $a_1, a_2, \ldots, a_n$ es denotado por $(a_1, a_2, \ldots, a_n)$ y consiste en todos los elementos que se pueden escribir de la forma $r_1 a_1 + r_2 a_2 + \cdots + r_n a_n$, donde los r_i son cualquier elemento de R.

Se dice que tal ideal está generado finitamente y los elementos a_i son llamados una base o bases de un ideal.

Además, el ideal generado por la suma y el producto se definen de la siguiente manera:

$$(a_1, a_2, \ldots, a_m) + (b_1, b_2, \ldots, b_n) = (a_1, \ldots, a_m, b_1, \ldots, b_n)$$
$$(a_1, a_2, \ldots, a_m)(b_1, b_2, \ldots, b_n) = (\ldots, a_i b_j, \ldots)$$

Observación.- Cuando el ideal es generado por un solo elemento, es decir, (a) se llama el *ideal principal.*

1.4. Ideales primos e ideales maximales

Sea R un anillo, un elemento $a \in R$ se llama un *divisor de cero* si existe un elemento no nulo $b \in R$ tal que $ab = 0$. Los elementos de R que no son divisores de cero se llaman **elementos regulares**. Cuando el elemento cero es el único divisor de cero de un anillo R, se dice que R es un **domino de integridad** o simplemente un **dominio**.

Definición 1.10. Un ideal $\mathfrak{p}$ se llama *ideal primo* siempre que $ab \in \mathfrak{p}$, al menos uno de ellos pertenece a $\mathfrak{p}$, es decir si a pertenece a $\mathfrak{p}$ o b pertenece a $\mathfrak{p}$.

Equivalentemente podemos definir los siguiente.

Definición 1.11. 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 $b \in \mathfrak{p}$.

Ejemplo 1.4. En el caso de anillo $\mathbb{Z}$ de los números enteros los ideales primos son:

1. El ideal cero
2. Los ideales de la forma $p\mathbb{Z}$, con p un entero primo (positivo).

Proposición 1.2. Sea $\mathfrak{p}$ un ideal primo, y supongamos que $a_1 \cdot a_2 \cdots a_n \in \mathfrak{p}$, entonces para al menos un valor de i tenemos que $a_i \in \mathfrak{p}$. Además, si $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n$ son ideales y $\mathfrak{a}_1 \cdot \mathfrak{a}_2 \cdots \mathfrak{a}_n \subseteq \mathfrak{p}$, entonces $\mathfrak{a}_i \subseteq \mathfrak{p}$ para al menos un valor de i.

Demostración. Supongamos por contradicción que $a_1 \cdot a_2 \cdots a_n \in \mathfrak{p}$ y que $a_i \notin \mathfrak{p}$.

Tenemos $a_1 \cdot a_2 \cdots a_n = a_1(a_2 \cdots a_n) \in \mathfrak{p}$ y $a_1 \notin \mathfrak{p}$ por definición de un ideal primo, entonces $a_2 a_3 \cdots a_n \in \mathfrak{p}$. Ahora repetimos el argumento y para ello tenemos $a_2 a_3 \cdots a_n = a_2(a_3 \cdots a_n) \in \mathfrak{p}$ y $a_2 \notin \mathfrak{p}$ entonces $a_3 \cdots a_n \in \mathfrak{p}$ y así sucesivamente obtenemos una sucesión $a_2 a_3 \cdots a_n \in \mathfrak{p}$, $a_3 a_4 \cdots a_n \in \mathfrak{p}$, $a_4 a_5 \cdots a_n \in \mathfrak{p}$, y finalmente $a_n \in \mathfrak{p}$ pero esto es una contradicción ya que habíamos supuesto que $a_n \notin \mathfrak{p}$.

Por por otra parte, asumamos que $\mathfrak{a}_1 \mathfrak{a}_2 \cdots \mathfrak{a}_n \subseteq \mathfrak{p}$, 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 $a_1(a_2 \cdots a_n) \in \mathfrak{a}_1(\mathfrak{a}_2 \cdots \mathfrak{a}_n) \subseteq \mathfrak{p}$ y entonces tenemos que $a_1(a_2 \cdots a_n) \in \mathfrak{p}$ pero esto es una contradicción ya que en la construcción de la sucesión tenemos que $a_1, (a_2, \cdots, a_n) \notin \mathfrak{p}$. Por la tanto $\mathfrak{a}_i \subseteq \mathfrak{p}$ para al menos un valor de i. □

Definición 1.12. 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 1.13. 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 1.14. 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 $\mathfrak{p}$.

1.5. El radical de un ideal

Definición 1.15. Sea $\mathfrak{a}$ un ideal en un anillo R. El conjunto de todos los elementos x, tal que algún exponente positivo de x está en $\mathfrak{a}$, se llama el *radical* del ideal $\mathfrak{a}$. Es decir,

$$r(\mathfrak{a}) = \left\{x \in R : x^n \in \mathfrak{a}, \text{ para algún } n > 0 \text{ con } n \in \mathbb{N}\right\}$$

Este conjunto es un ideal.

Sea $x \in r(\mathfrak{a})$, entonces existe $n > 0$ tal que $x^n \in \mathfrak{a}$, está 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, $x + y \in r(a)$. De forma análoga se prueba que $x - y \in r(\mathfrak{a})$.

Por tanto $r(\mathfrak{a})$ es un ideal.

Proposición 1.3. Sean $\mathfrak{a}$ y $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n$ ideales en el anillo R, entonces

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

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

(3) $r(\mathfrak{a}) = R$ si y solo si $\mathfrak{a} = R$

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

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

Demostración. (1) Para todo $x \in \mathfrak{a}$, se tendrá que $x^1 \in \mathfrak{a}$ como $1 \in \mathbb{N}$, entonces $x \in r(\mathfrak{a})$, por tanto $\mathfrak{a} \subseteq r(\mathfrak{a})$.

Ahora mostremos que $r(\mathfrak{a}) \subseteq r(r(\mathfrak{a}))$, sea $x \in r(\mathfrak{a})$, por definición de radical existe $n \in \mathbb{N}$ tal que $x^n \in \mathfrak{a}$, ahora tomando algún $m \in \mathbb{N}$ $(x^n)^m \in r(\mathfrak{a})$, es decir $x \in r(\mathfrak{a})$. Por lo tanto, $r(\mathfrak{a}) \subseteq r(r(\mathfrak{a}))$. De modo análogo, si $x \in r(r(\mathfrak{a}))$, existe un $n \in \mathbb{N}$ tal que $x^n \in r(\mathfrak{a})$, por lo cual implica que $x^{nm} = (x^n)^m$ para $m \in \mathbb{N}$, entonces $x \in \mathfrak{a}$. Por lo tanto, $r(r(\mathfrak{a})) \subseteq r(\mathfrak{a})$.

(2) Si $x \in \bigcap_{j=1}^n r(\mathfrak{a}_j)$, existen $m_1, m_2, \ldots, m_n > 0$ tal que $x^{m_j} \in \mathfrak{a}_j$ para cada $j = 1, 2, \ldots, n$; luego tomando $m = m_1 + m_2 + \cdots + m_n$ tenemos

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

Así, $\bigcap_{j=1}^{n} r(\mathfrak{a}_j) \subseteq r(a_1 \cdot a_2 \cdots a_n)$, dado que $\mathfrak{a}_1 \cdot \mathfrak{a}_2 \cdots \mathfrak{a}_n \subseteq \bigcap_{j=1}^{n} \mathfrak{a}_j$ por la Proposición 1.1 literal 3.1 tenemos que $r(\mathfrak{a}_1 \cdot \mathfrak{a}_2 \cdots \mathfrak{a}_n) \subseteq r\left(\bigcap_{j=1}^{n} \mathfrak{a}_j\right)$. Finalmente, si $x \in r\left(\bigcap_{j=1}^{n} \mathfrak{a}_j\right)$, existe un $n > 0$ tal que $x^n \in \bigcap_{j=1}^{n} \mathfrak{a}_j$, entonces para cada $j = 1, 2, \ldots, n$, $x^n \in \mathfrak{a}_j$, es decir, $x \in r(\mathfrak{a}_j)$. Entonces $x \in \bigcap_{j=1}^{n} r(\mathfrak{a}_j)$ y $r\left(\bigcap_{j=1}^{n} \mathfrak{a}_j\right) = \bigcap_{j=1}^{n} r(\mathfrak{a}_j)$.
Así, $r\left(\bigcap_{j=1}^{n} \mathfrak{a}_j\right) = \bigcap_{j=1}^{n} r(\mathfrak{a}_j) \subseteq r(\mathfrak{a}_1 \cdot \mathfrak{a}_2 \cdots \mathfrak{a}_n) \subseteq r\left(\bigcap_{j=1}^{n} \mathfrak{a}_j\right)$, es lo que se quería probar.

(3) Sea $r(\mathfrak{a}) = R$, para todo $\mathfrak{a} \in R$, existe un $n \in \mathbb{N}$ 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 $R \subseteq r(\mathfrak{a})$.
Ahora, $x \in r(\mathfrak{a})$, entonces $x^n \in \mathfrak{a}$, 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:

$$\mathfrak{a}_1 + \mathfrak{a}_2 \subseteq r(\mathfrak{a}_1) + r(\mathfrak{a}_2)$$
$$r(\mathfrak{a}_1 + \mathfrak{a}_2) \subseteq r\big(r(\mathfrak{a}_1) + r(\mathfrak{a}_2)\big).$$

Para probar la otra inclusión, tomemos $x \in r\big(r(\mathfrak{a}_1) + r(\mathfrak{a}_2)\big)$, 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 $x_1 \in r(\mathfrak{a}_1)$ y $x_2 \in r(\mathfrak{a}_2)$, 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 $\mathfrak{a}_1$ o 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 $r\big(r(\mathfrak{a}_1) + r(\mathfrak{a}_2)\big) \subseteq r(\mathfrak{a}_1 + \mathfrak{a}_2)$.

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

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

Pero por (1) sabemos que $r(p^n) = r(\mathfrak{p}) \supseteq \mathfrak{p}$. 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 $x \in \mathfrak{p}$ o $x^{n-1} \in \mathfrak{p}$, pero como n es el menor entero positivo entonces $n = 1$ y por lo tanto $x \in \mathfrak{p}$, entonces $r(\mathfrak{p}) \subseteq \mathfrak{p}$.

□

1.6. Ideales primarios

Definición 1.16. 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 una potencia positiva 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 $b^n \in q$ para algún $n > 0$. Una definición equivalente es la siguiente.

Definición 1.17. Un ideal $\mathfrak{q}$ en un anillo R es primario si $\mathfrak{q} \neq R$ y si $ab \in \mathfrak{q}$ entonces para cada $a \in \mathfrak{q}$ o $b^n \in \mathfrak{q}$ para algún $n > 0$.

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

Ejemplo 1.5. Es claro que todo ideal primo es primario, pero no vale la recíproca. Si $\mathfrak{p}$ es número primo y $n > 2$ un entero positivo, luego $\mathfrak{p}^n = (\mathfrak{p}^n)$ es un ideal primario en $\mathbb{Z}$ que no es primo, pues $\mathfrak{p}\mathfrak{p}^{-1} \in (\mathfrak{p}^n)$, pero $\mathfrak{p}$ y $\mathfrak{p}^{-1}$ no están en $(\mathfrak{p}^n)$. Para ver que es primario, sean $a, b \in \mathbb{Z}$ tales que $ab \in (\mathfrak{p}^n)$ y $a \notin (\mathfrak{p}^n)$ luego $\mathfrak{p}^n$ divide a ab pero no divide a $\mathfrak{a}$, entonces $\pm$ divide a b y en consecuencia $b^n \in (\mathfrak{p}^n)$.

Proposición 1.4. 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 $x, y \in \mathfrak{p}$ e $r \in R$, entonces existen enteros m y n, tal que $x^m \in \mathfrak{q}$ y $y^n \in \mathfrak{q}$. Ahora tenemos:

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

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 $\mathfrak{p}$. Por tanto, $\mathfrak{p}$ 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 $(ab)^s \in \mathfrak{q}$ 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 alguna potencia 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 $\mathfrak{q} \subseteq \mathfrak{p}$ vamos a realizarlo de modo recíproco. Sea $x \in \mathfrak{p}$, como $\mathfrak{p}$ es el conjunto de todos los elementos x tal que $x^n \in \mathfrak{q}$ para al meno un valor entero positivo 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 $\mathfrak{q} = \mathfrak{q}_1 \cdot \mathfrak{q} \cdots \mathfrak{q} \subseteq \mathfrak{p}'$, entonces por la proposición 1.2 sabemos que $x^n\mathfrak{q} = \mathfrak{q}_1 \cdot \mathfrak{q} \cdots \mathfrak{q} \subseteq \mathfrak{p}'$ entonces $\mathfrak{q}_i \subseteq \mathfrak{p}'$ para al menos un valor de i, con $i = 1, 2, \ldots, n$, 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 $\mathfrak{p} \subseteq \mathfrak{p}'$. □

1.7. Descomposición primaria de ideales

Definición 1.18. Si un ideal $\mathfrak{a}$ se puede expresar de la siguiente forma:

$$\mathfrak{a} = \mathfrak{q}_1 \cap q_2 \cap \cdots \cap \mathfrak{q}_n,$$

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 una *componente primaria* de la descomposición primaria del ideal $\mathfrak{a}$.

Dependiendo del tipo de anillo y del tipo de ideal, encontrar una descomposición primaria resultará más o menos sencillo. Si el ideal que queremos descomponer es principal, es decir está generado por un solo elemento, entonces la obtención de una descomposición primaria es inmediata: basta con descomponer en factores irreducibles el polinomio que genera el ideal y considerar los ideales generados por cada uno de esos factores. Veamos algunos ejemplos.

Ejemplo 1.6. Dado el ideal $(x^4 - 1) \in \mathbb{Q}[x]$, una descomposición primaria vendrá dada por los componentes primarios irreducibles del polinomio

$$(x^4 - 1) = (x^2 + 1) \cap (x - 1) \cap (x + 1)$$

Definición 1.19. 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 1.20. Diremos que ideal $\mathfrak{a}$ es *descomponible* si tiene una descomposición primaria.

Ejemplo 1.7. Encontrar una descomposición primaria del ideal $\mathfrak{a} = (x^2, xy)$.

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

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

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

Teorema 1.1. Sea $\mathfrak{a} = \mathfrak{q}_1 \cap q_2 \cap \cdots \cap \mathfrak{q}_n$, donde $\mathfrak{q}_i$ es $\mathfrak{p}_i$-primario para $1 \leq i \leq n$. Entonces cualquier ideal primo que esté contenido en $\mathfrak{a}$ debe contener al menos uno de los $\mathfrak{p}_i$; el ideal primo minimal de $\mathfrak{a}$ es precisamente los ideales primos $\mathfrak{p}_i$ que no contienen estrictamente cualquier otro $\mathfrak{p}_j$, es decir, el $r(\mathfrak{a}) = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \cdots \cap \mathfrak{q}_n$, 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 conteniendo $\mathfrak{a}$, entonces

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

Consecuentemente, por la Proposición 1.1 literal 3.1) y por la Proposición 1.2, podemos escoger un i tal que $\mathfrak{q}_i \subseteq \mathfrak{p}$, por la Proposición 1.4 tenemos que $\mathfrak{p}_i \subseteq \mathfrak{p}$, por la definición de ideales primos minimales de un ideal tenemos que $\mathfrak{p}_i \subseteq \mathfrak{a}$ y $\mathfrak{p} \nsubseteq \mathfrak{a} \subseteq \mathfrak{p}$.
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 $x \in \bigcap_{i=1}^{n} \mathfrak{q}_i$ y por lo tanto tenemos que

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

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

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

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

Corolario 1.1. 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 $n = 1$, se tiene $x \in \mathfrak{q}$, por lo tanto $\mathfrak{p} \subseteq \mathfrak{q}$.

Se tiene que para todo $x \in \mathfrak{q}$, para algún entero positivo $n = 1$ $x^1 \in \mathfrak{q}$, 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 $\mathfrak{q} = \mathfrak{p}$.

Ahora por hipótesis $ab \in \mathfrak{q}$ y $a \notin \mathfrak{p}$ o como se mostró anteriormente $a \notin \mathfrak{q}$. Por definición de ideal primo, no queda de otra que $b \in \mathfrak{q}$. □

Corolario 1.2. 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 1.1, y como b es un elemento cualquiera de $\mathfrak{b}$ entonces $\mathfrak{b} \subseteq \mathfrak{q}$. □

Corolario 1.3. 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 literal (4). Dado que $\mathfrak{a} \nsubseteq \mathfrak{p}$, por el Corolario 1.2 tenemos:

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

La otra inclusión es inmediata utilizando la Proposición 1.1 literal 4.1.
Así

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

De (1.9) y (1.10) tenemos que $(\mathfrak{q} : \mathfrak{a}) = \mathfrak{q}$ y es lo que se quería mostrar. □

Lema 1.1. 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 alguna potencia positiva 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), $a \in \mathfrak{p}'$, 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 $\mathfrak{q}'$ 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 1.19 $\mathfrak{p} = r(\mathfrak{q}')$, 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 $x \in \mathfrak{q}' \subseteq \mathfrak{p}'$ por (1), entonces $x \in \mathfrak{p}'$. Luego $\mathfrak{p} = \mathfrak{p}'$.
Por lo tanto, $\mathfrak{q}' \subseteq \mathfrak{p}'$. □

Proposición 1.5. Si $\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_n$ son todos ideales $\mathfrak{p}$—primarios, entonces $\mathfrak{q} = \bigcap_{i=1}^{n} \mathfrak{q}_i$ es también un ideal $\mathfrak{p}$—primario.

Demostración. Sean $\mathfrak{q}$ y $\mathfrak{p}$ ideales donde $\mathfrak{q} = \bigcap_{i=1}^{n} \mathfrak{q}_i$ y como cada q_i es $\mathfrak{p}$—primario, por hipótesis para algún $\mathfrak{q}_i$ 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 $m = \text{máx}\{m_1, m_2, \ldots, m_n\}$ 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 $\mathfrak{q} = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \cdots \cap \mathfrak{q}_n$ entonces $ab \in \mathfrak{q} = \bigcap_{i=1}^{n} \mathfrak{q}_i$ 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 1.1 deducimos que $\mathfrak{q}$ es $\mathfrak{p}$-primario. □

Proposición 1.6. 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. Sea $\mathfrak{a} \subseteq \mathfrak{q}$ ahora supongamos que $\mathfrak{q}' = (\mathfrak{q} : \mathfrak{a})$ con $\mathfrak{q}' \neq (1)$, como $\mathfrak{a} \subseteq \mathfrak{q}$ podemos encontrar $a_0 \in \mathfrak{a}$ tal que $a_0 \in \mathfrak{q}$. Si tomamos $y \in \mathfrak{q}'$ entonces $a_0 y \in \mathfrak{q}$ y $a_0 \in \mathfrak{q}$. 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 $x^m \mathfrak{q} \subseteq \mathfrak{p}$ 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 1.1 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 $(\mathfrak{q} : \mathfrak{a}) = R = (1)$. □

2 Anillos noetherianos conmutativos

Dada la amplitud de los anillos noetherianos conmutativos el estudio de los mismos en el presente trabajo será con un alcance restringido mostrando operaciones familiares, en particular para el Teorema de la base de Hilbert.

2.1. Definiciones y conceptos en anillos noetherianos

Recuerde que un ideal $\mathfrak{a}$ es finito, si podemos encontrar un conjunto $\{a_1, a_2, \ldots, a_n\}$ finito tal que

$$\mathfrak{a} = Ra_1 + Ra_2 + \cdots + Ra_n,$$

Ra_i con $i = 1, \ldots, n$ es sólo otra manera de escribir el ideal principal (a_i), que utilizaremos cuando resaltemos el hecho de 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. Un anillo R se llama *noetheriano* si todo ideal de R es finito.

A continuación se mostrará dos definiciones alternativas los cuales también se utilizan para mostrar que un anillo cumple la condición de ser noetheriano.

Definición 2.2. Una cadena ascendente de ideales en R es *estacionaria*, es decir, si

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

entonces, existe un entero m tal que $a_n = a_m$ para todo $n \geq m$.

Definición 2.3. La *condición maximal*, dice que R tiene un *ideal maximal*, si dado cualquier conjunto no vacío $\mathscr{G}$ de ideales, existe un ideal $\mathfrak{a}$ en el conjunto $\mathscr{G}$ y tal que si $\mathfrak{b}$ pertenece a $\mathscr{G}$ con $\mathfrak{a} \subseteq \mathfrak{b}$, entonces $\mathfrak{a} = \mathfrak{b}$.

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

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

Teorema 2.1. Los siguientes tres enunciados son equivalentes en el anillo R:

(1) El anillo R cumple la condición de cadena ascendente;

(2) La condición de ideal maximal, cumple en R;

(3) Todos y cada uno de los ideales en R son generados finitamente, es equivalente a decir que: R es noetherino.

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

Una vez más, ya que $\mathfrak{a}_2$ no es maximal, entonces existe un $\mathfrak{a}_3 \in \mathscr{G}$ tal que $\mathfrak{a}_3 \supset \mathfrak{a}_2$ y así sucesivamente. Esto da una contradicción porque en la sucesión $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \ldots$ va en contra de la condición de cadena ascendente, definición 2.3.

(2) $\Rightarrow$ (3): Ahora supongamos que cumple la condición de maximal y sea $\mathfrak{a}$ un ideal dado. Denotemos por $\mathscr{G}$ el conjunto de todos los ideales finitamente generados que están contenidos en $\mathfrak{a}$ entonces $\mathscr{G}$ no es vacío porque contiene a (0). Si $\mathfrak{a}^* = Ra_1 + Ra_2 + \cdots + Ra_n$ es un ideal del conjunto $\mathscr{G}$ 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, pues $\mathfrak{a}^*$ y por tanto, habríamos demostrado que (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

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

pertenecerá a $\mathscr{G}$ y contendrán estrictamente a $\mathfrak{a}^*$. Esto, sin embargo, es imposible por la elección de $\mathfrak{a}^*$, pues es maximal.

(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 $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots$ 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 tal que 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, tiene una base finita. Sea $\mathfrak{a} = (a_1, a_2, \ldots, a_n)$ y para cada i asignamos m_i así que $\mathfrak{a}_i \subseteq \mathfrak{a}_{m_i}$, entonces todos los a_i están en $\mathfrak{a}_m$, donde

$$m = \text{máx}\{m_1, m_2, \ldots, m_n\}$$

Ahora, si $n > m$ tenemos

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

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

Proposición 2.1. 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 $\mathscr{B}$ el conjunto de todos los ideales en R, en otras palabras,

$$\mathscr{B} = \left\{\mathfrak{a} : \mathfrak{a} \neq R,\ \mathfrak{a} \text{ es un ideal de } R\right\}$$

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

Ahora por ser R un anillo noetheriano por el Teorema 2.1 entonces la condición de cadena ascendente y la condición maximal se mantiene en R.

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

Si $x, y \in \mathfrak{a}$, entonces existen $\mathfrak{b}_1, \mathfrak{b}_2 \in \mathscr{G}$ de modo que $x \in \mathfrak{b}_1$, $y \in \mathfrak{b}_2$, pero como $\mathscr{G}$ 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 $\mathfrak{b}_1 \in \mathscr{G}$ tal que $x \in \mathfrak{b}_1$, entonces $rx \in \mathfrak{b}_1 \subset \mathfrak{a}$ en consecuencia $rx \in \mathfrak{a}$.

Por tanto $\mathfrak{a} = \bigcup_{\mathfrak{a} \in \mathscr{G}} \mathfrak{b}$ 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 2.4. Se dice 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, implica bien $\mathfrak{a} = \mathfrak{b}$ o $\mathfrak{a} = \mathfrak{c}$.

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

Lema 2.1. Si R es noetheriano, entonces todo ideal se puede representar como la intersección de un número finito de ideales irreducibles.

Demostración. Sea $\mathscr{G}$ el conjunto de todos los ideales que no es la intersección finita del ideal irreducible. Tenemos que demostrar que $\mathscr{G}$ es vacío.

Asumiendo lo contrario y por el Teorema 2.1, podemos encontrar un ideal $\mathfrak{a} \in \mathscr{G}$ que es maximal para el conjunto $\mathscr{G}$. Dado que $\mathfrak{a} \in \mathscr{G}$, 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 aplicada a $\mathfrak{a}, \mathfrak{b} \in \mathscr{G}$ y $c \notin \mathscr{G}$, 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 $\mathfrak{a} \in \mathscr{G}$, entonces es una contradicción.

Por lo tanto R se puede representar como la intersección de un número finito de ideales irreducibles. □

Lema 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 tales que $bc \in \mathfrak{a}$, $c \notin \mathfrak{a}$, y ninguna potencia de b está en $\mathfrak{a}$.

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

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

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

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

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 el elemento $x = a + rb^m$, donde $a \in \mathfrak{a}$ y $r \in R$. También tenemos que $x \in (\mathfrak{a} : (b^m))$ y como $x = a + rb^m$, entonces al multiplicar la ecuación anterior a ambos lados por b^m tenemos

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

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. □

Los conceptos de ideal primario y descomposición primaria si bien pueden generalizarse a todo tipo de anillos conmutativos y unitarios sin embargo, en estos anillos no todo ideal tiene porque admitir una descomposición primaria. Gracias a Emmy Noether sabemos que en un anillo noetheriano en particular en $K[x_1, x_2, \ldots, x_n]$, todo ideal admite una descomposición primaria.

Teorema 2.2. En un anillo noetheriano R todo 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 2.1 tenemos que

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

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

Luego como cada $\mathfrak{a}_i$ es irreducible por el Lema 2.2 tenemos que cada $\mathfrak{a}_i$ es primario y luego por la Definición 1.7 el ideal $\mathfrak{a}$ 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 2.2. 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 finitamente generado, es decir, $\mathfrak{b} = Rb_1 + Rb_2 + \cdots + Rb_n$.

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

Pongamos

$$m = m_1 + m_2 + \cdots + m_n,$$

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

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

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

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

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. Sea R un anillo noetheriano, $\mathfrak{m}$ un ideal maximal de R y $\mathfrak{q}$ 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) $\Rightarrow$ (3): Como $\mathfrak{q}$ es $\mathfrak{m}-$primario, entonces por Definición 1.19 tenemos que $\mathfrak{m} = r(\mathfrak{q})$ y por la Definición 1.15 potencia de un ideal, 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) $\Rightarrow$ (2): Partamos de que $\mathfrak{m}^n \subseteq \mathfrak{q} \subseteq \mathfrak{m}$ para algún $n > 0$. Tomando radicales en la relación tenemos:

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

Luego por la Proposición 1.3 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 se tiene que

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

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

(2) $\Rightarrow$ (1): Por la Definición 1.19 está claro que si $r(\mathfrak{q}) = \mathfrak{m}$, entonces $\mathfrak{q}$ es $\mathfrak{m}$-primario. □

Corolario 2.1. 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.

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

$$r(\mathfrak{q}) = \left\{\mathfrak{q} \in R : \ x^n \in \mathfrak{q},\, n > 0,\, n \in \mathbb{N}\right\},$$

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 finitamente generado, tal que

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

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 $\alpha = \alpha_1 + \alpha_2 + \cdots + \alpha_n$.

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

$$p_1^{\beta_1}, p_2^{\beta_2}, \cdots, p_n^{\beta_n}$$

donde los β_i son números enteros positivos tales que

$$\beta_1 + \beta_2 + \cdots + \beta_n = \alpha_1 + \alpha_2 + \cdots + \alpha_n,$$

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

$$p_2^{\beta_2}, p_2^{\beta_2}, \cdots, p_n^{\beta_n} \in \mathfrak{q}.$$

Entonces todos los generadores de $\mathfrak{p}^\alpha$ están en $\mathfrak{q}$. Por lo tanto $\mathfrak{p}^\alpha \subset \mathfrak{q}$ para algún entero positivo α. □

En síntesis lo que quiere mostrar el corolario anterior es que si $\mathfrak{p}$ es un ideal primario en un anillo noetheriano, una de las condiciones necesarias para que el ideal dado sea $\mathfrak{p}$-primario es que el ideal contenga una potencia de $\mathfrak{p}$.

Hay una situación importante en la que la condición es suficiente así como necesaria, por lo que podemos mencionar el siguiente resultado.

Proposición 2.4. 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 una potencia de $\mathfrak{p}$.

Pero como $\mathfrak{a}$ es $\mathfrak{p}$-primario y R es un anillo noetheriano por el Corolario 2.1, existe un entero positivo m tal que

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

Por lo tanto para alguna potencia de $\mathfrak{a}$ está contenido en $\mathfrak{p}$.

Recíprocamente, supongamos que $\mathfrak{a}$ contiene una potencia 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 contiene a $\mathfrak{a}$.
Como tenemos que

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

por la Proposición 2.3,(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 solo si contiene una potencia de $\mathfrak{p}$. □

2.4. Teorema de la base de Hilbert

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

Una expresión como $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ se llama un *polinomio en la variable* x.

El coeficiente de x^i en este polinomio es a_i, si $i \leq n$ y cero si $i > n$. Dos polinomios

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \quad \text{y } b_0 + b_1x + b_2x^2 + \cdots + b_px^p$$

se consideran *iguales*, si y sólo si, los coeficientes de x^i son iguales en ambos polinomios para todos los valores de i. La suma y la multiplicación de polinomios se definen de 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 se llama la *nula polinómica*, que tiene todos sus coeficientes igual a cero. Los polinomios constantes, son aquellos 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 único $a+0x+0x^2+\cdots$, 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 el polinomio 1 constante, o de acuerdo con nuestras identificaciones, es simplemente el elemento unidad de R. Por el *coeficiente principal* de $f(x) = a_0+a_1x+a_2x^2+\cdots+a_nx^n$ 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 $x_1, x_2, \ldots, x_n$ con coeficientes en R, en cuyo caso se obtiene el anillo que se denota por $R[x_1, x_2, \ldots, x_n]$.

Teorema 2.3 (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 $\mathscr{U}$ es un ideal de $R[x]$ y además supongamos que $\mathscr{U}$ es generado finitamente. Los elementos de $\mathscr{U}$ son polinomios. Formemos un conjunto $\mathfrak{a}$, de elementos de R, formado por los coeficientes principales de todos los polinomios en $\mathscr{U}$ 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 $\alpha_1 x^m + \cdots$ y $\alpha_2 x^n + \cdots$ que están en $\mathscr{U}$. Y sea $p = m + n$, multipliquemos el primer polinomio por x^n y el segundo polinomio por x^m, de este modo, obtenemos dos polinomios

$$\alpha_1 x^p + \cdots \text{ y } \alpha_2 x^p + \cdots$$

y ambos están en $\mathscr{U}$, cuando los sumamos tenemos

$$(\alpha_1 x^p + \cdots) + (\alpha_2 x^p + \cdots) = (\alpha_1 + \alpha_2) x^p + \cdots \in \mathscr{U},$$

y cuando hacemos la resta tenemos

$$(\alpha_1 x^p + \cdots) - (\alpha_2 x^p + \cdots) = (\alpha_1 - \alpha_2) x^p + \cdots \in \mathscr{U},$$

entonces $\alpha_1 + \alpha_2 \in \mathfrak{a}$ y $\alpha_1 - \alpha_2 \in \mathfrak{a}$.

Además, si $r \in R$, entonces

$$r(\alpha_1 x^p + \cdots) = (r\alpha_1) x^p + \cdots \in \mathscr{U}$$

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, $\mathfrak{a} = (\alpha_1, \alpha_2, \ldots, \alpha_h)$, de modo que existen polinomios $f_1 = f_1(x), f_2 = f_2(x), \ldots, f_h = f_h(x)$ tal que $f_i \in \mathscr{U}$ 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, digamos de grado N, para obtener

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

Consideremos todos los polinomios en $\mathscr{U}$ 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, $\mathfrak{b} = (\beta_1, \beta_2, \ldots, \beta_k)$ y podemos elegir los polinomios $g_1 = g_1(x), g_2 = g_2(x), \ldots, g_k = g_k(x)$ tal que

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

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

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

Mediante este procedimiento, obtenemos un conjunto finito

$$f_1, f_2, \ldots, f_h, g_1, g_2, \ldots, g_k, h_1, h_2, \ldots, h_l$$

de polinomios. Estos polinomios están todos en $\mathscr{U}$. Vamos a demostrar que estos polinomios generan $\mathscr{U}$. Supongamos que $\phi(x) = \alpha x^p + \cdots$ pertenece a $\mathscr{U}$, entonces $\alpha \in \mathfrak{a}$, es decir,

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

donde $\omega_i \in R$.

Si $P > N$, entonces

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

está de nuevo en $\mathscr{U}$, pero tiene 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 $A_1(x), A_2(x), \ldots, A_h(x)$, tal que

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

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

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

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

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

como lo es en

$$\nu_1 h_1(x) + \nu_2 h_2(x) + \cdots + \nu_l h_l(x).$$

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

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

donde $\psi(x) = \mu_1(x)g_1(x) + \mu_2(x)g_2(x) + \cdots + \mu_k(x)g_k(x) + \nu_1 h_1(x) + \cdots + \nu_l h_l(x) + \cdots$ y como lo hemos escrito como una combinación lineal de los polinomios

$$f_1, f_2, \ldots, f_h, g_1, g_2, \ldots, g_k, h_1, h_2, \ldots, h_l,$$

por la Definición 1.3 de un ideal generado por un conjunto entonces estos polinomios generan finitamente a $\mathscr{U}$. Y por definición de anillo noetheriano entonces $R[x]$ es noetheriano. □

Ejemplo 2.1. 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 2.2. Si R es un anillo noetheriano, entonces el anillo de polinomios $R[x_1, x_2, \ldots, x_n]$ también es noetheriano.

Demostración. Supongamos que $R_0 = R$, y que $R_i = R[x_1, x_2, \ldots, x_i]$ para $1 \leq i \leq n$.

Puesto que cada polinomio en $x_1, x_2, \ldots, x_{i+1}$ puede considerarse, precisamente de una manera, como un polinomio en x_{i+1} cuyos coeficientes son polinomios en $x_1, x_2, \ldots, x_i$, 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 que R_i sea 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 $R_n = R[x_1, x_2, \ldots, x_n]$, es decir, que R_n es noetheriano. Por lo tanto, $R[x_1, x_2, \ldots, x_n]$ es noetheriano. □

2.5. Homomorfismos e isomorfismos

Definición 2.5. Si una aplicación σ de un anillo R aplicado sobre un anillo R' es tal que $\sigma(a+b) = \sigma(a) + \sigma(b)$ 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 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 aplicado sobre un anillo R'. Debemos notar que, aunque $\sigma(0)$ debe ser el elemento cero de R', y puede suceder que $\sigma(1)$ no sea el elemento unidad de R'.

Definición 2.6. Si σ es un homomorfismo de R sobre R' 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', decimos también que R y R' son isomorfos y lo denotamos por $R \cong R'$.

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

Definición 2.7. Consideremos un anillo R y un ideal $\mathfrak{a}$. Diremos que dos elementos x_1 y x_2 de R son congruentes módulo $\mathfrak{a}$, abreviado $x_1 \equiv x_2 \pmod{\mathfrak{a}}$, si $x_1 - x_2 \in \mathfrak{a}$. O equivalentemente $x_2 \equiv x_1 \pmod{\mathfrak{a}}$.

Esta relación entre los elementos es relación de equivalencia.

Vamos a decir que es *reflexiva* cuando cumple que $x \equiv x \pmod{\mathfrak{a}}$ para todo $x \in R$, se entenderá que es *simétrica* cuando se cumpla que $x \equiv y \pmod{\mathfrak{a}}$ entonces $y \equiv x \pmod{\mathfrak{a}}$ para todo $x, y \in R$ y por *transitividad* cuando $x \equiv y \pmod{\mathfrak{a}}$ y $y \equiv z \pmod{\mathfrak{a}}$ entonces tenemos que $x \equiv z \pmod{\mathfrak{a}}$ 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 2.3. Sean $x_1 \equiv x_2 \pmod{\mathfrak{a}}$ y $y_1 \equiv y_2 \pmod{\mathfrak{a}}$, entonces tenemos que $x_1 + y_1 \equiv x_2 + y_2 \pmod{\mathfrak{a}}$, $x_1 - y_1 \equiv x_2 - y_2 \pmod{\mathfrak{a}}$ y que $x_1 y_1 \equiv x_2 y_2 \pmod{\mathfrak{a}}$.

Demostración. Como tenemos que $x_1 \equiv x_2 \pmod{\mathfrak{a}}$ y si $y_1 \equiv y_2 \pmod{\mathfrak{a}}$, 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 usando la hipótesis $x_1 - x_2 \in \mathfrak{a}$ y que $y_1 - y_2 \in \mathfrak{a}$, tenemos que:

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

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

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

Por hipótesis $x_1 - x_2 \in \mathfrak{a}$ y que $y_1 - y_2 \in \mathfrak{a}$, tenemos que:

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

Para probar que $x_1 y_1 \equiv x_2 y_2 \pmod{\mathfrak{a}}$ tenemos que probar que:

$$x_1 y_1 - x_2 y_2 \in \mathfrak{a}. \tag{α}$$

Entonces a (α) sumemos y restemos al mismo tiempo el termino $x_2 y_1$ y agrupamos de manera conveniente para poder aplicar la hipótesis entonces tenemos:

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

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 $(x_1 y_1) - (x_2 y_2)$ están todos en $\mathfrak{a}$.

Y esto es lo que queríamos demostrar. □

Proposición 2.5. La función que asigna cada elemento a su clase de residuos módulo $\mathfrak{a}$, es un homomorfismo.

Demostración. Sea σ una función de R sobre $R/\mathfrak{a}$ tal que tomamos un elemento x y la lleva a las clases de residuo $x+\mathfrak{a}$, es decir, $\sigma(x) = x+\mathfrak{a}$.

Probemos que σ es un homomorfismo. Sean x e y elementos de R, entonces

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

Tenemos que demostrar que $\sigma(x+y) = \sigma(x)+\sigma(y)$.

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

Por lo tantos tenemos:

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

Ahora probemos que se cumple para el producto.

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

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 2.6. La imagen de los generadores de un anillo noetheriano 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'. Pongamos que $\mathfrak{a} = \sigma^{-1}(\mathfrak{a}')$, entonces $\mathfrak{a}$ es un ideal del anillo noetheriano y por lo tanto es finitamente generado, es decir,

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

Al aplicarle el homomorfismo al ideal $\mathfrak{a}$, tenemos:

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

Entonces $\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_n)$ generan a $\sigma(\mathfrak{a}) = \mathfrak{a}'$, es decir $\mathfrak{a}'$ es finitamente generado.
Por lo tanto $\sigma(a)$ es noetheriano. □

3 Variedades algebraicas afines

El conjunto de soluciones de un sistema de ecuaciones algebraicas se llama una *variedad algebraica afín*. Se podría considerar como objeto de la geometría en espacios afines. En este capítulo se estudiará sus propiedades básicas y su relación con la teoría de ideales.

3.1. Ideales y variedades

Trabajamos con un k cuerpo algebraicamente cerrado y $k[x] = k[x_1, x_2, \ldots, x_n]$ el anillo noetheriano de polinomios en n términos finitos con coeficientes en k.

Notación.- Denotamos k^n al espacio afín n-dimensional sobre k, es decir, al conjunto de $x = (x_1, x_2, \ldots, x_n)$ con $x_i \in k$, con la estructura de espacio afín.

Definición 3.1. Sea $X \subset k[x]$ finito. El conjunto

$$U = V(X) = \left\{x \in k^n : f(x) = 0; \text{ para todo } f \in X\right\}$$

se llama la *variedad algebraica afín* definida por X.

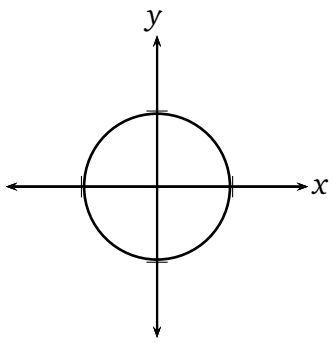
En general, decimos que un conjunto de puntos $U \subset k^n$ es una variedad algebraica afín, si existe $X \subset k[x]$ tal que $U = V(X)$.

En otras palabras, una variedad algebraica afín $V(X) \subset k^n$ es el conjunto de todas las soluciones del sistema de ecuaciones

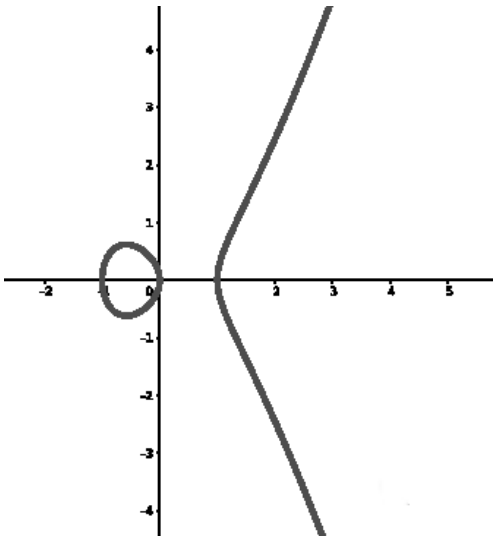
$$f_1(x_1, x_2, \ldots, x_n) = f_2(x_1, x_2, \ldots, x_n) = \cdots = f_n(x_1, x_2, \ldots, x_n) = 0,$$

con $f_1, f_2, \ldots, f_n \in X$.

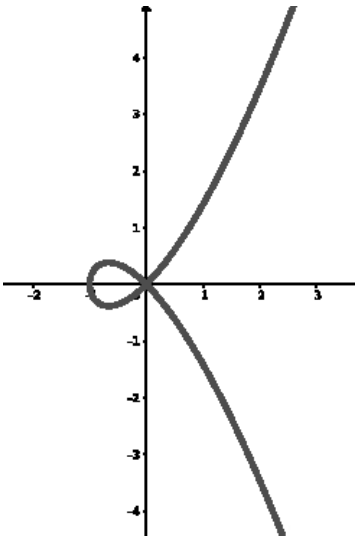
Ejemplo 3.1. (a) Tomando $k = \mathbb{R}$ y $n = 2$, entonces $k^n = \mathbb{R}^2$. La variedad $V(x^2 + y^2 - 1)$ no es más que el círculo unitario.



(b) Sea $k^n = \mathbb{R}^2$ se tiene la variedad $V\left(y^2 - x(x^2-1)\right)$



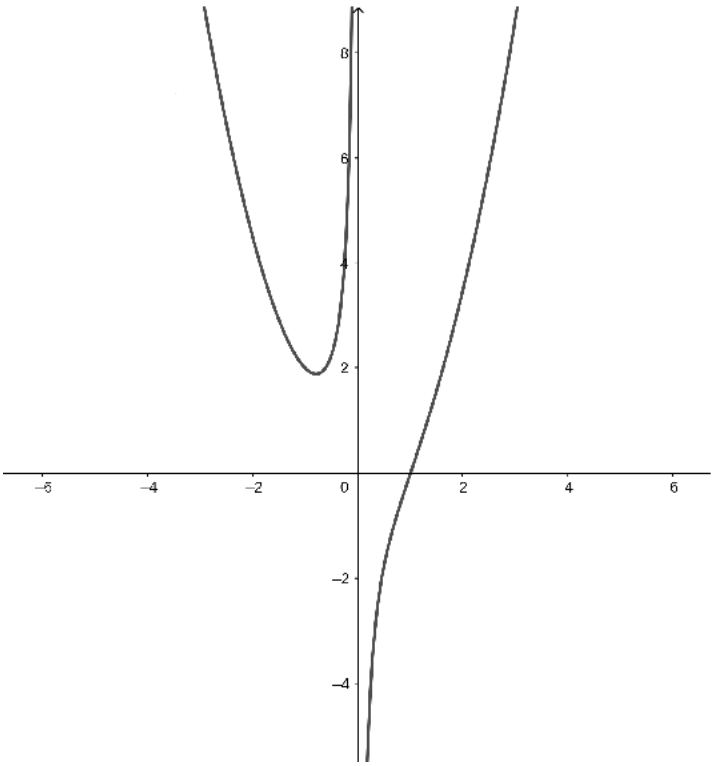
(c) Sea $k^n = \mathbb{R}^2$, $V\left(y^2 - x^2(x+1)\right)$.



Mencionar que las secciones cónicas que se estudian en geometría analítica (círculos, elipses, hipérbolas y parábolas) también son variedades afines. Al igual que el gráfico de las funciones

polinómicas son variedades afines. Así el gráfico de $y = f(x)$ es $V(y - f(x))$.

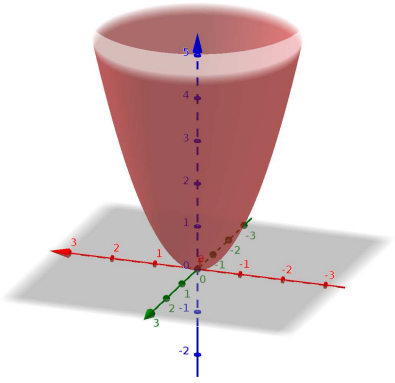
Aunque no siempre es obvio, el gráfico de una función racional también define una variedad algebraica afín. Por ejemplo, considere el gráfico de $y = \frac{x^3-1}{x}$.



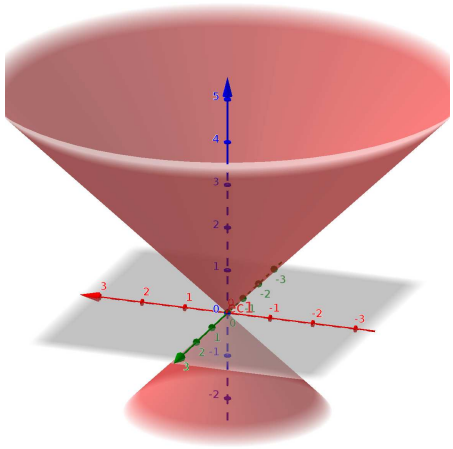
Es fácil ver que esta ecuación define la variedad algebraica afín $V(xy - x^3 + 1)$.

A continuación se verá una variedad afín algebraica afín en el espacio tridimensional $\mathbb{R}^3$ que puede ser dada por un paraboloide de revolución.

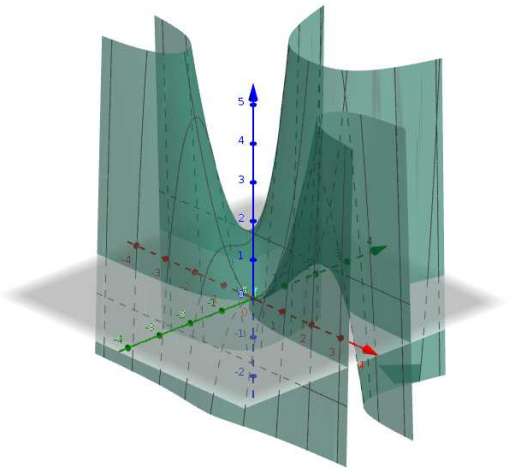
(d) Sea $k^n = \mathbb{R}^3$, $V(z - x^2 - y^2)$, se obtiene al rotar la parábola $z = x^2$ alrededor del eje z.



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

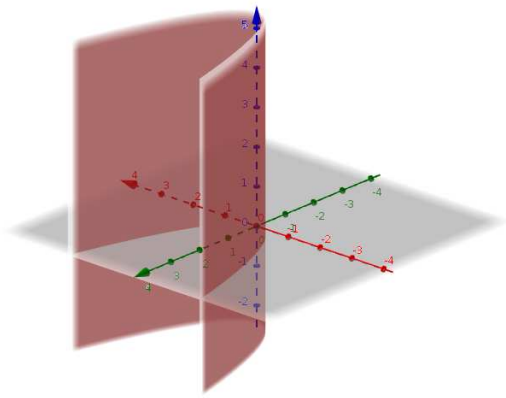


(f) Mucho más complicada es la superficie dada por $V(x^2 - y^2x^2 + y^3)$:

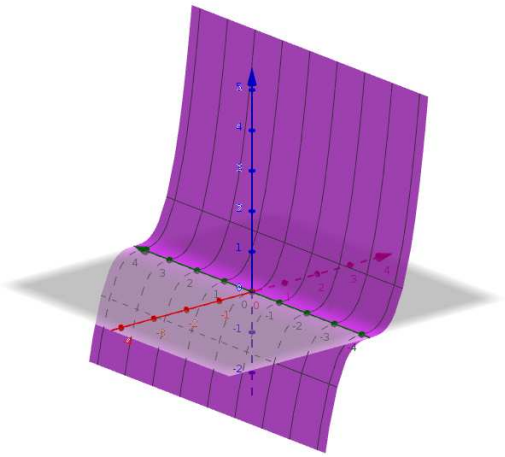


En estos dos últimos ejemplos, las superficies no son uniformes en todas partes: el cono tiene un punto fuerte en el origen, y el último ejemplo se cruza a lo largo de todo el eje. Estos son ejemplos de *puntos singulares*.

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:

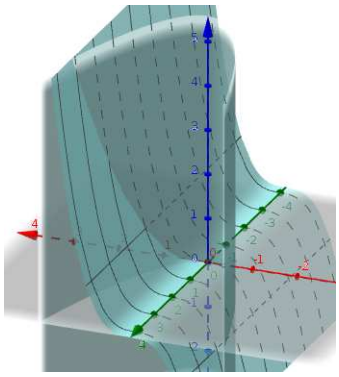


$y = x^2$



$z = x^3$

Entonces su intersección da el cubo retorcido:



Un concepto familiar de variedades de mayor dimensión se obtiene del álgebra lineal. Suponiendo que k es un cuerpo, y consideremos un sistema de m ecuaciones lineales en n incógnitas $x_1, x_2, \ldots, x_n$ con coeficientes en k:

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ \vdots \\ a_{1m}x_1 + \cdots + a_{mn}x_n = b_m \end{cases} \tag{3.1}$$

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 (3.1), 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 $\nabla f = (F_x, F_y, F_z)$]. Esto da el siguiente sistema de cuatro ecuaciones con cuatro incógnitas, x, y, z, λ, a resolver:

$$\begin{cases} 3x^2 + 2yz = 2x\lambda \\ 2xz = 2y\lambda \\ 2xy - 2z = 2z\lambda \\ x^2 + y^2 + z^2 = 1 \end{cases} \tag{3.2}$$

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

Hay que mencionar también que las algebraicas afines podría 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 sí tiene 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 $xy = 1$.

Definición 3.2. 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 $gf \in \mathfrak{a}$

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

El objetivo aquí es introducir algunos ejemplos de ideales de origen natural en el anillo de polinomios 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 es el ideal generado por un número finito de polinomios.

Definición 3.3. Sea $X \subset k[x]$. Definimos el *ideal generado por* X como

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

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. Y las sumamos, obtenemos

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

que es una combinación de nuestro sistema original. Observe que el lado izquierdo de 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 siguiente 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

$$\begin{aligned} x - 1 - t &= 0 \\ y - 1 - t^2 &= 0 \end{aligned} \tag{3.3}$$

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

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

Al sumarlas obtenemos

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

En términos del ideal generado por las ecuaciones (3.3), podemos escribir esto como

$$x^2 - 2x + 2 - y = (x - 1 + t)(x - 1 - t) + (-1)(y - 1 - t^2) \in \langle x - 1 - t, y - 1 - t^2 \rangle$$

De manera similar, cualquier otra combinación del sistema (3.3) conduce a un elemento de este ideal.

Decimos que un ideal k es finitamente generado si existen $f_1, f_2, \ldots, f_\lambda \in k[x]$ de tal manera que $\mathfrak{a} = \langle f_1, f_2, \ldots, f_\lambda \rangle$ y decimos que $\langle f_1, f_2, \ldots, f_\lambda \rangle$ 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*. 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 subespacio: ambos tienen que ser cerrados bajo la adición y la multiplicación, con la diferencia de que, para un subespacio, se multiplica por escalares, mientras que para un ideal, se multiplica por polinomios. Además, observe que el ideal generado por los polinomios $f_1, f_2, \ldots, f_\lambda$ es similar al subespacio generado por un número finito de vectores $v_1, v_2, \ldots, v_\lambda$. En cada caso, se tiene combinaciones lineales, utilizando los respectivos coeficientes del campo, escalares y polinomios.

Otro papel 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. Si $f_1, f_2, \ldots, f_\lambda$ y $g_1, g_2, \ldots, g_\mu$ son bases del mismo ideal en $k[x]$, de modo que $\langle f_1, f_2, \ldots, f_\lambda \rangle = \langle g_1, g_2, \ldots, g_\mu \rangle$, entonces tenemos que $V(f_1, f_2, \ldots, f_\lambda) = V(g_1, g_2, \ldots, g_\mu)$.

Demostración. Sea $x \in V(f_1, f_2, \ldots, f_\lambda)$, entonces $f_i(x) = 0$ para todo $1 \leq i \leq \lambda$, es decir, $f_1(x) = f_2(x) = \cdots = f_\lambda(x) = 0$.

Luego si $f_1(x) = 0$, le multiplicamos por $h_1(x) \in k[x]$ tomando el mismo elemento 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 $h_2(x)f_2(x) = 0$.

$$\begin{aligned} &h_1(x)f_2(x) \\ &h_2(x)f_2(x) \\ &\vdots \\ &h_\lambda(x)f_\lambda(x) \end{aligned} \tag{β}$$

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 sumar (β) 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 lineales, es decir, que es generado por $\langle f_1, f_2, \ldots, f_\lambda \rangle$; pero por hipótesis $\langle f_1, f_2, \ldots, f_\lambda \rangle = \langle g_1, g_2, \ldots, g_\mu \rangle$ entonces $t(x) = \sum_{i=1}^{\lambda} h_i(x)f_i(x) = 0 = \sum_{i=1}^{\mu} q_i(x)g_i(x)$ con $h_i, q_i \in k[x]$, entonces $x \in V(g_1, g_2, \ldots, g_\mu)$. La otra inclusión es análoga. □

Ejemplo 3.2. 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 los puntos singulares son $(\pm i, \pm 1)$.
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 3.4. Sea $\mathfrak{a} \subset k[x]$ un ideal, definimos la *variedad del ideal* $\mathfrak{a}$ como

$$V(\mathfrak{a}) = \left\{x \in k^n : f(x) = 0, \text{ para todo } f \in \mathfrak{a}\right\}.$$

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 $f_1, f_2, \ldots, f_\lambda \in \mathfrak{a}$ tales que $\mathfrak{a} = \langle f_1, f_2, \ldots, f_\lambda\rangle$, además $\mathfrak{a}$ es el conjunto de los puntos singulares de estos polinomios. Por lo tanto, tenemos un mapeo:

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

Ya se mencionó antes que existe esa correspondencia entre ideales y variedades afines. Sin embargo, notar que no es una correspondencia uno a uno, ya que diferentes ideales pueden dar lugar a 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 necesidad de que k sea algebraicamente cerrado.

Lema 3.1. 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 la 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 $V(\mathfrak{a}) \supset V(\mathfrak{b})$. □

Proposición 3.2. 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 la 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 $f \in X$, es decir y es un cero común de todos los

polinomios de X (y también lo es de cualquier elemento que sea una combinación lineal de X con coeficientes en $k[x]$). Entonces tenemos que para todo $f \in \mathfrak{a}$,

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

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 3.3. Sean $\mathfrak{a} = \langle f_1, f_2, \ldots, f_n \rangle$ y $\mathfrak{b} = \langle g_1, g_2, \ldots, g_n \rangle$ ideales en $k[x]$. Entonces

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

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

(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 $g_j \in \mathfrak{b}$. Por tanto

$$f_1(x) = f_2(x) = \cdots = f_n(x) = g_1(x) = g_2(x) = \cdots = g_m(x) = 0$$

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 la 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 $V(\mathfrak{a}) \cap V(\mathfrak{b}) \subseteq V(\mathfrak{a}+\mathfrak{b})$. Por lo tanto $V(\mathfrak{a}+\mathfrak{b}) = V(\mathfrak{a}) \cap V(\mathfrak{b})$.

(ii) Sea $x \in V(\mathfrak{a}) \cup V(\mathfrak{b})$, entonces $x \in V(\mathfrak{a})$ o $x \in V(\mathfrak{b})$, es decir, que $f(x) = 0$ para todo $f \in \mathfrak{a}$ o $g(x) = 0$ 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 g polinomio en $\mathfrak{b}$ tenemos

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

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

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

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

Recíprocamente supongamos que $x \in V(\mathfrak{a}\mathfrak{b})$ 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

$$f(x)g(x) \neq 0$$
$$(fg)(x) \neq 0$$

y por lo tanto $x \notin V(\mathfrak{ab})$ teniendo una contradicción 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 $V(\mathfrak{a} \cap \mathfrak{b}) \subseteq V(\mathfrak{a}) \cup V(\mathfrak{b})$. 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 $g \in b$ tal que $g(x) \neq 0$.
Luego el polinomio fg está en $\mathfrak{a}$ y en $\mathfrak{b}$, por lo que fg está en $\mathfrak{a} \cap \mathfrak{b}$, entonces tenemos

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

para todo $h \in \mathfrak{a} \cap \mathfrak{b}$, así $x \notin V(\mathfrak{a} \cap \mathfrak{b})$. Por tanto $V(\mathfrak{a} \cap \mathfrak{b}) \subseteq V(\mathfrak{a}) \cup V(\mathfrak{b})$.
Sabemos por (ii) esta proposición que $V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{ab})$, entonces $V(\mathfrak{a}) \cap V(\mathfrak{b}) \subseteq V(\mathfrak{ab})$.
Finalmente supongamos que $x \in V(\mathfrak{ab})$ pues $x \notin V(\mathfrak{a} \cap \mathfrak{b})$, entonces existe $f \in \mathfrak{a} \cap \mathfrak{b}$ tal que $f(x) \neq 0$. Pero por la proposición 1.2, (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 $x \notin V(\mathfrak{ab})$. Esto es una contradicción pues $x \in V(\mathfrak{ab})$.
Por tanto $V(\mathfrak{ab}) \subseteq V(\mathfrak{a} \cap \mathfrak{b})$.
Así, $V(\mathfrak{ab}) = V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$.

□

3.2. El ideal de una variedad

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

Definición 3.5. Sea $X \subset k^n$ una variedad afín y consideremos el conjunto de todos los polinomios $g \in k[x] = k[x_1, x_2, \ldots, x_n]$. Definimos el conjunto $\mathfrak{a}(X)$ como

$$\mathfrak{a}(X) = \big\{ g \in k[x] : \, g(x) = 0 \text{ para todo } x \in X \big\}.$$

Este conjunto es un ideal en el anillo de polinomios y lo llamaremos el *ideal de la variedad* X.

Lema 3.2. Para cualquier variedad $X \subset k^n$, se cumple que $V\big(\mathfrak{a}(X)\big) = X$.

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 $X \subseteq V\big(\mathfrak{a}(X)\big)$.

Para la otra inclusión, tomemos funciones polinómicas $g_1, g_2, \ldots, g_n$ tales que

$$X = V(g_1, g_2, \ldots, g_n) = \big\{ x \in k^n : \, g_i(x) = 0 \text{ para todo } 1 \leq i \leq n \big\}.$$

Entonces $g_1, g_2, \ldots, g_n \in \mathfrak{a}(X)$.

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

En consecuencia, $x \in X$ y entonces $V\big(\mathfrak{a}(X)\big) \subseteq X$. Por lo tanto $V\big(\mathfrak{a}(X)\big) = X$. □

Lema 3.3. 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 3.4. Sea $V_1 \supset V_2 \supset V_3 \supset \ldots$, una cadena descendente de variedades en k^n. Entonces existe un entero $N \geq 1$ tal que

$$V_N = V_{N+1} = V_{N+2} = \ldots$$

Demostración. Partamos de la cadena descendente de variedades

$$V_1 \supset V_2 \supset V_3 \supset \cdots$$

Tomando los ideales que generan esas variedades por el Lema 3.3 obtenemos

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

Por la condición de cadenas ascendentes de ideales esta cadena es estacionaria, es decir, existe un $N \in \mathbb{N}$ tal que

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

Tomando ahora las variedades de estos ideales, tenemos

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

pero por el Lema 3.2 tenemos que $V\big(\mathfrak{a}(V_N)\big) = V_N$. Por lo tanto existe un $N \geq 1$ tal que $V_N = V_{N+1} = V_{N+2} = \cdots$ □

Proposición 3.5. Sea $(\mathfrak{a}_\alpha) \in R$ una familia cualesquiera de ideales que están en el anillo $R \subseteq k[x]$ entonces:

1. Si $V_\alpha = V\big(\mathfrak{a}(V_\alpha)\big)$ para todo $\alpha \in R$, entonces $\bigcap_{\alpha\in R} V_\alpha = V\big(\bigcup_{\alpha\in R} \mathfrak{a}(V_\alpha)\big)$
2. Si $V_j = \big(\mathfrak{a}(V_j)\big)$ para todo $j = 1, 2, \ldots, r$, entonces $\bigcup_{j=1}^{r} V_j = V\big(\prod_{i=1}^{r} \mathfrak{a}(V_j)\big)$.
3. $V(0) = k^n$ y $V(1) = \emptyset$.
4. $V(\mathfrak{a}) = V\big(r(\mathfrak{a})\big)$.

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 $\alpha \in R$ 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 $\alpha \in R$. Luego por el Lema 3.2, tenemos que $V_\alpha = V\big(\mathfrak{a}(V_\alpha)\big)$, entonces $x \in V\big(\mathfrak{a}(V_\alpha)\big)$, por lo que $f(x) = 0$, entonces $x \in V\big(\bigcup_{\alpha\in R} \mathfrak{a}(V_\alpha)\big)$.

Por tanto $\bigcap_{\alpha\in R} V_\alpha \subseteq V\big(\bigcup_{\alpha\in R}\mathfrak{a}(V_\alpha)\big)$.
($\supseteq$) Sea $x \in V\big(\bigcup_{\alpha\in R}\mathfrak{a}(V_\alpha)\big)$ entonces para todo $f \in \bigcup_{\alpha\in R}\mathfrak{a}(V_\alpha)$, tenemos 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 $x \in V\big(\mathfrak{a}(V_\alpha)\big)$ para todo $\alpha \in R$.
Así $x \in \bigcap_{\alpha\in R} V\big(\mathfrak{a}(V_\alpha)\big)$. De nuevo por el Lema 3.2 $x \in \bigcap_{\alpha\in R} V_\alpha$. Por tanto $\bigcap_{\alpha\in R} V\alpha \supseteq V\big(\bigcup_{\alpha\in R}\mathfrak{a}(V_\alpha)\big)$.

2. ($\subseteq$) Sea $x \in \bigcup_{j=1}^{r} V_j$, entonces existe un $j \in \{1, 2, \ldots, r\}$ tal que $x \in V_j$, pero por el Lema 3.2 tenemos que $V_j = V\big(\mathfrak{a}(V_j)\big)$ y $x \in \big(\mathfrak{a}(V_j)\big)$. Entonces podemos asignar para todo $f_j \in \mathfrak{a}(V_j)$, $f_j(x) = 0$ y en consecuencia
$$f_1(x)f_2(x)\cdots f_r(x) = 0$$
porque $f_j \in \mathfrak{a}(V_j)$. Por lo tanto, $x \in V\big(\prod_{j=1}^{r}\mathfrak{a}(V_j)\big)$.
($\supseteq$) Supongamos que $x \notin \bigcup_{j=1}^{r} V_j$. Por el Lema 3.2 para cualquier variedad $V\big(\mathfrak{a}(V_j)\big) = V_j$, entonces $x \notin \bigcup_{j=1}^{r} V\big(\mathfrak{a}(V_j)\big)$, entonces $x \notin V\big(\mathfrak{a}(V_j)\big)$. Así

   - para $V\big(\mathfrak{a}(V_1)\big)$, existe entonces un $f_1 \in \mathfrak{a}(V_1)$ tal que $f_1(x) \neq 0$;
   - para $V\big(\mathfrak{a}(V_2)\big)$, existe entonces un $f_2 \in \mathfrak{a}(V_2)$ tal que $f_2(x) \neq 0$ y así sucesivamente hasta r. Es decir,
   - para $V\big(\mathfrak{a}(V_r)\big)$ existe un $f_r \in \mathfrak{a}(V_r)$ tal que $f_r(x) \neq 0$.
     Luego si consideramos el producto
     $$f_1(x)f_2(x)\cdots f_r(x)$$
     tenemos que este polinomio es no nulo, con lo que $x \notin V\big(\prod_{j=1}^{r}\mathfrak{a}(V_j)\big)$ ya que
     $$\mathfrak{a}(V_i) = \left\{\prod_{j=1}^{r} f_j : f_j \in \mathfrak{a}(V_j),\ j \in 1, 2, \ldots, r\right\}$$
     Por lo tanto $\bigcup_{j=1}^{r} V_j \supseteq V\big(\prod_{j=1}^{r}\mathfrak{a}(V_j)\big)$.

3. ($\subseteq$) Sea $x \in V(0)$, entonces por la definición de una variedad $x \in k^n$. Por lo que $V(0) \subseteq k^n$.
($\supseteq$) Sea $x \in k^n$, por la 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 $V(1) = \emptyset$. Por definición.
$$V(1) = \{x \in k^n :\ f(x) = 0;\ \text{para todo } f \in 1\}$$
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 la Definición 3.4 $f(x) = 0$ para todo $f \in \mathfrak{a}$. Sabemos que $\mathfrak{a} \subseteq r(\mathfrak{a})$, entonces $f \in r(\mathfrak{a})$, y por Definición 3.4, $x \in \big(r(\mathfrak{a})\big)$. Como consecuencia $V(\mathfrak{a}) \subseteq V\big(r(\mathfrak{a})\big)$.

Sea $y \in V\big(r(\mathfrak{a})\big)$, entonces $f(y) = 0$ para todo $f \in r(\mathfrak{a})$, 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 todo $f \in \mathfrak{a}$, por la definición 3.4 tenemos $V\big(r(\mathfrak{a})\big) \subseteq V(\mathfrak{a})$. 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 3.6. Sea X el conjunto algebraico afín o también variedad algebraica afín definimos el anillo cociente como

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

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 3.6. 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 todo $x \in X$. 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 son dos polinomios que definen la misma función polinomio en X. □

3.4. Descomposición de variedades

Retomemos la idea de descomponer variedades.

Definición 3.7. 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 $V = V_1$ o $V = V_2$.

Proposición 3.7. Sea $V \subseteq k^n$ una variedad algebraica afín, entonces V se puede escribir como una unión finita

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

donde cada V_i es una variedad irreducible.

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

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

Si podemos descomponer 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 una unión de irreducibles, es decir,

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

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

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

Continuando este proceso, obtenemos una sucesión infinita de variedades

$$V \supsetneq V_1 \supsetneq V_2 \supsetneq V_3 \supsetneq \cdots$$

Como las inclusiones son estrictas, esto contradice la Proposición 3.4. Por tanto $V = V_1 \cup V_2 \cup \cdots \cup V_t$. □

Lema 3.4. Sea $\mathfrak{a} \subset k[x]$ un ideal y sean $f, g \in k[x]$ polinomios, 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 $x \in V(\mathfrak{a}, f)$ o $x \in V(\mathfrak{a}, g)$. 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

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

obtenemos que $x \in V(\mathfrak{a}, fg)$.

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

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

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

Suponiendo que $f(x) = 0$, obtenemos que $x \in V(\mathfrak{a}, f)$. Y suponiendo que $g(x) = 0$, obtenemos que $x \in V(a, g)$. Por lo tanto, $x \in V(\mathfrak{a}, f) \cup V(\mathfrak{a}, g)$. □

4

El Teorema de los ceros de Hilbert

El Teorema de la situación de los ceros (como podría versar la traducción del término Nullstellensatz del alemán al español) es la generalización del Teorema Fundamental del Álgebra de Gauss en el siguiente sentido: mientras que este último garantiza la existencia de las raíces o ceros de cualquier polinomio en una variable con coeficientes en $\mathbb{C}$, el Nullstellensatz de Hilbert extiende la aseveración a ciertos ideales de polinomios en varias variables, toda vez que los coeficientes de dichos polinomios pertenezcan a un campo algebraicamente cerrado. Antes de enunciarlo y probarlo, nos será útil considerar algunos resultados a cotinuación.

4.1. Lema de Normalización de Noether

Definición 4.1. Sea R un anillo, R un subanillo de R' tal que $1 \in R'$. Un elemento x de R se dice que es un *entero sobre* R' si x es una raíz de un polinomio mónico con coeficientes en R', es decir, si x satisface una ecuación de la forma

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

donde los a_i son elementos de R'.

Es evidente que cada elemento de R' es entero sobre R'.

Definición 4.2. 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 (Lema de Normalización de Noether)**.** Sea k un cuerpo y sea $R \neq 0$ una k-álgebra con generación finita. Entonces existen elementos $y_1, y_2, \ldots, y_r \in R$ que son *algebraicamente independiente*[1] sobre k y tales que R es un *entero* sobre $k[y_1, y_2, \ldots, y_r]$.

[1]Sea k un cuerpo y R $k-$álgebra. Un conjunto de n elementos $b_1, b_2, \ldots, b_n \in R$ se dice que es algebraicamente independiente sobre k si para cada polinomio $f \in k[x_1, x_2, \ldots, x_n]$ se verifica $f(b_1, b_2, \ldots, b_n) = 0$, se tiene que $f = 0$.

Demostración. Supongamos que k es infinito.
Sean $\{x_1, x_2, \ldots, x_n\}$ generadores de R como álgebra.

Luego sea $\{x_1, x_2, \ldots, x_r\}$ un subconjunto de $\{x_1, x_2, \ldots, x_n\}$ algebraicamente independiente sobre k y cada una de las $x_{r+1}, x_{r+2}, \ldots, x_n$ sean algebraicas sobre el anillo de polinomios $k[x_1, x_2, \ldots, x_r]$. 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 $f \in k[x_1, x_2, \ldots, x_n]$ tal que $f(x_1, x_2, \ldots, x_n) = a$ entonces $a \in k[x_1, x_2, \ldots, x_n]$ y donde $x - a$ es un polinomio mónico con coeficientes en $k[x_1, x_2, \ldots, x_n]$ en donde a es una raíz y por lo tanto R es un entero sobre $k[y_1, y_2, \ldots, y_r]$.

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

Como ya se mencionó F es la parte homogénea de mayor grado f.

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

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

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 $\lambda_1, \lambda_2, \ldots, \lambda_{n-1} \in k$ con coeficientes en el anillo de polinomios $k[\lambda_1, \lambda_2, \ldots, \lambda_{n-1}]$ tales que el polinomio $F(\lambda_1, \lambda_2, \ldots, \lambda_{n-1}, 1) \neq 0$.

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

Como $x_i' = x_i - \lambda_i x_n$, para toda $i = 1, 2, \ldots, n-1$ 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 $f(x_1, x_2, \ldots, x_{n-1}) = 0$ tenemos

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

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

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

Siendo $F(\lambda_1, \lambda_2, \ldots, \lambda_{n-1}, 1) \neq 0$, podemos dividir el polinomio en la ecuación 4.2 entre

$$F(\lambda_1, \lambda_2, \ldots, \lambda_{n-1}, 1)$$

y obtenemos un polinomio mónico

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

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

Por la Definición la 4.1 x_n es raíz del polinomio mónico (4.4) con coeficientes en $R'[x_i',\ldots,x_{n-1}']$ y por en consecuencia R es un entero sobre R'.

Por hipótesis de inducción, existen $y_1,y_2,\ldots,y_r$ algebraicamente independientes sobre k tales que R' es un entero sobre $k[y_1,y_2,\ldots,y_r]$ por la definición. Pero como los x_i (con $i<n$) son enteros sobre R', pues $x_i=x_i'+\lambda_i x_n$ entonces $x_1,x_2,\ldots,x_r$ son enteros sobre $k[y_1,y_2,\ldots,y_r]$. Por lo tanto R es un entero sobre $k[y_1,y_2,\ldots,y_r]$. □

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

Proposición 4.1. Sea k un campo algebraicamente cerrado[2] y sean $a_1,a_2,\ldots,a_n$ elementos de k, entonces todo ideal maximal $\mathfrak{a}$ del anillo de polinomios $k[x_1,x_2,\ldots,x_n]$ es de la forma

$$(x_1-a_1,x_2-a_2,\ldots,x_n-a_n),\quad a_i\in k.$$

Demostración. Sea $\mathfrak{a}=(x_1-a_1,x_2-a_2,\ldots,x_n-a_n)$ y supóngase que existe un ideal $\mathfrak{b}$ tal que $\mathfrak{a}\subseteq\mathfrak{b}\subseteq k$. Debemos probar que $\mathfrak{a}=\mathfrak{b}$ o $\mathfrak{b}=k$.

Sea $f\in\mathfrak{b}-\mathfrak{a}$, luego aplicando el algoritmo de la división, entre x_1-a_1 tenemos[3]

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

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:

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

Ahora sustituyendo todos los residuos en f tenemos

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

[2]Un campo k se dice *algebraicamente cerrado* si cada polinomio de grado al menos 1, con coeficientes en k, tiene un cero en k. En ese caso, cada polinomio de tal clase se descompone en factores lineales.

[3]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 $r(x)=0$ o $\partial^0 r(x)<\partial^0 g(x)$.

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

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

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

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 $r_n \in \mathfrak{b}$ inversible[4] de $\mathfrak{b}$ (ya que r_n es un elemento no nulo del cuerpo escalar k), entonces $\mathfrak{b} = k[x_1, x_2, \ldots, x_n]$.

Por lo tanto $(x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n)$ debe ser un ideal maximal. □

Teorema 4.1. Sea k un campo algebraicamente cerrado y sea $\mathfrak{a}$ un ideal maximal de $k[x_1, x_2, \ldots, x_n]$, entonces existen elementos $a_1, a_2, \ldots, a_n$ en k tales que

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

Demostración. Sea

$$\phi : k[x_i] \to k[x_1, x_2, \ldots, x_n]$$

un homomorfismo en el campo k.

Sea $\mathfrak{a} \subseteq k[x_1, x_2, \ldots, x_n]$ un ideal tomado en la imagen. Luego como $k[x_1, x_2, \ldots, x_n]$ es un anillo noetheriano, tenemos que $k[x_1, x_2, \ldots, x_n]$ es finitamente generado, entonces la pre-imagen $\phi^{-1}(\mathfrak{a}) = k[x_i] \cap \mathfrak{a}$ es también un ideal maximal, para cada $i = 1, 2, 3, \ldots, n$.

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 $a_1, a_2, \ldots, a_n \in k$ tal que $x_i - a_i \in \mathfrak{a}$ ya que $k[x_i] \cap \mathfrak{a} = (x_i - a_i)$. Entonces tenemos que $(x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n) \subseteq \mathfrak{a}$. Pero $\mathfrak{a}$ es un ideal maximal entonces $(x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n) = \mathfrak{a}$. Por tanto

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

□

Teorema 4.2 (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 $k[x_1, x_2, \ldots, x_n]$. Y si $\mathfrak{a}(X) \neq (1)$ entonces X es no vacío.

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

[4] 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 $\mathfrak{a} = R$.

Demostración. Sea $\mathfrak{a}$ un ideal propio de $k[x_1, x_2, \ldots, x_n]$, siendo k un anillo conmutativo con unidad y $\mathfrak{a} \neq k[x_1, x_2, \ldots, x_n]$, luego por la Proposición 2.1 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 $k[x_1, x_2, \ldots, x_n]$ entonces por el Teorema 4.1 existen elementos $a_1, a_2, \ldots, a_n$ en k, es decir, que el elemento $a = (a_1, a_2, \ldots, a_n) \in k$ tal que $\mathfrak{b} = (x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n)$ que es maximal.

Luego $\mathfrak{a} \subseteq \mathfrak{b}$ por el Lema 3.1 tenemos que $X(\mathfrak{a}) \supseteq X(\mathfrak{b})$.
Como $X(\mathfrak{b}) \subseteq X(\mathfrak{a})$, para ver que $X(\mathfrak{a}) \neq \emptyset$, bastará probar que $X(\mathfrak{b}) \neq \emptyset$.
Sea $f \in \mathfrak{b} = (x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n)$, luego existen $q_1, q_2, \ldots, q_n \in k[x_1, x_2, \ldots, x_n]$ tal que

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

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

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

Luego como $f(a) = 0_k$ para toda $f \in \mathfrak{b}$ por la Definición 3.4, tenemos que $a \in X(\mathfrak{b})$, por lo tanto $X(\mathfrak{b}) \neq \emptyset$ ya que $(a_1, a_2, \ldots, a_n) \in X(\mathfrak{b})$.

Como $X(\mathfrak{b}) \subseteq X(\mathfrak{a})$ entonces $a \in \mathfrak{a}$, es decir que, $a = (a_1, a_2, \ldots, a_n) \in \mathfrak{a}$. Por tanto $X(\mathfrak{a}) \neq \emptyset$. □

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

Teorema 4.3. Sea R el anillo de polinomios $k[x_1, x_2, \ldots, x_n]$ 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. $\subseteq$: Sean $f \in r(\mathfrak{a})$ y $x \in V(\mathfrak{a})$, entonces como existe un $n \in \mathbb{N}$ tal que $f^n \in \mathfrak{a}$.

Ahora como $x \in V(a)$, 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 3.5, $f \in \mathfrak{b}(V)$. Por tanto $r(\mathfrak{a}) \subseteq \mathfrak{b}(V)$.
$\supseteq$: Sea $f \in \mathfrak{b}(V)$. Como $\mathfrak{a}$ es un ideal de $R = k[x_1, x_2, \ldots, x_n]$ y como R es un anillo noetheriano, entonces $\mathfrak{a}$ es finitamente generado, es decir, que $\mathfrak{a} = (f_1, f_2, \ldots, f_m)$.

Introduzcamos un elemento adicional Y, y trabajemos en $k[x_1, x_2, \ldots, x_n, Y]$.

Sea $\mathfrak{a}^*$ el ideal de $k[x_1, x_2, \ldots, x_n, Y]$, generado por

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

Vamos a probar que $V(a^*) = \emptyset$.

Sean $(a_1, a_2, \ldots, a_n, a_{n+1}) \in V(\mathfrak{a}^*) \subseteq k^{n+1}$ y $(a_1, a_2, \ldots, a_n) \in V(\mathfrak{a})$. Entonces $f \in \mathfrak{a}$,

$$f(a_1, a_2, \ldots, a_n) = 0.$$

Evaluaremos el polinomio $1 - Yf$ en $(a_1, a_2, \ldots, a_n, a_{n+1})$.

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

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

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

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

Recordando que $\mathfrak{a}^*$ esta generado por $\left(f_1, f_2, \ldots, f_m, (1-Yf)\right)$, existe una combinación lineal para 1 tal que

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

Haciendo [5] $Y = \frac{1}{f}$ y evaluando la igualdad (4.8) en $(x_1, x_2, \ldots, x_n, Y)$ tenemos

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

[5] Este truco especial fue inventado por S. Rabinowitch en 1929 y en su honor fué bautizado como el truco de Rabinowitch, para más detalles ver R. MILES A. (1995), Undergraduate Conmutative Algebra, Cambridge University Press.

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

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

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

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

donde el producto de los polinomios $f^r g_i \in k[x_1, x_2, \ldots, x_n]$ y las $f_i \in \mathfrak{a}$, entonces $f^r \in \mathfrak{a}$ y por la Definición 1.15 $f \in \mathfrak{a}$.

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

Bibliografía

[1] D. Eisenbud. (1995). *Commutative Álgebra with a view towards Algebraic Geometry.* Springer-Verlag: Board.

[2] H. Matsumura. (1970). *Commutative Algebra.* New York: W.A.: Benjamin Co.

[3] M. Atiyah, I.G. Macdonald. (1973). *Introducción al Álgebra Conmutativa.* Barcelona: Editorial Reverté.

[4] P. Dubreil, M.L. Dubreil - Jacotin. (1961). *Lecciones de Álgebra Moderna.* Madrid España: Editorial Reverté.

[5] T. W. Hungerford. (1974). *Abstract Algebra an Introduction.* Boston: Cleveland

[6] Zariski O., Samuel P. (1975). *Commutative algebra.* Springer-Verlag: Omega.